NOTA DE FUNDAMENTARE

la proiectul Hotărârii de Guvern pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă

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

Autor: Ministerul Afacerilor Interne.

Alte autorități publice participante: Inspectoratul General al Poliției.

Sectorul privat: Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare; Moldcell S.A; Orange Moldova S.A; Moldtelecom S.A; StarNet S.R.L.

2. Condițiile ce au impus elaborarea proiectului actului normativ

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

Temeiul legal din care rezultă prezentul proiect de lege reprezintă:

1. acțiunea nr. 172 din Planul național de reglementări pentru anul 2025, aprobat prin Hotărârea Guvernului nr. 841/2024;

2. Art. II alin. (2) din Legea nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

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

Progresele considerabile în domeniul tehnologiilor informației și comunicațiilor au favorizat interconectarea unei societăți globale, ceea ce, din păcate, a dus la apariția unor noi infracțiuni de diferit calibru: criminalitatea informatică/cibernetică.

Criminalitatea informatică/cibernetică reprezintă activitatea de utilizare a sistemelor, rețelelor de calculatoare și în special a internetului pentru a comite infracțiuni.

Termenul a fost creat la sfârșitul anilor 1990, când internetul a început să se răspândească în America de Nord. Atunci a fost momentul cînd criminalitatea informatică/cibernetică a devenit o preocupare globală. Astfel, *„criminalitatea informatică/cibernetică”* a fost folosită pentru a desemna infracțiunile comise pe internet, în special cele legate de piraterie, pornografie și atacuri asupra sistemelor informatice.

Prin urmare, criminalitatea informatică/cibernetică se referă la un set de infracțiuni comise prin rețele de calculatoare și, în special, prin internet. Aceste infracțiuni includ pirateria, pornografia, fraudele prin telemarketing și altele. Conform Comisiei Europene, termenul include trei categorii de activități criminale:

- infracțiuni tradiționale, cum ar fi frauda informatică și falsificarea;
- difuzarea de conținut ilegal prin mijloace electronice, cum ar fi pornografia sau incitarea la ură rasială, etc.;
- atacuri asupra rețelelor electronice, cum ar fi atacurile asupra sistemelor informatice, atacurile de tip „*deny of service*”, „hacking-ul”, etc.

În contextul acestor amenințări, statele membre al Consiliului Europei, fiind conștiente de profundele schimbări determinate de digitalizarea, convergenta si globalizarea continuă a rețelelor de calculatoare; preocupate de riscul că rețelele de calculatoare si informația electronică ar putea fi utilizate si pentru comiterea de infracțiuni si că probele privind asemenea infracțiuni ar putea fi stocate și transmise prin intermediul acestor rețele; recunoscând necesitatea cooperării între state și industria privată în lupta împotriva criminalității informatice, precum și nevoia de a proteja interesele legitime în utilizarea si dezvoltarea tehnologiilor informației; considerând că lupta eficientă purtată împotriva criminalității informatice impune o cooperare internațională intensificată, rapidă si eficace în materie penală; au adoptat, la 23.11.2001, la Budapesta, Convenția privind criminalitatea informatică – act normativ care reglementează măsuri de prevenire și combatere a criminalității informatice/cibernetice. Totodată, la 28.01.2003, Consiliul Europei a adoptat Protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice. În final, la 28.02.2023, Consiliul Europei a

adoptat al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice.

În paralel, cu unele mici întârzieri, Republica Moldova a înregistrat progrese semnificative în domeniul combaterii criminalității informatice/cibernetice, care pot fi listate după cum urmează:

1. La 02.02.2009, Parlamentul Republicii Moldova a adoptat Legea nr. 6/2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică;

2. La 03.02.2009, Parlamentul Republicii Moldova a adoptat Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice;

3. La 03.02.2009, Parlamentul Republicii Moldova a adoptat Legea nr. 302/2016 pentru ratificarea Protocolului adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă comise prin intermediul sistemelor informatice;

4. La 09.11.2022, a fost semnat Decretul Președintelui Republicii Moldova, Maia Sandu, pentru aprobarea semnării celui de-al doilea Protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică referitor la cooperarea consolidată și divulgarea probelor electronice.

Aceste progrese normative au apropiat Republica Moldova tot mai mult de standardele Uniunii Europene de prevenire și combatere a criminalității informatice/cibernetice. Le fel, se menționează că, în anul 2024, au fost operate unele modificări în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice, care au dus la dezvoltarea instrumentelor de conservare a datelor informatice și de sistare a accesului la paginile web care conțin informații destinate și utilizate pentru comiterea infracțiunilor.

Potrivit noilor prevederi legale, subdiviziunea specializată din cadrul Ministerului Afacerilor Interne și Serviciul de Informații și Securitate dispun sistarea accesului la paginile web care sunt destinate și utilizate pentru pregătirea sau comiterea infracțiunilor în cazul în care informația publicată sau oferită în orice mod pe aceasta, inclusiv sub formă de linkuri, se referă la fapte infracționale. Pe de altă parte, furnizorii de servicii sunt obligați să sisteze, la solicitarea autorităților competente, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la paginile web ce cuprind informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor.

Totuși, prevederile legale referite mai sus nu oferă o reglementare completă a procedurii de sistare, fapt ce naște necesitatea elaborării prezentului proiect de hotărâre de Guvern, care vine să aprobe Instrucțiunile privind procedura de sistare a accesului la paginile web care conțin informații destinate și utilizate pentru comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă. Altfel spus, prezentul proiect de lege are ca scop crearea unui mecanism de interacțiune dintre organele de drept și furnizorii de servicii în vederea implementării prevederilor legale introduse în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

În același timp, prezentul proiect vine spre realizarea sarcinii trasate Guvernului, la Art. II alin. (2) din Legea nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, unde este indicat că Guvernul, în termen de 3 luni de la data intrării în vigoare a prezentei legi, va aproba instrucțiunile privind modul de emitere și executare a ordinelor emise în temeiul art. 4 alin. (1) lit. b) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice, adică a ordinelor de sistare a accesului la paginile web.

Prin urmare, prezentul proiect are ca scop definitivarea, perfecționarea mecanismului de sistare a accesului la paginile web destinate și utilizate pentru pregătirea sau comiterea infracțiunilor instituit prin Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Scopul și obiectivele Instrucțiunii:

Scopul Instrucțiunii constă în stabilirea procedurii de identificare a paginilor web care conțin informații destinate și utilizate pentru comiterea infracțiunilor și de interacțiune dintre Ministerul Afacerilor Interne și/sau Serviciul de Informații și Securitate, pe de o parte, și furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și/sau furnizorii de conținut, pe de altă parte, în ceea ce privește sistarea accesului la paginile web respective sau eliminarea conținutului respectiv la sursă.

Obiectivele Instrucțiunii sunt:

1. Prevenirea și combaterea criminalității informatice: reglementează identificarea și sistarea paginilor web care conțin informații destinate și utilizate pentru comiterea infracțiunilor, contribuind astfel la protejarea securității cibernetice;

2. Colaborarea eficientă între autorități și furnizorii de servicii de internet: stabilește proceduri clare pentru interacțiunea dintre Ministerul Afacerilor Interne, Serviciul de Informații și Securitate și furnizorii de servicii de acces la internet și găzduire de conținut online, pentru a asigura implementarea măsurilor de prevenire a criminalității informatice;

3. Protecția utilizatorilor de internet: prin sistarea accesului la site-uri infracționale și eliminarea conținutului ilegal, Instrucțiunea protejează utilizatorii de informații periculoase, cum ar fi cele legate de abuzuri sau activități ilegale;

4. Asigurarea unui cadru legal și proporțional de aplicare a măsurilor: reglementează aplicarea măsurilor într-un mod legal, proporțional și transparent, respectând drepturile fundamentale ale utilizatorilor și furnizorilor de servicii de internet;

5. Crearea unui mecanism de revizuire și contestare: oferă posibilitatea contestării măsurilor luate în instanță și stabilește proceduri de revizuire periodică a paginilor web care au fost sistate, asigurând astfel corectitudinea și echitatea în aplicarea Instrucțiunii.

Principalele prevederi ale proiectului și elementele noi care se conțin în cuprinsul acestuia:

Punctul 1 al Instrucțiunii reglementează procesul prin care autoritățile competente (Ministerul Afacerilor Interne și Serviciul de Informații și Securitate) pot identifica și lua măsuri împotriva paginilor web care conțin informații destinate și utilizate pentru comiterea infracțiunilor. De asemenea, stabilește cum vor interacționa autoritățile cu furnizorii de servicii de internet și găzduire de conținut pentru a opri accesul la aceste pagini sau pentru a elimina conținutul ilegal de pe ele. Scopul este protejarea securității cibernetice și prevenirea utilizării internetului pentru activități infracționale.

Punctul 2 definește noțiunile cheie utilizate în Instrucțiune pentru a asigura o înțelegere corectă a termenilor.

Punctul 3 din Instrucțiune explică când o pagină web va fi considerată ca având scop infracțional, menționându-se că acest lucru se poate întâmpla dacă pagina web oferă informații care încurajează sau facilitează comiterea de infracțiuni, conform legislației naționale (Legea nr. 20/2009). Aceasta include, de exemplu, site-uri care promovează activități ilegale, cum ar fi fraudele sau distribuirea de materiale ilegale.

Punctul 4 din Instrucțiune prevede că paginile web destinate sau utilizate pentru comiterea infracțiunilor pot fi identificate fie din oficiu, adică autoritățile descoperă site-urile pe cont propriu, fie pe baza unei sesizări din partea oricărei persoane fizice sau juridice.

Punctul 5 din Instrucțiune stabilește faptul că în situațiile când o persoană sau instituție sesizează autoritățile că o pagină web conține informații infracționale, această sesizare trebuie să fie formală, sub forma unei petiții, care va include detalii suficiente pentru ca autoritățile să poată evalua situația.

Punctul 6 reglementează procesul de intervenție al subdiviziunii specializate în cazul identificării unor pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, stabilind procedurile concrete pe care autoritățile trebuie să le urmeze pentru a combate difuzarea acestor informații online. În primul rând, subdiviziunea specializată trebuie să examineze paginile web identificate ca fiind posibile surse de informații ce sprijină

comiterea infracțiunilor, iar în urma acestei examinări autoritatea întocmește un act de evaluare detaliată care va reflecta conținutul considerat ilegal, motivând astfel necesitatea intervenției. În termen de 24 de ore, autoritățile sunt obligate să ia măsuri concrete pentru a elimina riscurile asociate acestor informații periculoase, iar dacă conținutul ilegal este găzduit de furnizori din Republica Moldova, se poate emite un ordin de eliminare a conținutului la sursă, cerând furnizorului să elimine respectivul conținut de pe platformele sale, pentru a preveni răspândirea acestuia. În caz contrar, dacă nu este posibilă eliminarea conținutului, se va emite un ordin de sistare a accesului, prin care se va solicita restricționarea accesului la pagina web respectivă, împiedicând utilizatorii din Republica Moldova să acceseze acea pagină. Scopul general al acestei proceduri este protejarea utilizatorilor de internet din Republica Moldova de conținuturi periculoase ce ar putea sprijini infracțiuni, prevenind astfel răspândirea unor informații ce pot fi folosite în scopuri ilegale, iar procedura impune un termen scurt de acțiune de 24 de ore pentru a asigura o intervenție rapidă și eficientă în fața riscurilor reprezentate de aceste site-uri.

Punctul 7 reglementează modalitatea de comunicare a ordinelor emise de autoritățile competente către furnizorii de servicii de găzduire sau furnizorii de conținut. În cazul emiterii unui Ordin de eliminare a conținutului la sursă sau a unui Ordin de sistare a accesului, acestea vor fi comunicate furnizorilor în două forme: în format fizic, dacă este necesar, și în format electronic prin intermediul poștei electronice guvernamentale a subdiviziunii specializate, asigurându-se astfel că ordinul ajunge rapid și în mod oficial la destinatar. De asemenea, ordinul va conține informațiile necesare, inclusiv adresa URL a paginii web unde urmează a fi restricționat accesul, care va fi comunicată în format textual, pentru a fi ușor identificată de către furnizorii de servicii sau conținut, astfel încât aceștia să poată lua măsurile necesare.

Punctul 8 din Instrucțiune enumeră principiile de care se ghidează actorii implicați la aplicarea măsurilor, astfel încât activitatea respectivă să fie corectă și proporțională. Autoritățile trebuie să aplice cele mai puțin restrictive tehnici pentru a preveni accesul, fără a afecta inutil alte aspecte ale internetului. De asemenea, trebuie să informeze furnizorii de servicii despre motivele măsurii și despre cum pot contesta ordinul emis.

Punctul 9 reglementează conținutul și structura unui Ordin de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă, stabilind elementele esențiale care trebuie să fie incluse în document pentru a asigura transparența și legalitatea măsurii. Ordinul trebuie să conțină informații clare care identifică autoritatea emitentă, pentru a asigura transparența și responsabilitatea acțiunii, precum și temeiul juridic al măsurii, pentru a justifica măsurile impuse și a se asigura că procedura respectă cadrul normativ existent. De asemenea, ordinul trebuie să motiveze de ce informațiile sau conținutul online sunt considerate destinate sau utilizate pentru pregătirea ori comiterea infracțiunilor, prin prezentarea argumentelor specifice care susțin evaluarea autorităților și a temeiurilor legale invocate, astfel încât furnizorii să înțeleagă clar rațiunea luării acestor măsuri. În plus, ordinul va include informații suficiente pentru ca furnizorul de servicii să poată localiza și identifica conținutul care trebuie eliminat sau la care trebuie să se restricționeze accesul, incluzând cel puțin adrese URL specifice și, dacă este necesar, informații suplimentare. În final, Ordinul va informa furnizorul despre posibilitatea de a contesta măsura și despre termenul în care poate face acest lucru, garantând astfel dreptul de apărare al părților implicate.

Punctul 10 din Instrucțiune precizează faptul că Ordinul de sistare a accesului sau de eliminare a conținutului trebuie să fie publicat pe site-ul autorităților competente, pentru a asigura transparența și pentru ca persoanele afectate să fie informate, în termen de 10 zile.

Punctul 11 din Instrucțiune ne spune că Ordinul poate fi contestat în instanță de către orice persoană care consideră că i-au fost încălcate drepturile, inclusiv de către furnizorii de servicii sau conținut. Contestarea nu va suspenda efectele ordinului, adică măsurile vor rămâne în vigoare până la o decizie judecătorească.

Punctul 12 din Instrucțiune precizează că toate documentele legate de aplicarea Instrucțiunii trebuie păstrate conform legii pentru a fi utilizate în cazul unui control sau a unei verificări ulterioare.

Punctul 13 din Instrucțiune menționează că în situațiile în care autoritățile specializate refuză să emită un ordin de sistare a accesului sau de eliminare a conținutului, persoanele interesate pot contesta acest refuz în instanță.

Punctele 14 și 15 din Instrucțiune stabilesc că furnizorii de servicii de internet sunt obligați să aplice ordinul de sistare a accesului imediat, dar nu mai târziu de ziua lucrătoare următoare primirii acestuia. Ei pot utiliza diverse metode tehnice pentru a bloca accesul la site-urile respective.

Punctul 16 din Instrucțiune precizează faptul că autoritățile competente vor crea o pagină web care va conține informații despre paginile web blocate, motivele pentru care accesul a fost sistat, autoritatea emitentă și modalitățile de contestare a ordinului.

Punctul 17 din Instrucțiune comunică faptul că, după aplicarea măsurii de sistare a accesului, furnizorii de internet vor redirecționa utilizatorii care încearcă să acceseze pagini web blocate către o pagină web dedicată, administrată de autoritățile competente, care va informa utilizatorii despre motivul blocării.

Punctul 18 din Instrucțiune este despre restabilirea accesului. Dacă autoritățile decid să ridice măsura de sistare a accesului, furnizorii de internet trebuie să restabilească accesul la paginile web respective. Acest lucru poate apărea după ce au fost înlăturate informațiile infracționale sau dacă măsurile nu mai sunt justificate.

Punctul 19 din Instrucțiune reglementează procedura deblocării paginii web care a fost supusă procedurii de sistare la cererea persoanei interesate.

Punctul 20 din Instrucțiune reglementează acțiunile autorității competente în condițiile recepționării unei cereri primite în baza punctului 19. Actul procesual prin care se va dispune anularea parțială sau integrală a Ordinul de sistare a accesului și/sau Ordinul de eliminare a conținutului la sursă va fi Ordinul.

Punctul 21 din Instrucțiune reglementează o procedură simplificate pentru paginile care distribuie materiale de abuz sexual asupra minorilor (pornografie infantilă). În aceste cazuri, Ordinul de sistare se emite fără întocmirea unui Act privind examinarea paginilor web în cauză și fără adresarea prealabilă către furnizorul de găzduire sau de conținut.

Punctul 22 din Instrucțiune prevede că autoritățile vor comunica furnizorilor de servicii de internet și de găzduire a conținutului lista cu paginile web care promovează pornografia infantilă, astfel încât aceștia să poată lua măsuri imediate pentru a le bloca.

Punctul 23 din Instrucțiune oferă posibilitatea furnizorilor de servicii să sisteze materialele ilegale din oficiu. Astfel, furnizorii de servicii de internet pot lua măsuri pro-activ pentru a sista paginile care distribuie materiale de abuz sexual asupra minorilor și care sunt incluse în lista elaborată de Organizația Internațională a Poliției Criminale (The INTERPOL "Worst of" List), fără a fi necesar să urmeze procedura prevăzută în Instrucțiune.

Punctul 24 reglementează mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului.

Intrarea în vigoare:

Potrivit dispozițiilor tranzitorii ale Legii nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice:

Art. II. – (1) Prezenta lege intră în vigoare la expirarea a 3 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) Guvernul, în termen de 3 luni de la data intrării în vigoare a prezentei legi, va aproba instrucțiunile privind modul de emitere și executare a ordinelor emise în temeiul art. 4 alin. (1) lit. b) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

Astfel, Legea nr. 200/2024 a fost publicată în Monitorul Oficial la 15.08.2024 și a intrat în vigoare la 14.11.2024. Prin urmare, Guvernul avea obligația ca până la 13.02.2025 să aprobe această instrucțiune.

Potrivit art. 56 alin. (3) din Legea nr. 100/2017 cu privire la actele normative, intrarea în vigoare a actelor normative poate fi stabilită pentru o altă dată doar în cazul în care se

urmăreşte protecţia drepturilor şi libertăţilor fundamentale ale omului, realizarea angajamentelor internaţionale ale Republicii Moldova, conformarea cadrului normativ hotărîrilor Curţii Constituţionale, eliminarea unor lacune din legislație sau contradicţii între actele normative ori dacă există alte circumstanţe obiective.

Prin urmare, având în vedere circumstanțele de drept și de fapt menționate mai sus, se consideră justificat și necesar ca prezenta hotărâre să intre în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

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

Menționăm că, în urma analizelor efectuate, nu au fost identificate opțiuni alternative.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul nu presupune impact structural și instituțional asupra sistemului administrației publice. Ceea ce se schimbă este faptul că autoritățile competente din subordinea Ministerului Afacerilor Interne și/sau Serviciul de Informații și Securitate vor avea competența să dispună sistarea accesului la paginile web ce conțin date și informații utilizate sau destinate pentru comiterea infracțiunilor.

4.2. Impactul financiar și argumentarea costurilor estimative

Proiectul nu presupune costuri financiare suplimentare.

4.3. Impactul asupra sectorului privat

În partea ce se referă la sectorul privat, se menționează că furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și furnizorii de conținut vor începe să execute obligațiile ce le-au revenit conform modificărilor operate în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice. Aceste obligații pot fi sumarizate după cum urmează:

1. Creşterea responsabilității în monitorizarea și filtrarea conținutului: furnizorii de servicii de internet și de găzduire a conținutului vor avea o responsabilitate mult mai mare în ceea ce privește monitorizarea și gestionarea conținutului găzduit pe platformele lor. Aceștia vor fi obligați să acționeze rapid pentru a elimina conținutul sau bloca accesul la paginile care conțin informații ilegale, cum ar fi site-uri care promovează infracțiuni, fraude, sau pornografia infantilă. În unele cazuri, furnizorii pot fi obligați să intervină imediat, fără a aștepta un ordin formal, dacă detectează conținut care poate avea un impact dăunător;

2. Costuri suplimentare și investiții în tehnologie: potrivit celor comunicate Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare; Moldcell S.A; Orange Moldova S.A; Moldtelecom S.A; StarNet S.R.L nu sunt preconizate costuri suplimentare, fiindcă mecanismul a fost deja implementat.

3. Creşterea costurilor operaționale: nu este aplicabil.

4. Necesitatea conformării rapide cu ordinele autorităților: furnizorii de internet vor fi obligați să acționeze rapid pentru a implementa măsurile de blocare a site-urilor sau de eliminare a conținutului ilegal. Aceste măsuri trebuie implementate în termen de 24 de ore de la primirea unui ordin.

4.4. Impactul social

Implementarea acestei Instrucțiuni va aduce un impact pozitiv semnificativ asupra cetățenilor, asigurând un mediu online mai sigur și mai protejat. Prin blocarea și eliminarea rapidă a conținutului ilegal și periculos, cetățenii vor fi expuși mai puțin la informații dăunătoare, cum ar fi fraudele online, pornografia infantilă sau incitarea la violență. De asemenea, Instrucțiunea asigură transparență și protecția drepturilor utilizatorilor, oferindu-le posibilitatea de a contesta măsurile luate și de a fi informați în mod clar despre motivele blocării paginii web. În acest fel, cetățenii vor avea acces la o experiență online mai sigură și mai responsabilă, protejându-le integritatea și securitatea personală.

4.4.1. Impactul asupra datelor cu caracter personal

Implementarea acestei instrucțiuni va avea un impact pozitiv asupra protecției datelor cu caracter personal, întrucât măsurile de blocare a accesului la site-uri sau eliminare a

conținutului ilegal vor contribui la reducerea riscurilor de expunere a datelor personale pe platformele online periculoase. Prin prevenirea accesului la pagini web care promovează activități infracționale, cum ar fi fraudele sau furtul de identitate, cetățenii vor fi mai bine protejați împotriva riscurilor de abuzuri și atacuri cibernetice. În plus, reglementările asigură transparență în procesul de luare a măsurilor, ceea ce contribuie la încrederea cetățenilor că datele lor personale sunt gestionate în mod responsabil și securizat.
4.4.2. Impactul asupra echității și egalității de gen
Implementarea acestei instrucțiuni poate avea un impact pozitiv asupra echității și egalității de gen, prin crearea unui mediu online mai sigur și mai protejat pentru toate persoanele, indiferent de sex sau gen. Prin eliminarea conținutului ilegal și dăunător, inclusiv materialele care pot incita la discriminare, violență de gen sau hărțuire online, Instrucțiunea va contribui la protejarea drepturilor femeilor, bărbaților și persoanelor non-binare. De asemenea, măsurile de prevenire a accesului la pagini web care promovează comportamente abuzive sau infracționale vor ajuta la asigurarea unui spațiu virtual mai echitabil, în care toate persoanele se pot simți în siguranță, fără teama de a fi expuse unor tratamente inechitabile sau abuzuri pe baza genului.
4.5. Impactul asupra mediului
Deși Instrucțiunea se concentrează pe securitatea cibernetică și protecția cetățenilor online, aplicarea sa poate aduce și un impact pozitiv indirect asupra mediului. Prin eliminarea paginilor web care conțin conținut dăunător, precum infracțiuni informatice sau fraude, se reduce utilizarea de resurse tehnologice, cum ar fi lățimea de bandă și capacitatea serverelor, care sunt necesare pentru a găzdui și distribui acest conținut. Astfel, se poate reduce consumul de energie asociat cu aceste activități online.
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
Nu este aplicabil.
5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE
Nu este aplicabil.
6. Avizarea și consultarea publică a proiectului actului normativ
Lista autorităților și instituțiilor a căror avizare este necesară: 1. Ministerul Finanțelor; 2. Ministerul Muncii și Protecției Sociale; 3. Ministerul Dezvoltării Economice și Digitalizării; 4. Ministerul Educației și Cercetării; 5. Ministerul Culturii; 6. Serviciul de Informații și Securitate 7. Procuratura Generală; 8. Consiliul Superior al Magistraturii Proiectul a fost elaborat cu sprijinul Asociației naționale a companiilor din sectorul tehnologii informaționale și comunicare. Totodată, împreună cu Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare, a companiilor Moldcell S.A; Orange Moldova S.A; Moldtelecom S.A; StarNet S.R.L s-a organizat o ședință comună de lucru în care a fost abordat fiecare punct al proiectului, decizându-se versiunea finală al acestora. De asemenea, proiectul a fost prezentat la Masa rotundă „*Parteneriat pentru siguranța copiilor online: reglementări și soluții pentru eliminarea conținutului ilegal*” organizat de La Strada, la 24 ianuarie 2025. Avizarea a fost realizată, avizele au fost recepționate și Sinteza a fost elaborată Anunțul privind inițierea elaborării proiectului a fost plasat pe site-ul web Particip.gov.md la adresa: https://particip.gov.md/ro/document/stages/proiectul-hotararii-de-

guvern-pentru-aprobarea-regulamentului-privind-procedura-de-sistare-a-accesului-la-paginile-web-care-contin-informatii-destinate-si-utilizate-pentru-comiterea-infractiunilor/13515.

Anunțul despre inițierea procedurii de avizare a proiectului, număr unic /MAI/2025, autor Ministerul Afacerilor Interne a fost plasat pe site-ul web Particip.gov.md la adresa: https://particip.gov.md/ro/document/stages/proiectul-hotararii-de-guvern-pentru-aprobarea-instructiunii-privind-procedura-de-sistare-a-accesului-la-pagini-web-care-contin-informatii-destinate-si-utilizate-pentru-pregatirea-sau-comiterea-infractiunilor-si-de-eliminare-a-continutului-respectiv-la-sursa/14136.

7. Concluziile expertizelor

Ministerul Justiției

Raportul de expertiză nu conține o Concluzie separată. Totuși toate propunerile au fost examinate, iar proiectul Instrucțiunii a fost racordat la cerințele formulate de Ministerul Justiției (a se vedea Sinteza).

Centrul Național Anticorupție

Proiectul hotărârii Guvernului pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă, în scopul creării unui mecanism de interacțiune dintre organele de drept și furnizorii de servicii în vederea implementării prevederilor legale introduse în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

Proiectul corespunde normelor de tehnică legislativă și respectă parțial rigorile de transparență impuse de Legea nr.239/2008 privind transparența în procesul decizional.

Proiectul corespunde interesului public general, în cazul în care prevederile acestuia vor fi aplicate cu respectarea strictă a cadrului legal, adică evitarea unor eventuale abuzuri din partea entităților responsabile de sistarea accesului la paginile web.

În normele proiectului supus expertizei anticorupție au fost identificați următorii factori de corupție:

– utilizarea neuniformă a termenilor;

– formulare ambiguă care admite interpretări abuzive;

– concurența normelor de drept.

În scopul preîntâmpinării apariției manifestărilor de corupție la aplicarea în practică a prevederilor proiectului, considerăm oportună redactarea acestuia în contextul obiecțiilor și recomandărilor din prezentul raport de expertiză anticorupție.

8. Modul de încorporare a actului în cadrul normativ existent

Nu este aplicabil

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Nu este aplicabil.

Ministru afacerilor interne /semnat/ Daniella MISAIL-NICHITIN