



SIGURANȚA , ONLINE A COPIILOR

Studiu de politici publice

Cum poate fi îmbunătățit răspunsul statului pentru a preveni și combate abuzul sexual online față de copii?



Siguranța online a copiilor. Studiu de politici publice.

Cum poate fi îmbunătățit răspunsul statului pentru a preveni și combate abuzul sexual online față de copii?

Acest studiu de politici publice a fost elaborat de către autor în anul 2020 în cadrul proiectului „Public Policy Fellowship”, implementat de către Departamentul Buna Guvernare al Fundației Soros Moldova. Opiniile exprimate în acest studiu de politici publice aparțin în exclusivitate autorului și nu reflectă neapărat punctul de vedere al Fundației Soros Moldova sau al partenerilor săi. Dreptul de autor asupra acestui studiu aparține în egală măsură autorului precum și Fundației Soros Moldova. Autorul oferă Fundației Soros Moldova dreptul de a edita și difuza studiul fără niciun fel de restricții.

Autoare:

Elena BOTEZATU, avocată, Directoare a Programului Copii, Centrul Internațional „La Strada Moldova”

Coordonatorii studiului:

Ana REVENCO

Victor GOTIȘAN

Pentru informații suplimentare despre prezenta publicație, ne puteți contacta:

Fundația Soros Moldova, 2019

str. Bulgara, nr. 32, mun. Chișinău,
Republica Moldova, MD-2001

Telefon: +373 22 274 480,
+373 22 270 031 Fax: +373 22 270 507,

E-mail: foundation@soros.md

AO Centrul Internațional „La Strada”

MD-2012, CP 259, Chișinău,
Republica Moldova

Tel.: (+373) 22 23 49 06
Fax.: (+373) 22 23 49 07

E-mail: office@lastrada.md www.lastrada.md

Cuprins

| | |
|--|----|
| Introducere | 5 |
| Sumarul executiv | 6 |
| Metodologia cercetării | 9 |
| 1. Copiii în mediul online: tendințe și riscuri asociate | 11 |
| 2. Rolul statului în diminuarea riscurilor cărora se expun copiii online.... | 19 |
| 2.1. Cartografierea politicilor naționale în domeniu | 20 |
| 2.2. Realizări și restanțe în implementarea politicilor | 26 |
| 2.3. Mecanismul de coordonare a politicilor | 29 |
| 2.4. Lacune și provocări identificate..... | 32 |
| 3. Standarde și abordări internaționale | 37 |
| 3.1. Modul de integrare a siguranței copiilor online în politicile internaționale..... | 38 |
| 3.2. Dimensiuni ale politicilor în domeniul siguranței online | 43 |
| 3.3. Modele de coordonare a eforturilor | 47 |
| Concluzii generale și recomandări | 51 |
| Recomandări de ordin strategic | 53 |
| Recomandări operaționale..... | 55 |
| Referințe | 58 |

Introducere

În anul 2017, Guvernul Republicii Moldova a adoptat pentru prima dată un Plan de Acțiuni ce își propunea să promoveze siguranța copiilor online, cu implicarea unui spectru divers de autorități și instituții publice. Documentul a fost aprobat în contextul mediatizării unui joc online periculos pentru copii¹, care a bulversat opinia publică și întreg sistemul de protecție a copiilor, sistemul de drept și sistemul educațional, semnalând despre necesitatea unor măsuri urgente și consolidate pentru prevenirea unor situații similare.

Procesul de implementare a acestui document de politici a fost unul provocator, mai ales că sistemul a fost luat pe nepregătite, siguranța online a ajuns brusc subiect de interes, iar nivelul de cunoaștere a subiectului era minim. Măsurile de siguranță online au fost abordate în special din perspectiva tehnologică, de securizare a accesului, navigării online, a dispozitivelor digitale, dar nu de formare a comportamentelor și abilităților de gândire critică ale copiilor. În pofda acțiunilor întreprinse, datele statistice

indică despre un nivel sporit al riscurilor de abuz sexual în mediul online la care se expun copiii. Unul dintre factorii ce contribuie la acest risc este atitudinea adolescenților față de expedierea fotografiilor intime în mediul online persoanelor cu care comunică și inițierea unor relații online cu persoane necunoscute.

La trei ani de implementare a acestui Plan de Acțiuni, e necesară evaluarea eforturilor întreprinse și stabilirea unui nou curs al acțiunilor de promovare a siguranței online. Totodată, e necesară o analiză aprofundată a conceptului de siguranță online: ce presupune acesta și la ce aspecte face referire, care sunt practicile altor state în domeniu, care sunt recomandările și politicile internaționale ce ar putea seta un cadru directoriu de elaborare a propriilor politici.

Scopul prezentului studiu este de a analiza cadrul politicilor publice naționale și internaționale în domeniul siguranței copiilor online, de a prezenta experiența statelor europene în elaborarea și coordonarea politicilor în domeniu și de a formula recomandări de politici publice pentru Republica Moldova (RM), conform necesităților identificate.

¹ Joc online cunoscut cu denumirea de „Babelena albastră”.

Sumarul executiv

În contextul expirării mai multor documente de politici ce reglementau măsuri de promovare a siguranței copiilor online (Planul de acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților, Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 și Planul de acțiuni pentru implementarea acestuia, etc.), a devenit necesară stabilirea următoarelor priorități în domeniu.

În ultimii ani, în RM s-au înregistrat mai multe progrese în domeniul promovării siguranței online a copiilor, cu scopul de a reduce din riscurile online. Documentele de politici ce reglementau acțiuni menite să promoveze siguranța copiilor online au o abordare complexă, fiind planificate acțiuni ce vizează diferite domenii de competență, începând cu promovarea siguranței copiilor online, acțiuni menite să contribuie la reducerea conținutului ilegal din Internet, până la acțiuni de actualizare a cadrului legal în domeniul abuzului sexual și exploatării sexuale, facilitate de utilizarea tehnologiilor informaționale și de comunicare (TIC).

Pentru fiecare document de politici ce planifica acțiuni în domeniul siguranței online a copiilor au fost stabilite propriile mecanisme de coordonare a eforturilor, fără să existe însă o platformă unică de discuții și monitorizare a tuturor acțiunilor în domeniu. Aceste mecanisme de coordonare nu sunt interconectate. Din acest motiv, procesul de monitorizare și evaluare este inefficient, fiind limitat la raportarea rezultatelor statistice, adesea dublate în diferite rapoarte.

Principalele realizări în domeniul siguranței copiilor online vizează progresul din domeniul educației, justiției și recomandările de auto-reglementare pentru furnizorii de servicii Internet. Totodată, restanțele înregistrate vizează unele aspecte-cheie, fără implementarea cărora nu poate fi asigurată o abordare complexă și sistematică a siguranței online la nivel de politici:

- Lipsesc unele mecanisme de raportare a conținutului ilegal online, motiv pentru care este imposibil de a semnala despre existența acestor

conținuturi ilegale online și de a solicita eliminarea lor, după modelul serviciilor Hotline² din întreaga lume;

- Unica platformă web www.siguronline.md de consiliere și informare despre siguranța online este gestionată de o organizație neguvernamentală și nu au fost stabilite parteneriate oficiale între MAI, MECC, MSMPS și La Strada Moldova, care a creat și gestionează portalul www.siguronline.md;
- Nu a fost dezvoltată și consolidată expertiza conținutului online ilegal și dăunător, iar Agenția pentru Protecția Moralității continuă să realizeze expertiza conținutului ilegal bazându-se doar pe prevederile Legii nr. 30 din 07.03.2013;
- Nu a fost actualizat cadrul legal la prevederile Convenției de la Lanzarote și ale Convenției de la Budapesta, angajament asumat de către RM odată cu ratificarea acestor Convenții;
- Lipsesc date statistice calitative disponibile online, ce vizează criminalitatea informatică cu implicarea copiilor și adolescenților, ceea ce creează impedimente în estimarea complexității și ponderii abuzurilor față de copii în mediul online.

Deși despre siguranța online s-a discutat mai mult în ultimii trei ani, studiile naționale indică despre faptul că copiii utilizează Internetul mai mult, comunică

și socializează mai mult, fiind expuși riscurilor de contact și conduită în mediul virtual (hărțuire online, sexting, abuz sexual, etc.). Cele mai problematice situații cu care se confruntă copiii online vizează relaționarea și comunicarea online, în special cu persoane necunoscute, după cum urmează:

- 16,3% dintre copii au accesat involuntar imagini sau video cu caracter sexual;
- 8,1% dintre copii au fost încurajați să expedieze fotografii sau video cu părți intime ale corpului;
- 14,8% dintre copii au primit mesaje cu caracter sexual în mediul online;
- 10% dintre copiii care au transmis poze persoanelor necunoscute au primit propuneri indecente de la persoanele cunoscute pe Internet.

Multiplele riscuri la care se supun copiii în mediul online se află în strânsă legătură cu nivelul minim de implicare a părinților în educația despre siguranța online, abordarea sporadică și superficială a siguranței online în programul școlar, dar și cu o insuficientă informare a publicului larg despre riscurile online și serviciile de suport la care pot apela în caz de abuz online. Acest fapt indică despre necesitatea unor eforturi consolidate în promovarea siguranței online, care să stabilească măsuri de informare a cadrelor didactice, părinților și elevilor despre siguranța online, cu regularitate.

² <https://www.inhope.org/EN>

Pe plan internațional, statele din Uniunea Europeană (în continuare – UE) își elaborează politicile ce vizează siguranța online pornind de la cadrul stabilit de Strategia Europeană pentru un Internet mai bun pentru copii, Modelul național de răspuns pentru prevenirea și combaterea abuzului și exploatării sexuale online a copilului WeProtect, dar și un șir de recomandări ale unor instituții internaționale precum Uniunea Internațională a Telecomunicațiilor (în continuare – UIT), Consiliul Europei (în continuare – CoE), etc. Toate acestea stabilesc un cadru complex de măsuri menite să asigure informarea și sensibilizarea publicului larg despre riscurile în mediul virtual, educarea copiilor în școală despre siguranța online prin

integrarea subiectului în programul școlar, formarea cadrelor didactice, pe de-o parte, și elaborarea unor politici instituționale despre siguranța online, ajustarea cadrului legal național la standardele internaționale, pe de altă parte.

Abordările și recomandările internaționale pot servi ca linii directorii pentru RM în stabilirea dimensiunilor următoarelor politici în domeniul siguranței copiilor în mediul online. Acest studiu își propune să formuleze unele recomandări pentru următorul ciclu de politici, pentru a asigura o abordare comprehensivă a siguranței online, care să răspundă necesităților naționale, reieșind din principalele probleme identificate în acest domeniu.

Metodologia cercetării

Această cercetare își propune să susțină eforturile statului în acțiunile de protecție a copiilor în mediul online, în special față de riscul abuzului și exploatarei sexuale online, ținând cont de recomandările internaționale și regionale existente, precum și de practicile de succes din acest domeniu.

Obiectivele cercetării sunt:

- Identificarea riscurilor la care se expun copiii în mediul online și descrierea problematicii care necesită a fi soluționată prin documente de politici;
- Stabilirea cadrului de politici publice naționale care reglementează măsuri în domeniul siguranței copiilor în mediul online;
- Studierea recomandărilor și politicilor internaționale în domeniul protecției copiilor în mediul online;
- Elaborarea recomandărilor pentru îmbunătățirea răspunsului statului față de protecția copiilor în mediul online, în concordanță cu recomandările internaționale.

Sarcinile cercetării:

- Analiza tendințelor în modul de utilizare a internetului de către copii, riscurilor asociate și factorilor ce contribuie la dezvoltarea comportamentelor riscante;
- Studierea realizărilor și restanțelor în implementarea politicilor publice în domeniul siguranței online a copiilor;
- Identificarea lacunelor și provocărilor în implementarea politicilor ce vizează siguranța online a copiilor, în monitorizarea și coordonarea măsurilor în domeniu și stabilirea relevanței obiectivelor propuse în contextul actual;
- Analiza abordărilor naționale în documentele de politici publice naționale, tipul de acțiuni planificate, identificarea autorităților responsabile de implementarea acestora;
- Analiza modelelor de coordonare a măsurilor ce vizează siguranța copiilor online pe plan internațional și identificarea unor exemple de bune practici;

- Analiza priorităților setate la nivel internațional în domeniul siguranței copiilor online, a principalelor obiective și domenii de intervenție;
- Formularea propunerilor pentru îmbunătățirea răspunsului statului față de riscurile online la care se expun copiii, de ordin strategic și operațional, pentru a asigura o abordare comprehensivă și o viziune strategică consolidată în domeniu.
- Studierea cadrului de politici publice naționale în raport cu recomandările și politicile publice internaționale;
- Chestionarea online a specialiștilor din cadrul autorităților publice responsabile de implementarea acțiunilor în domeniul siguranței copiilor online;
- Desfășurarea interviurilor individuale semi-structurate cu reprezentanții instituțiilor naționale responsabile de implementarea politicilor în domeniul protecției copiilor în mediul online în RM.

Pentru atingerea scopului și sarcinilor, au fost utilizate următoarele metode de cercetare:



1.

**Copiii în mediul online:
tendențe și riscuri
asociate**

În RM, se remarcă tendința **creșterii numărului de utilizatori de Internet** de la an la an. Datele despre dezvoltarea comunicațiilor electronice în RM în anii 2018-2019 confirmă existența unui număr în creștere de abonați la serviciul de acces la Internet fix și Internet mobil³. Internetul a devenit mai accesibil pentru toată populația țării, inclusiv pentru copii.

cu persoane pe care le cunosc ori își fac prieteni noi, postează diverse fotografii sau video⁴. În ultimii 5 ani, am atestat următoarele tendințe în modul în care copiii utilizează Internetul⁵:

- A crescut consumul de Internet în rândul copiilor de 12-13 ani;
- Copiii comunică și socializează mai mult online;

Numărul abonaților la serviciul de acces la Internet

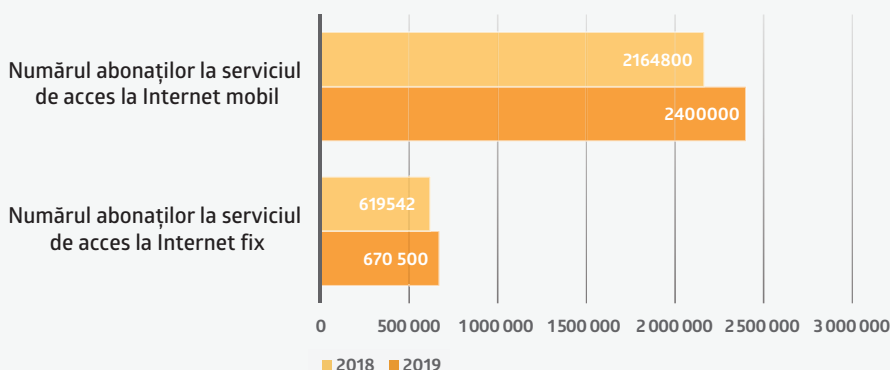


Diagrama nr. 1

„Numărul abonaților la serviciul de acces la Internet”, Sursa: Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (în continuare – ANRCETI)

Utilizarea activă a Internetului de către copii le oferă varii oportunități, dar îi expune și numeroaselor riscuri pentru integritatea fizică, emoțională sau sexuală. Copiii accesează Internetul pentru a socializa și comunica cu prietenii, pentru a găsi informații și a-și face temele pentru acasă, pentru a viziona filme sau pentru jocuri online. De obicei, copiii comunică pe rețele de socializare

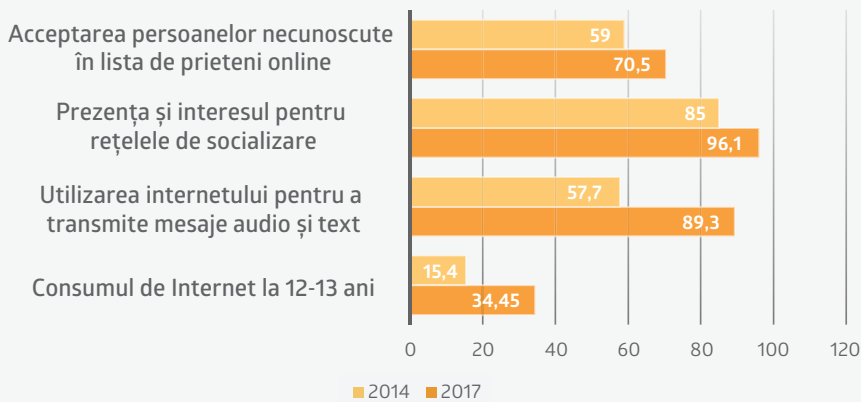
- Mai mulți copii sunt prezenți pe rețelele de socializare de la o vârstă mai mică de 10 ani (deși, în majoritatea cazurilor, vârsta minimă admisibilă este de 13 ani);
- Mai mulți copii și-au făcut prieteni noi în mediul online, persoane pe care nu le cunosc în realitate.

³ https://www.anrceti.md/files/filefield/Anuar%20statistic%202019_22aprilie_2020.pdf

⁴ http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet_final.pdf

⁵ Ibidem

Tendențe în modul de utilizare a Internetului de către copii

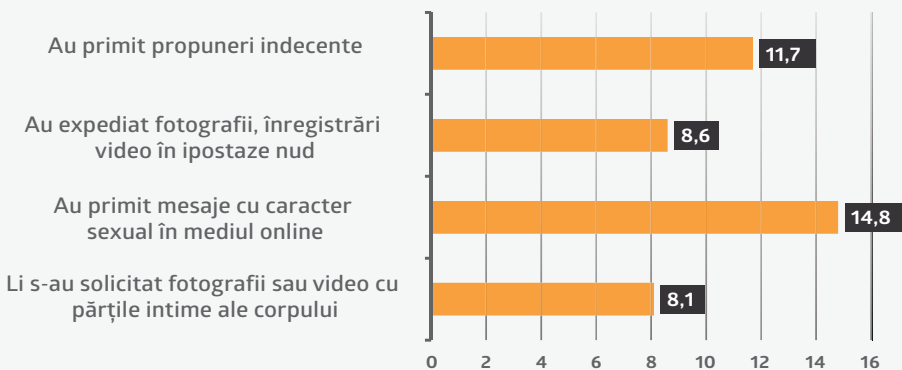


„Tendențe în modul de utilizare a Internetului de către copii”, Sursa: La Strada Moldova (Studiul privind siguranța copiilor online în Republica Moldova”, ediția a II-a, 2014 și Studiul privind siguranța copiilor pe Internet, 2017).

Acțiunile copiilor în mediul online îi expun numeroaselor **riscuri de contact** ce presupun interacțiunea directă a copilului cu un adult, care e inițiată și domina-

tă de către acesta. Din această categorie e riscul abuzului sexual online, despre care indică următoarele experiențe ale copiilor⁶:

Experiențele copiilor ce îi expun riscului de abuz sexual online



„Experiențele copiilor care se expun riscului de abuz sexual online”, Sursa: Siguranța copiilor pe Internet, 2017, La Strada Moldova.

⁶ http://lastrada.md/files/resources/3/Siguranța_copiilor_pe_Internet_final.pdf

- Expedierea de către copil a unor fotografii sau video cu părți intime ale corpului său;
- Recepționarea de mesaje cu caracter sexual în mediul online;
- Transmiterea de fotografii intime persoanelor necunoscute;
- Recepționarea unor propuneri indecente online.

Unul dintre factorii care **sporesc vulnerabilitatea copiilor față de riscul abuzului sexual online** este percepția eronată a adolescenților despre relațiile de iubire online. Mai mult de 50% dintre adolescenții de 14-15 ani din RM consideră că este normal să expediezi fotografii intime persoanei cu care ești în relație⁷. Chiar dacă copilul cunoaște acea persoană în realitate, expediind fotografii intime pierde orice control și poate ajunge în situații de hărțuire sau șantaj sexual. Riscul e mult mai mare dacă copilul e în relație cu o persoană cunoscută online, întrucât în spatele monitorului poate fi oricine. După expedierea fotografiilor sau video intime, probabilitatea ca să i se solicite și alte materiale sau să fie implicat și în alt tip de acțiuni cu caracter sexual online sau offline este foarte mare.

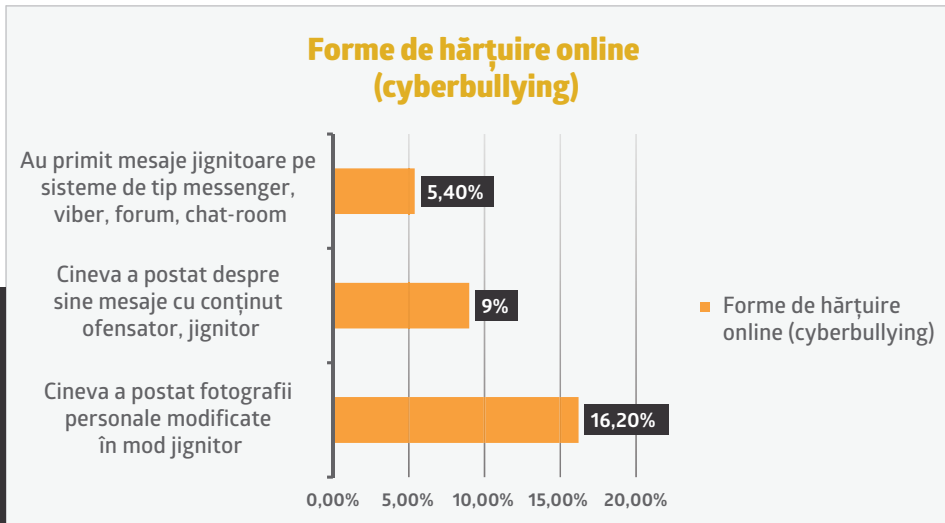
Fiind receptori ai informației distribuite în masă de către alte persoane, copiii din RM sunt expuși **riscurilor de conținut**. Copiii pot accesa conținuturi ce promovează violență sau pornografie, conținut ce nu-i potrivit vârstei lor, cu impact negativ asupra dezvoltării lor psiho-emoționale. Statisticile naționale indică despre faptul că 16,3% dintre copiii de 12-15 ani au accesat involuntar un video sau unele imagini cu caracter sexual în timp ce navigau pe Internet și căutau altceva. Cu astfel de situații s-au confruntat mai des adolescenții de 15 ani (aproximativ 29,7% din numărul total de copii), riscul fiind mai redus la categoriile mai mici de vârstă (7,4% din numărul total de copii)⁸.

Riscurile de conduită se referă la situațiile dintre semeni (peer-to-peer), atunci când copilul inițiază sau provoacă o anumită situație, având rolul de „agresor” online. Hărțuirea online este unul dintre cele mai des întâlnite riscuri de conduită. Un studiu național privind fenomenul bullyingului în RM indică despre faptul că 70,8% dintre elevii din țară s-au confruntat cu o situație de bullying, iar 28,9% dintre aceștia au trecut prin experiența bullyingului manifestat și în mediul online⁹. Interacțiunile online dintre semeni, în care copiii sunt jigniți, agresați verbal sau înjosiți în alt mod, se manifestă diferit:

⁷ http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet_final.pdf

⁸ Ibidem

⁹ <https://www.unicef.org/moldova/media/3146/file>



„Forme de hărțuire online (cyberbullying)”, Sursa: Siguranța copiilor pe Internet, 2017, La Strada Moldova.

Comportamentele riscante online nu întotdeauna evoluează într-un abuz, însă, cu certitudine, influențează nivelul de vulnerabilitate al copiilor. Amploarea abuzului sexual online nu poate fi estimată, întrucât copiii nu semnalează despre abuz. **21,3% dintre adolescenți nu discută cu nimeni despre problemele pe care le au în mediul online, preferând să găsească singuri soluții**¹⁰. În cazurile de abuz sexual online ce vizează intimitatea, sexualitatea copilului, din motiv că acestea sunt subiecte tabu în familie și societate, probabilitatea ca aceste cazuri să fie raportate este și mai mică.

Despre acest fapt indică și datele oficiale despre numărul de cazuri de abuz sexual online investigate de organele de poliție și care sunt mult mai mici com-

parativ cu datele despre vulnerabilitatea copilului online. În anul 2019, Inspectoratul General al Poliției (în continuare IGP) a înregistrat și investigat 49 de cauze penale ce reprezintă abuz sexual sau exploatare sexuală online a minorilor (4 infracțiuni de ademenire a minorilor în scopuri sexuale – art. 175/1 CP RM; 5 infracțiuni de trafic de copii în scop de exploatare sexuală online – art. 206 CP RM; 39 de infracțiuni de pornografie infantilă – art. 208/1 CP RM; 1 infracțiune de recurgere la prostituția practică de un minor – art. 208/2 CP RM)¹¹.

Totodată, în anul 2019, www.siguronline.md - serviciu de consiliere online pentru copiii victime ale abuzului și exploatării sexuale online, a înregistrat 29 de cazuri de abuz sexual online¹². Doar

¹⁰ http://lastrada.md/files/resources/3/Siguranta_copiiilor_pe_Internet__final.pdf

¹¹ Conform datelor furnizate de Procuratura Generală.

¹² http://lastrada.md/pic/uploaded/ffFactSheet%20siguronline%202019_FINAL.pdf

50% dintre acestea au fost ulterior referite organelor de drept, din motiv că, în celelalte cazuri, copiii au refuzat colaborarea cu organele de poliție, fiindu-le frică de reacțiile părinților¹³. Totodată, în primul semestru al anului 2020, pe www.siguronline.md au fost raportate 36 de cazuri de abuz sexual online. Cifrele sunt de 3 ori mai mari comparativ cu perioada similară a anului trecut, ceea ce indică despre tendința în creștere a numărului de cazuri înregistrate¹⁴.

Identificarea cazurilor de abuz sexual online față de copii este o provocare globală, nu doar pentru RM. Materialele ce conțin abuzuri sexuale ale copiilor sunt tot mai accesibile, iar resursele online care oferă hosting pentru aceste materiale sunt lansate și accesate mai ușor decât sunt identificate și blocate. Amploarea, severitatea și complexitatea exploatării și abuzului sexual online al copiilor evoluează mai rapid decât măsurile de combatere a acestor practici nefaste. Între 2014 și 2018, numărul de URL-uri cu materiale ce reprezintă abuzuri sexuale ale copiilor, blocate pe parcursul unui an, s-au triplat - de la 31 226 la 105 047 în 2018¹⁵.

Totodată, în 2019 Centrul Național pentru Copiii Dispăruți și Exploațați din SUA (National Center for Missing & Exploited Children, în continuare - *NCMEC*) a în-

registrat **10516 materiale de abuz sexual al copilului încărcate online din RM.**

Comparativ cu indicatorii din alte state: în Austria au fost încărcate și distribuite 10216 materiale, în Elveția - 8567 materiale, în Norvegia - 8031 materiale, în Slovacia - 6769 materiale, în Slovenia - 6890 materiale. Deși aceste date nu semnaleză în mod obligatoriu despre faptul că 10516 materiale reprezintă copiii din RM, cert este faptul că în RM există un interes sporit al abuzatorilor sexuali pentru acest tip de conținut.

Așadar, deși numărul de cauze penale ce reprezintă abuz sexual și exploatare sexuală online a minorilor, investigate în anul 2019, este relativ mic (49 de cauze penale), datele despre comportamentele riscante ale copiilor în mediul online și experiențele negative ale copiilor în mediul virtual¹⁶ semnaleză despre **un număr mult mai mare de cazuri neidentificate**. Totodată, datele despre numărul de materiale ce reprezintă exploatare sexuală online a minorilor, încărcate din RM în anul 2019 (10516 materiale¹⁷), la fel, indică despre faptul că există cerere și interes pentru conținut sexual ce reprezintă copii, **ceea ce îi face pe copii și mai vulnerabili în interacțiunile online cu persoanele necunoscute**.

Cu toate acestea, nivelul de informare și pregătire a copilului despre cum poate

¹³ http://lastrada.md/pic/uploaded/EAC%20Factsheet%20sem%202%20_%202019.pdf

¹⁴ http://lastrada.md/pic/uploaded/Siguronline%2520factsheet_1%2520sem_2020.pdf

¹⁵ <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+++Global+Threat+Assessment.pdf>

¹⁶ În baza studiului „Siguranța copiilor pe Internet”, La Strada, 2017.

¹⁷ Conform datelor NCMEC.

face față acestor riscuri este minim. Doar 30% dintre copiii de 12-15 ani au aflat despre siguranța online de la profesori, în școală, iar ceilalți au aflat despre acest subiect de la părinți, prieteni sau specialiști¹⁸. Chiar și în aceste cazuri, copiii **li s-a vorbit mai mult despre aspecte de securitate online, de securizare a parolilor sau protejare a informației în mediul virtual**. Despre relații și comunicare intimă în mediul virtual nu s-a discutat, ceea ce indică despre faptul că, atât acasă, cât și la școală sunt abordate superficial aspectele ce vizează comportamentele sigure în mediul virtual. Iar, în condițiile în care tehnologiile sunt integrate tot mai mult în procesul educațional, ca parte a procesului de digitalizare a educației, abordarea acestor aspecte este absolut justificată și necesară.

Un alt factor ce contribuie la vulnerabilitatea copiilor în mediul online **este implicarea minimă a părinților în educația despre siguranța online**. Părinții nu sunt informați despre potențiale riscuri și metode de mediere a acestora, nu cunosc cum să dezvolte abilități de gândire critică a copiilor în mediul online și apelează la metode restrictive, de limitare sau chiar interzicere a utilizării tehnologiilor. La fel, „conflictul dintre generații” accentuează lipsa de comunicare și înțelegere în relația părinte – copil. Părinții nu percep siguranța online ca o dimensiune obligatorie în educația copilului. Mai mult decât atât, părinții pot considera, în mod greșit, că copilul lor cunoaște suficient de multe despre Internet și

se pot descurca singuri. La fel, migrația masivă a părinților peste hotare și faptul că mulți copii au rămas acasă în grija bunelor, care practic nu au abilități de utilizare a tehnologiilor digitale, contribuie în egală măsură la informarea deficientă a copiilor despre siguranța online.

Impactul abuzului online asupra copilului are consecințe pe termen lung. O experiență traumatizantă online poate fi asociată cu probleme emoționale, cu un nivel redus de eficacitate, probleme de somn, asumare nejustificată de riscuri, consum de tabac, probleme de alimentație, dar și alte probleme de sănătate. Mai mult decât atât, distribuirea imaginilor sau secvențelor video ce reprezintă copilul în mediul virtual, posibilitatea de a viziona materialele de pe Internet de mii de ori victimizează repetat copilul și, inevitabil, amplifică consecințele negative ale abuzului.

Pe termen lung, abuzul din copilărie determină un nivel redus de eficacitate în viața adultă, rata minimă de menținere la același loc de muncă, nivel redus de interes și implicare în viața socială, etc. **Din punct de vedere economic**, fenomenul implică costuri pentru reabilitare și reintegrare în societate a copilului/adultului care a suferit de abuz în copilărie, cheltuieli pentru dezvoltarea unor programe de reabilitare corespunzătoare, costuri pentru diminuarea consecințelor negative indirecte ale abuzului (șomaj, probleme de sănătate, rata înaltă de criminalitate, etc.).

¹⁸ http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet_final.pdf

Impactul abuzului online asupra societății se manifestă printr-un nivel sporit de anxietate în raport cu agresorii sexuali din comunitate. Modul cum sunt abordate în public aceste cazuri va influența nivelul de înțelegere și răspunsul emoțional față de fenomen. Deși impactul acestor cazuri asupra fiecărei persoane din societate poate fi mic, impactul colectiv asupra siguranței copilului online este considerabil. Părinții ar putea simți că nu există nicio modalitate de a-și proteja copilul online, decât prin interzicerea accesării Internetului. Pe termen lung, aceste restricții pot dimi-

nua nivelul de reziliență al copiilor față de abuz. Interzicerea utilizării tehnologiilor îi face mai curioși, mai puțin pregătiți să identifice situațiile cu potențial riscant și, respectiv, mai vulnerabili la abuz.

Totodată, lipsa de cunoștințe și nivelul redus de sensibilizare despre abuzul sexual online contribuie la blamarea socială a copilului. La rândul lor, asemenea reacții amplifică consecințele psiho-emoționale ale abuzului, acutizează sentimentul de vină și rușine, copilul considerându-se responsabil pentru abuzul care a fost comis asupra sa.

Principalele constatări:

1. Se atestă un nivel înalt de vulnerabilitate a copiilor în mediul online determinat de lipsa unei educații orientate spre dezvoltarea abilităților de gândire critică și nivelul minim de implicare a părinților și școlii;
2. Există un nivel sporit al comportamentelor riscante ale copiilor în mediul online, cu potențial dăunător;
3. Cele mai problematice situații cu care se confruntă copiii online vizează relaționarea și comunicarea online, în special cu persoane necunoscute;
4. Părinții dau dovadă de un nivel redus de cunoștințe și sunt slab informați despre practicile pozitive de mediere parentală;
5. Conflictul dintre generații, frica de a fi blamați sau învinovați pentru cele întâmplate diminuează din probabilitatea ca un copil să raporteze direct un caz de abuz online.



2.

**Rolul statului în
diminuarea riscurilor
cărora se expun
copiii online**

2.1 Cartografierea politicilor naționale în domeniu

În ultimii ani, subiectul protecției copiilor în mediul online a ajuns în vizorul factorilor de decizie, fapt care a impulsivat aprobarea mai multor documente de politici în domeniu.

Strategia securității informaționale a Republicii Moldova pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia¹⁹

Strategia a fost elaborată în baza Concepției securității informaționale a Republicii Moldova, aprobată prin Legea nr. 299/2017²⁰. Aceasta a fost determinată de necesitatea protejării intereselor statului, ale societății și ale persoanei, obiectivelor vitale și de importanță strategică pentru securitatea națională, de necesitatea asigurării protecției informației atribuite la secret de stat, precum și de necesitatea prevenirii și combaterii criminalității informatice.

Scopul Concepției este asigurarea protecției drepturilor și libertăților fundamentale în spațiul informațional, democrației și statului de drept, iar obiectivele de bază în domeniul asigurării securității informaționale vizează, în linii generale, dezvoltarea capacităților de reacție, monitorizarea nivelului securității informaționale sau spațiului informațional, crearea unui sistem de comunicare

și evaluare a amenințărilor la adresa securității informaționale și multe alte aspecte orientate spre îmbunătățirea răspunsului statului la riscurile pentru securitatea informațională.

În textul Strategiei, la capitolul III, au fost constatate un șir de bariere și lacune de ordin normativ în domeniul prevenirii și combaterii criminalității informatice. Acestea vizează lipsa incriminării infracțiunii penale de violare a secretului corespondenței, lipsa procedurii de „percheziție informatică”, prevăzută de Convenția de la Budapesta, imposibilitatea efectuării măsurilor speciale de investigații necesare la documentarea infracțiunilor informatice, lipsa măsurii speciale de investigații de interceptare a datelor informatice, precum și alte măsuri ce vizează criminalitatea informatică. În acest capitol e menționată și problema lipsei incriminării obținerii accesului cu bună știință, prin intermediul tehnologiilor informaționale și a comunicațiilor, la pornografia infantilă (prevedere prevăzută de Convenția de la Lanzarote).

Reieșind din aceasta, Obiectivul 7 din Strategie este „Protecția copiilor de orice formă de abuz în spațiul online”, iar în acest scop au fost prevăzute următoarele acțiuni:

1. Combaterea fenomenului de pornografie infantilă pe Internet;

¹⁹ Hotărârea Guvernului nr. 257 din 22.11.2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia, publicat la 18.01.2019 în Monitorul Oficial nr. 13-21, art. 80.

²⁰ Legea nr. 299 din 21 decembrie 2017 privind aprobarea Concepției securității informaționale a Republicii Moldova.

2. Combaterea fenomenelor de ade-menire (grooming) și hărțuire sexuală a copiilor prin intermediul Internetului;
3. Promovarea unui Internet mai sigur pentru copii prin intermediul consilierilor online și încurajarea raportărilor prin proiecte informaționale specializate.

Reflectarea problemelor ce vizează pornografia infantilă în contextul descrierii problemelor din domeniul prevenirii și combaterii criminalității informatice nu este justificată legal. Art. 208¹ CP e prevăzut la Capitolul VII „Infrațiuni contra familiei și minorilor”, iar infracțiunile informatice sunt reglementate în Capitolul XI „Infrațiuni informatice și infracțiuni în domeniul telecomunicațiilor”. Chiar și în Convenția de la Budapesta, măsurile referitoare la pornografia infantilă sunt incluse în Titlul nr. 3 „Infrațiuni referitoare la conținut”, fiind reglementate separat de Infrațiunile împotriva confidențialității, integrității și disponibilității datelor și sistemelor informatice (Titlul 1), precum și de Infrațiunile informatice (Titlul 2).

Reglementarea măsurilor ce vizează combaterea pornografiei infantile în politici din domeniul securității informaționale e ancorată în prevederile Convenției de la Budapesta, însă o astfel de abordare este epuizată, mai ales în con-

textul evoluțiilor pe plan internațional ce vizează protecția copilului față de abuzul și exploatarea sexuală online. Convenția de la Budapesta a fost aprobată în anul 2001, fiind primul tratat internațional ce incrimina infracțiunile de pornografie infantilă. La acea etapă, contextul indica despre o evoluție de amploare a tehnologiilor, ce favoriza dezvoltarea fenomenului infracțional în mediul online. Reglementarea pornografiei infantile în Convenția de la Budapesta a creat pârghii de combatere a exploatării sexuale online a copiilor²¹.

Ulterior, în 2007, abuzul sexual și exploatarea sexuală a copiilor, inclusiv în mediul virtual, au fost reflectate și în Convenția Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale și abuzurilor sexuale (Convenția de la Lanzarote), ca una dintre formele de exploatare sexuală a copiilor. Astfel, odată cu aprobarea Convenției de la Lanzarote, infracțiunea de pornografie infantilă a început a fi percepută dintr-o altă perspectivă – ca infracțiune ce atentează la integritatea sexuală a copiilor, dar nu ca o infracțiune din domeniul criminalității informatice.

Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 și Planul de acțiuni privind implementarea acestuia²²

²¹ Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, adopted by the Cybercrime Convention Committee, Working group on other forms of online violence, especially against women and children.

²² Hotărârea Guvernului nr. 811 din 29.11.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, publicat la 13.11.2015 în Monitorul Oficial nr. 306-310, art. 905.

Acest Program are drept scop crearea unui sistem de management al securității cibernetice a RM, prin securizarea serviciilor societății informaționale, contribuind astfel la dezvoltarea unei economii bazate pe cunoaștere, ceea ce, la rândul său, va stimula creșterea gradului de competitivitate economică și de coeziune socială și va asigura crearea de noi locuri de muncă.

La fel, conform pct. 14 din acest Program, securitatea cibernetică este o „stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri proactive și reactive prin care în spațiul cibernetic se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a sistemelor și resurselor informaționale, a serviciilor publice și private”. Măsurile proactive și reactive includ politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protecție a infrastructurilor cibernetice, managementul identității, managementul consecințelor.

Acest Program, la fel, include infracțiunea de pornografie infantilă (art. 208¹ CP RM) în categoria de infracțiune informatică, făcând referire în acest sens la prevederile Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001.

Planul de acțiuni al acestui Program, la Obiectul 4 „Prevenirea și combaterea criminalității informatice”, pct. 4.5 stabilește „Ajustarea legislației naționale la prevederile Convenției Consiliului Europei pentru protecția copiilor împotriva exploatarea și abuzurilor sexuale și ale Protocolului adițional la Convenție (Lanzarote, 25 octombrie 2007)”.

Acest document de politici a creat pârghii pentru ajustarea cadrului legal național la prevederile Convenției de la Lanzarote. Deși subiectul a fost inclus în platforma securității cibernetice, domeniu care protejează alte valori decât protecția integrității sexuale a copiilor în mediul virtual, acest fapt a stimulat primele acțiuni în vederea ajustării cadrului juridic național la standardele internaționale. La fel, acest document de politici a servit ca bază pentru eforturile inițiate de Ministerul Afacerilor Interne (în continuare – MAI) și La Strada Moldova în vederea creării unui mecanism național de monitorizare a implementării Convenției de la Lanzarote. Însă, în ultimă instanță, niciuna dintre acțiunile inițiate nu a fost implementată. Proiectul de lege pentru modificarea și completarea unor acte legislative, înregistrat în Parlamentul RM cu nr. 161 din 13.04.2017, nu a fost examinat în prima lectură în cadrul ședinței parlamentare, fiind declarat nul și retras. Mecanismul național de monitorizare a implementării Convenției Lanzarote nu a fost aprobat din motiv că MAI și Cancelaria de Stat nu au ajuns la un numitor comun privind organul principal care ur-

mează să monitorizeze această Convenție²³.

Planul de acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020²⁴

Acest Plan de acțiuni a fost elaborat în contextul implementării prevederilor Strategiei pentru protecția copilului pe anii 2014-2020 și Programului de activitate al Guvernului Republicii Moldova 2016-2018, precum și pentru coordonarea și stimularea eforturilor tuturor părților interesate în creșterea nivelului de siguranță pe Internet a copiilor și adolescenților.

Acest Plan de acțiuni are următoarele priorități:

1. Reducerea conținutului ilegal din Internet și abordarea comportamentului cu impact negativ în mediul online;
2. Promovarea unui mediu digital mai sigur pentru copii și adolescenți prin colaborarea tuturor părților implicate;
3. Sensibilizarea și informarea părților aflate în contact direct cu copiii despre riscurile mediului online și formularea recomandărilor privind navigarea în siguranță pe Internet;
4. Elaborarea statisticilor și promovarea cercetărilor privind siguranța online a copiilor și adolescenților.

Acesta a fost primul document de politici tematic care a reglementat acțiuni de promovare a siguranței copiilor online. Astfel, un șir de autorități și instituții publice, care până în 2017 nu aveau responsabilități în domeniul siguranței copiilor online, au fost implicate în acțiuni de promovare a siguranței online. Prin acest Plan de Acțiuni s-a pus baza primelor eforturi comune de protecție a copiilor față de pericolele online.

Planul de acțiuni pentru anii 2016-2020 privind implementarea Strategiei pentru protecția copilului pe anii 2014-2020²⁵

Unul dintre obiectivele acestui Plan de acțiuni este „Prevenirea și combaterea violenței, neglijării și exploatării copiilor, promovarea practicilor nonviolente în creșterea și educarea copiilor” (Obiectivul general 2). În acest context, au fost planificate următoarele acțiuni ce vizează siguranța online a copiilor:

Acțiunea 2.1.16 „Dezvoltarea și promovarea serviciilor de informare și prevenire în domeniul siguranței online a copiilor, prestate prin intermediul unei platforme online (oportunități de raportare a conținutului cu material de pornografie infantilă, abilitarea părinților privind securizarea accesului la informații de către copii).”

Acțiunea 2.1.18 „Elaborarea unui set minim de reguli obligatorii pentru furnizo-

²³ http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf

²⁴ Hotărârea Guvernului nr. 212 din 5 aprilie 2017 pentru aprobarea Planului de acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020.

²⁵ https://gov.md/sites/default/files/document/attachments/intr05_75.pdf

rii de servicii de internet și a unui set de recomandări privind mecanismele de autoreglementare privind limitarea accesului la spațiul informațional cu conținut cu potențial impact negativ asupra psihicului copilului prin opțiunea „control al părinților.”

Acțiunea 2.1.22 „Organizarea Campaniilor naționale de sensibilizare în domeniul prevenirii violenței față de copii și privind utilizarea sigură și responsabilă a internetului, adresate copiilor, părinților și publicului general.”

Acțiunea 2.2.18 „Organizarea activităților de informare în cadrul lunarului Securitatea cibernetică privind siguranța copiilor în mediul online.”

Acțiunea 2.2.19 „Elaborarea și instituționalizarea curriculumului privind prevenirea și combaterea infracțiunilor cu caracter sexual comise împotriva copilului cu utilizarea tehnologiilor informaționale, destinat reprezentanților organelor de drept și justiție.”

Aceste acțiuni au servit ca bază pentru elaborarea Planului de Acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020, toate acțiunile fiind transpuse și detaliate într-un document de politici tematic.

Strategia Națională de dezvoltare a societății informaționale „Moldova digitală 2020” și Planul de acțiuni pentru implementarea Strategiei²⁶

Strategia națională de dezvoltare a societății informaționale „Moldova digitală 2020” are obiectivul general de a crea condiții favorabile pentru dezvoltarea și utilizarea largă a potențialului TIC de către instituțiile publice, mediul de afaceri și cetățeni, pentru a-și atinge țintele economice, sociale și culturale în beneficiul tuturor. Strategia se axează pe trei linii principale de implicație politică:

1. Extinderea accesului și conectivității cu promovarea concurenței rețelelor și serviciilor de acces în bandă largă;
2. Stimularea creării/dezvoltării de conținut digital și servicii electronice;
3. Fortificarea capacităților de utilizare a beneficiilor oferite de TIC.

În această Strategie, o singură acțiune vizează domeniul cercetat:

Pilonul II, Obiectivul general: Crearea condițiilor propice pentru elaborarea și valorificarea conținutului național digital și digitizarea conținutului național existent, precum și implementarea și utilizarea serviciilor electronice.

Acțiunea 4.14. Elaborarea și diseminarea recomandărilor privind accesarea conținutului digital în spațiul Internet pentru copii și pentru maturi, inclusiv prin prisma pericolelor existente.

²⁶ Hotărârea Guvernului nr. 857 din 31 octombrie 2013 privind aprobarea Strategiei Naționale de dezvoltare a societății informaționale „Moldova digitală 2020”.

Așadar, documentele de politici ce reglementează acțiuni menite să promoveze siguranța copiilor online au o abordare

destul de complexă. Mai multe detalii sunt indicate în Tabelul nr. 1.

Domenii reglementate de documentele de politici naționale

| | | | | | |
|--------------------------------|--|---|--|---|--|
| Docu- mentul de politici | Hotărârea Gu- vernului nr. 857 din 31 octom- brie 2013 | Hotărârea Guvernului Nr. 835 din 04.07.2016 | Hotărârea Guvernului nr. 212 din 5 aprilie 2017 | Hotărârea Guvernului nr. 811 din 29.11.2015 | Hotărârea Guvernului nr. 257 din 22.11.2018 |
| Domeniul | Dezvoltarea societății informaționa- le - Moldova Digitală | Protecția copilului | Promovarea siguranței copiilor și adolescenți- lor online | Securitate cibernetică | Securitate informațio- nală |
| Dimensi- unea | Accesarea con- ținutului sigur | Informare și prevenire Raportarea pornografiei infantile Măsuri de auto-regle- mentare pentru furnizorii de servicii Internet Dezvoltarea de capacități a repre- zentanților organelor de drept și justiție | Reducerea conținutului ilegal din Internet Promovarea unui mediu digital mai sigur Sensibi- lizarea și informarea părților aflate în contact direct cu copiii Elaborarea statisticilor și promovarea cercetărilor privind sigu- ranța online a copiilor și adolescen- ților. | Ajustarea cadrelor legal în domeniul abuzului și exploatării sexuale | Combaterea fenomenului de pornogra- fie infantilă pe Internet; Combaterea fenomenelor de ademenire (grooming) și hărțuire sexuală a copiilor prin intermediul Internetului; Promovarea unui Internet mai sigur pentru copii prin interme- diul consilie- rilor online și încurajarea raportărilor prin proiecte informațio- nale speciali- zate. |

Tabelul nr. 1

Principalele constatări:

Documentele de politici ce reglementează acțiuni menite să promoveze siguranța copiilor online au o abordare destul de complexă, fiind planificate acțiuni ce vizează diferite domenii de competență, începând cu promovarea siguranței copiilor online, acțiuni menite să contribuie la reducerea conținutului ilegal din Internet, până la acțiuni de actualizare a cadrului legal în domeniul abuzului sexual și exploatării sexuale, facilitate de utilizarea TIC.

2.2. Realizări și restanțe în implementarea politicilor

Principalele realizări

Una dintre cele mai importante realizări din ultimii ani, ca urmare a implementării politicilor de promovare a siguranței copiilor online, este **sensibilizarea și informarea cadrelor didactice, elevilor și părinților despre utilizarea tehnologiilor online** într-un mod mai sigur și responsabil, despre riscurile pe Internet și modalitățile de a le face față. Anual, în contextul Zilei Siguranței Copiilor Online și Lunii securității informatice, în instituțiile de învățământ din țară s-au organizat, pentru părinți, elevi și profesori, diverse activități de informare despre riscurile online, comportamentele riscante și modalitățile de protecție pe Internet²⁷.

În domeniul educației, se remarcă integrarea mai multor subiecte ce vizează siguranța online în curriculum. Deși o astfel de actualizare nu a fost planificată în documentele de politici publice, evoluțiile pe acest segment au determinat necesitatea dezvoltării

unor programe educaționale menite să contribuie la alfabetizarea digitală a copiilor, precum este „Educație pentru media” – disciplină opțională pentru ciclul gimnazial și liceal- și „Educația digitală” - disciplină obligatorie pentru ciclul primar.

O altă realizare importantă în domeniul prevenirii riscurilor de conținut pentru copii este aprobarea **Recomandării privind autoreglementarea serviciului de filtrare a conținutului din Internet cu impact negativ asupra copiilor**, prestat de către furnizorii de rețele sau servicii de comunicații electronice. Astfel, potrivit datelor statistice pentru anul 2019, din cei 97 de furnizori de servicii de acces la Internet, o mare parte au pus la dispoziția utilizatorilor finali instrumente disponibile în vederea filtrării conținutului cu impact negativ asupra copiilor. Cu toate acestea, o bună parte dintre furnizori au raportat lipsa de adresări de la utilizatorii finali (părinți, tutori, educatori, etc.) privind punerea la dispoziția lor a serviciilor de filtrare a conținutului. Doar 3 furnizori au raportat despre prestarea serviciului de fapt²⁸.

²⁷ http://mei.gov.md/sites/default/files/raport_hg_212_pe_2019.pdf

²⁸ Ibidem

Cât privește domeniul de combatere a abuzurilor online față de copii, au fost elaborate **instrucțiuni metodice privind investigarea infracțiunilor sexuale online** comise împotriva copiilor și au fost organizate **instruiri pentru judecători, procurori privind metodele și tactica de investigare și urmărire a infracțiunilor comise împotriva copiilor, cu utilizarea tehnologiilor informaționale**. Despre desfășurarea acestor instruiri se menționează și în Informația privind implementarea Planului de acțiuni privind promovarea siguranței copiilor online, dar și în Raportul despre executarea, în semestrul II al anului 2019, a Programului național de securitate cibernetică a RM pentru anii 2016-2020²⁹. La fel, Procuratura Generală a raportat despre acțiunile întreprinse în vederea examinării legislației procesual-penale, măsurilor speciale de investigații, în raport cu prevederile documentelor internaționale, dar și despre realizarea unui studiu statistic al stării de fapt în domeniul investigării infracțiunilor de pornografie infantilă pentru anii 2013-2017 (conform Acțiunilor 4.6³⁰ și 4.7³¹ din Planul național de acțiuni privind implementarea Programului național de securitate cibernetică).

Principalele restanțe

- Nu au fost create mecanisme de raportare a conținutului ilegal din Internet (acțiunea 1.1, 1.2, 1.3 din PNA privind promovarea siguranței pe Internet a copiilor, responsabil - Agenția pentru Protecția Moralității și Ministerul Afacerilor Interne);
- Nu a fost creată o platformă web pentru informare și consiliere privind siguranța online, proceduri operaționale și procedura de referire la serviciile specializate de asistență și protecție, la organele de drept (acțiunea 2.1, 2.2, 2.3, 2.4 din PNA privind promovarea siguranței pe Internet a copiilor, responsabili - Institutul de Dezvoltare a Societății Informaționale, Ministerul Afacerilor Interne, Ministerul Sănătății, Muncii și Protecției Sociale și Ministerul Educației, Culturii și Cercetării);
- Nu a fost dezvoltată și consolidată expertiza conținutului ilegal și dăunător (acțiunea 4.6 din PNA privind promovarea siguranței pe Internet a copiilor, responsabil - Agenția pentru Protecția Moralității);
- Nu a fost realizată sistematizarea și analiza datelor statistice privind

²⁹ http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf

³⁰ Programul național de securitate cibernetică a RM, Acțiunea 4.6 „Efectuarea unui studiu pentru perfecționarea cadrului normativ în domeniul prevenirii și combaterii crimelor informatice”.

³¹ Programul național de securitate cibernetică a RM, Acțiunea 4.7 „Consolidarea în cadrul Procuraturii Generale, Serviciului de Informații și Securitate și Inspectoratului General al Poliției al Ministerului Afacerilor Interne a capacităților pentru prevenirea și combaterea criminalității informatice și, după caz, formularea unor propuneri de modificare a cadrului normativ și crearea unui laborator de testate și expertiză”.

criminalitatea informatică cu implicarea copiilor și adolescenților, nu au fost publicate date statistice sistematizate, nici rapoarte de analiză (acțiunea 12.1 din PNA privind promovarea siguranței pe Internet a copiilor – responsabil Ministerul Afacerilor Interne);

- Nu a fost creat un mecanism de monitorizare a implementării Convenției de la Lanzarote (acțiunea 4.5, Programul național de securitate cibernetică a RM pentru anii 2016-2020, responsabil MAI);
- Nu a fost ajustat cadrul legal la prevederile Convenției de la Budapesta în ceea ce vizează procedurile de investigație a infracțiunilor săvârșite cu utilizarea TIC (acțiunea 4.1, Programul național de securitate ciber-

netică a RM pentru anii 2016-2020 – responsabil MAI, SIS, PG);

- Nu a fost ajustat cadrul legal la prevederile Protocolului adițional la Convenția de la Budapesta, referitor la incriminarea actelor de natură rasistă, xenofobă săvârșite prin intermediul sistemelor informatice (acțiunea 3.1 din PNA privind promovarea siguranței pe Internet a copiilor – responsabil MAI);

Conform informației furnizate de reprezentantul MEI, urmare a restructurării și comasării ministerelor, au rămas puține resurse umane care puteau fi atrase în domeniu. Acest fapt a contribuit la implementarea cu dificultate a Planului de Acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților.

Principalele constatări:

Principalele realizări în domeniul siguranței copiilor online vizează progresul din domeniul educației, autoreglementarea în sectorul privat TIC și domeniul justiției. Totodată, restanțele înregistrate vizează unele aspecte-cheie, fără implementarea cărora nu poate fi asigurată o abordare complexă și sistematică a siguranței online la nivel de politici:

- Lipsesc unele mecanisme de raportare a conținutului ilegal online, ceea ce indică despre imposibilitatea de a semnaliza existența acestor conținuturi și de a solicita ștergerea lor, practică realizată de serviciile Hotline¹ din întreaga lume;
- Unica platforma web de consiliere și informare despre siguranța online disponibilă la moment, www.siguronline.md, este gestionată de o organizație neguvernamentală.
- Nu a fost dezvoltată și consolidată expertiza conținutului ilegal și dăunător online, ceea ce indică despre faptul că Agenția pentru Protecția

Moralității continuă să realizeze expertiza conținutului ilegal bazându-se doar pe prevederile Legii nr. 30 din 07.03.2013.

- Cadrul legal nu a fost ajustat la prevederile Convenției de la Lanzarote și ale Convenției de la Budapesta, angajamente asumate de către RM odată cu ratificarea acestor Convenții.
- Lipsesc date statistice calitative disponibile online despre criminalitatea informatică cu implicarea copiilor și adolescenților, ceea ce creează impedimente în estimarea complexității și ponderii abuzurilor față de copii în mediul online.

2.3. Mecanismul de coordonare a politicilor

Fiecare dintre documentele de politici ce reglementează acțiuni în domeniul pro-

tecției copiilor online are propriile mecanisme de coordonare, monitorizare și raportare a acțiunilor implementate, specificate în Tabelul nr. 2.

Autorități responsabile de coordonarea, monitorizarea și evaluarea politicilor în domeniu

| Documentul de politici | Autoritatea responsabilă de coordonare | Monitorizare și evaluare |
|--|--|--|
| Strategia securității informaționale a RM pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia | Conform HG nr. 257 din 22.11.2018, Serviciul Informații și Securitate | Conform HG nr. 257 din 22.11.2018, Serviciul Informații și Securitate - responsabil de monitorizare. Nu este specificată autoritatea responsabilă de evaluare. |
| Programul național de securitate cibernetică a RM pentru anii 2016-2020 și Planul de acțiuni privind implementarea acestuia | Conform HG nr. 811 din 19.10.2015, MTIC (în prezent – MEI) este responsabil de coordonarea Programului național de securitate cibernetică. | Conform HG nr. 811 din 19.10.2015, MTIC (în prezent – MEI) – responsabil de monitorizare. Nu este specificată autoritatea responsabilă de evaluare. |

Tabelul nr. 2

| | | |
|--|---|--|
| Planul de acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020 | Conform HG nr. 212 din 05.04.2017, MTIC (în prezent – MEI) este autoritatea responsabilă pentru controlul asupra executării, colectării informației despre acțiunile întreprinse de ministerele și instituțiile responsabile și prezentarea acestui raport Guvernului. | Nu este specificat. |
| Planul de acțiuni pentru anii 2016-2020 privind implementarea Strategiei pentru protecția copilului pe anii 2014-2020 | Conform HG nr. 434 din 10.06.2014, rolul de coordonare a implementării PNA e atribuit MMPSF (în prezent – MSMPS), care va crea în acest scop un grup de lucru constituit din reprezentanții autorităților, instituțiilor și organizațiilor relevante, implicate în procesul de implementare a Strategiei. | Conform HG nr. 434 din 10.06.2014, MMPSF este autoritatea responsabilă de monitorizare și evaluare. |
| Tabelul nr. 2 Strategia Națională de dezvoltare a societății informaționale „ Moldova digitală 2020 ” și Planul de acțiuni pentru implementarea Strategiei | În raportul de Evaluare intermediară a implementării Strategiei și Planului de acțiuni, e specificat că rolul de coordonare îl are Consiliul Național pentru Protecția Drepturilor Copilului. | Conform HG nr. 857 din 31 octombrie 2013, Consiliul e-Transformare, cu suportul tehnic asigurat de MTIC (în prezent MEI), este responsabil pentru monitorizarea și evaluarea implementării Strategiei. |
| | Conform HG nr. 857 din 31 octombrie 2013, MTIC (în prezent – MEI) este autoritatea responsabilă pentru implementarea Strategiei. | |

Existența mai multor documente de coordonare paralele determină deseori politici ce stabilesc măsuri în domeniul în practică raportarea aceluiași acțiuni siguranței online și unor mecanisme de pe diferite platforme.

Dublări în datele raportare

| Date raportate | Acțiunea planificată | Platforma de raportare a rezultatelor |
|--|--|---|
| Implicarea cadrelor didactice în activități de informare și sensibilizare a copiilor în cadrul „Lunii securității cibernetice”, zilei „Siguranța în Internet”; | Acțiunea 8.1. Promovarea subiectului privind mediul digital sigur în cadrul activităților extracurriculare, non-formale și informale pentru elevi și tineri; | Informația privind gradul de realizare, în anul 2019, a Planului de Acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020; |
| | Acțiunea 6.2 Completarea curriculumului de învățământ în domeniul securității cibernetice; | Raportul despre executarea, în semestrul II al anului 2019, a Programului național de securitate cibernetică a RM pentru anii 2016-2020 ² ; |
| | Acțiunea 2.1.22 Organizarea Campaniilor naționale de sensibilizare în domeniul prevenirii și violenței față de copii și privind utilizarea sigură și responsabilă a internetului, adresate copiilor, părinților și publicului general; | Raportul de implementare a Planului de Acțiuni pentru anii 2016-2020 privind implementarea Strategiei pentru protecția copilului pe anii 2014-2020; |
| Instrucțiuni metodice privind investigarea infracțiunilor sexuale online comise împotriva copiilor; | 1.2. Elaborarea și implementarea modulelor specializate de instruire în domeniul identificării, investigării și judecării infracțiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale; | Informația privind gradul de realizare, în anul 2019, a Planului de Acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020; |
| | 4.4. Elaborarea instrucțiunilor metodice cu privire la investigarea infracțiunilor cu caracter sexual săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale; | |

| | | |
|--|---|---|
| <p>Desfășurarea seminarelor cu tematica „Metodici și tactici de identificare, investigare și judecare a infrațiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale”</p> | <p>Acțiunea 4.2. Instruirea angajaților organelor de drept, specialiștilor certificați în domeniul securității cibernetice privind: a) depistarea, investigarea, urmărirea penală și judecarea infrațiunilor informatice; b) legătura dintre criminalitatea informatică, crima organizată, infrațiunile economice și alte categorii de infrațiuni.</p> | <p>Raportul despre executarea, în semestrul II al anului 2019, a Programului național de securitate cibernetică a RM pentru anii 2016-2020.</p> |
| | <p>4.3 Formarea profesională a reprezentanților organelor de drept și sistemului judecătoresc în domeniul identificării, investigării și judecării infrațiunilor săvârșite asupra copiilor cu utilizarea tehnologiilor informaționale.</p> | <p>Informația privind gradul de realizare, în anul 2019, a Planului de Acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020</p> |

Principalele constatări:

Mecanismele existente de coordonare nu sunt inter-conectate. Lipsește o unică entitate cu atribuții de coordonare a tuturor eforturilor în domeniul siguranței copiilor online, ceea ce face procesul de monitorizare și evaluare ineficient, limitându-l la raportarea datelor statistice, care deseori sunt dublate în diferite rapoarte.

2.4. Lacune și provocări identificate

Provocări în implementarea politicilor

Planul de Acțiuni privind promovarea siguranței copiilor online, în mare parte, nu a fost pus în practică din mai multe motive:

1. Lipsa resurselor financiare alocate pentru implementarea activităților. Această problemă a fost menționată de toate autoritățile publice ce au completat chestionarul online în contextul cercetării.
2. Formulări destul de vagi/confuze în HG nr. 212 din 5 aprilie 2017 ce au creat impedimente în implementarea acțiunilor planificate;
3. Nivel redus de înțelegere a subiectului de către autoritățile publice, confirmat prin permanenta confuzie dintre termenii „siguranță online” și „securitate cibernetică”.
4. Nivel redus de expertiză/cunoștințe despre domeniul dat în rândul specialiștilor din cadrul autorităților publice responsabile de implemen-

tarea acțiunilor planificate, ceea ce se confirmă și prin raportarea precară a acțiunilor realizate, fără a intra în esența acțiunilor ce trebuiau implementate. Despre problema resurselor umane și deficiențelor în pregătirea acestora au menționat reprezentanții MAI, MECC și MEI în contextul cercetării.

Din cauza evaluărilor contradictorii și datelor inconsistente furnizate de diverși reprezentanți ai autorităților publice devine o adevărată provocare de terminarea stadiului de implementare a Planului de acțiuni. Deși majoritatea activităților au fost raportate ca fiind puse în practică, diverși reprezentanți prezintă în rapoartele de implementare date irelevante, contradictorii sau care nu corespund indicatorilor de progres reglementați.

Nivelul de implicare și colaborare a autorităților responsabile în implementarea politicilor ce vizează siguranța copiilor online e redus. Spre exemplu, deși în Planul național de acțiuni privind siguranța copiilor online sunt prevăzute acțiuni ce urmau a fi implementate în parteneriat cu Centrul de Guvernare Electronică, autorități ale administrației publice locale, furnizori de rețele și/sau servicii de comunicații electronice, Centrul Republican de Asistență Psihopedagogică ș.a., datele furnizate în raportul de implementare a acestui PNA indică despre lipsa unei colaborări în domeniu, acțiunile fiind realizate doar de autoritățile responsabile. Această problemă

a fost menționată și de reprezentantul MAI, care a specificat că, aparent, multe acțiuni au fost realizate separat de către autorități, fără a colabora cu alte instituții sau parteneri.

Probleme ce vizează coordonarea politicilor în domeniu

După reforma de optimizare la nivelul autorităților publice centrale, subiectul siguranței copiilor online a ajuns pe agenda MEI. Ținând cont de faptul că domeniile gestionate de MEI sunt mai complexe și diverse, siguranța online, la moment, nu constituie o prioritate pe agenda MEI.

Cu toate acestea, în ultimii 3 ani, MEI a avut responsabilitatea de coordonare a Planului de acțiuni tematic în domeniul siguranței copiilor online, dar și altor politici ce stabileau măsuri de siguranță online. În această perioadă, nu a fost desfășurată nicio ședință de coordonare cu reprezentanții ministerelor responsabile pentru monitorizarea implementării politicilor. Cu regularitate, a fost solicitată prezentarea informațiilor actualizate pentru perioada de raportare. În unele cazuri, au fost expediate demersuri suplimentare în vederea identificării cauzelor nerealizării acțiunilor și întreprinderii măsurilor necesare de înlăturare a acestora. Motivele ce au împiedicat desfășurarea ședințelor de coordonare sunt lipsa personalului dedicat și/sau lipsa de resurse financiare. În această situație, convocarea ședințelor de coordonare a eforturilor de implementare ar fi fost puțin utilă, întrucât nu ar fi avut acțiuni de raportat.

O altă provocare este reglementarea unor acțiuni ce vizează siguranța online în cadrul mai multor documente de politici (Moldova Digitală, Protecția copilului, Securitate cibernetică, Securitate informațională, Promovarea siguranței copiilor și tinerilor online). Aceasta creează impedimente în asigurarea unei coordonări eficiente, în monitorizarea tuturor inițiativelor în domeniu și în realizarea unei evaluări corespunzătoare. Fiecare Plan de acțiuni sau Strategie vizată analizează segmentat eforturile întreprinse, ținând cont de obiectivele strategice propuse. Prin urmare, deși în Planul de acțiuni privind implementarea Strategiei privind protecția copilului sunt incluse acțiuni ce vizează protecția copiilor online, raportul intermediar de implementare a acestuia s-a focusat doar pe obiectivele strategice planificate și nu au fost specificate detalii despre implementarea acestor activități sau despre rezultatele obținute în domeniul siguranței online.

Lipsa unei unități de coordonare sau a unui mecanism de monitorizare/coordonare a eforturilor în domeniu, care să țină cont de toate politicile ce stabilesc măsuri de siguranță online, determină un mecanism deficitar de guvernare în politicile publice. Această problemă a fost menționată și de reprezentanții MAI în contextul acestei cercetării.

Problema lipsei unui mecanism de coordonare adecvat în sectorul politicilor

de protecție a copilului este una recunoscută de mai mulți ani. În contextul elaborării mai multor studii tematice³² ce vizează implementarea Convenției de la Lanzarote de către RM, s-a stabilit că lipsește un coordonator responsabil de punerea în aplicare a Convenției și o instituție distinctă care să monitorizeze eforturile în domeniu.

Probleme ce vizează monitorizarea și raportarea acțiunilor implementate

Rapoartele de implementare a politicilor în domeniul siguranței online indică despre o problemă considerabilă în colectarea de date relevante și în prezentarea acestora. Deși există un mecanism clar de raportare a informației către MEI, modul în care autoritățile/instituțiile vizate raportează informații despre acțiunile implementate nu ține cont de prevederile PNA privind promovarea siguranței pe Internet a copiilor. Un exemplu ar fi datele prezentate în contextul implementării subacțiunii 3.1, ce vizează implementarea cadrului legal **referitor la incriminarea actelor de natură xenofobă săvârșite prin intermediul sistemelor informatice.** La această rubrică, MAI a prezentat date privind numărul de **infrațiuni de abuz sexual și exploatare sexuală online** investigate de poliție, infrațiuni care nu au nicio legătură cu actele de natură xenofobă.

La fel, deși PNA stabilește clar care sunt indicatorii de progres, autoritățile responsabile în majoritatea cazurilor **au raportat**

³² Exploatarea sexuală și abuzul sexual față de copii. Implementarea Convenției de la Lanzarote de către RM, La Strada, 2017 și Studiul privind analiza problemelor sistemice care afectează răspunsul sistemului de protecție a copilului la exploatarea și abuzul sexual al copilului, CoE, 2019.

informații despre realizarea acțiunilor, fără a ține cont de cele planificate.

De exemplu, subacțiunea 4.5 „Dezvoltarea bazei de date naționale pentru materialul foto/video cu conținut ilegal”, conform PNA, are următorii indicatori de progres:

- Baza de date ajustată și eficientă;
- Mecanismul de clasificare a materialului foto/video cu conținut ilegal;
- Numărul de sesizări/raportări înregistrate cu material foto/video cu conținut ilegal;

Cu toate acestea, datele furnizate de MAI sunt despre colaborarea în cadrul proiectului internațional „I-CARE” inițiat în anul 2016. Nu este clar cum este clasificat materialul foto/video cu conținut ilegal, care este numărul de sesizări sau raportări de material foto/video cu conținut ilegal, dacă există o bază de date națională sau dacă totuși organele de poliție utilizează doar baza de date internațională a Interpol.

Informațiile raportate de către autorități sunt incoerente. Despre aceleași activități se menționează de mai multe ori, pe diferite platforme. De exemplu, activitățile realizate în contextul Zilei Siguranței Online și Lunarului securității cibernetice sunt raportate atât în contextul implementării PNA privind promovarea siguranței pe Internet a copiilor, cât și în contextul Programului de Securitate Cibernetică (a se vedea Figura nr. 3).

Mai mult decât atât, **datele raportate de către unele autorități sunt contradictorii și lipsite de relevanță.** Un exemplu se re-

feră la implementarea Acțiunii 1 de creare a punctelor de contact naționale pentru raportarea conținutului ilegal din internet. Așadar, deși nu a fost elaborat un cadru normativ privind funcționarea platformei web pentru raportarea conținutului ilegal din internet (subacțiunea 1.1), Agenția pentru Protecția Moralității a raportat că este în proces de creare a unei platforme web pentru raportarea conținutului ilegal din Internet (subacțiunea 1.2) și de promovare a acestei platforme (subacțiunea 1.3). Ținând cont de faptul că crearea platformei și promovarea acesteia ar fi subacțiuni, ce ar trebui să urmeze logic după crearea cadrului legal de reglementare/funcționare a acesteia, din datele publicate, reiese că promovarea platformei este îndeplinită chiar dacă platforma nu a fost creată.

În contextul anchetei realizate prin chestionar online, un reprezentant al MAI a specificat că ar trebui îmbunătățit procesul de monitorizare a rezultatelor din domeniul siguranței copiilor online pentru următorul ciclu de politici. Conform reprezentantului MEI, a fost dificil de monitorizat felul în care autoritățile au îndeplinit acțiunile Planului, întrucât acestea nu erau receptive la raportare. Unele autorități raportau că este imposibil sau dificil să pună în practică acțiunile din cauza lipsei de personal și/sau resurselor materiale necesare.

Relevanța obiectivelor anterioare în contextul actual

Reieșind din tendințele de utilizare a internetului de către copii și domeniile

problematică identificată, autoritățile publice intervievate în contextul cercetării au constatat că o bună parte dintre obiectivele planificate în Planul de acțiune privind promovarea siguranței pe Internet a copiilor și adolescenților rămân la fel de actuale, și anume:

- Obiectiv 1. Reducerea conținutului ilegal din Internet și abordarea comportamentului cu impact negativ online;
- Obiectiv 2. Promovarea unui mediu digital mai sigur pentru copii și adolescenți prin colaborarea tuturor părților implicate;

- Obiectiv 3. Sensibilizarea și informarea părților aflate în contact direct cu copiii despre riscurile mediului online și elaborarea recomandărilor privind navigarea în siguranță pe Internet;
- Obiectiv 4. Elaborarea statisticilor și promovarea cercetărilor privind siguranța online a copiilor și adolescenților.

Cu toate acestea, e necesară revizuirea modului în care sunt formulate obiectivele și acțiunile planificate, pentru a asigura o bună interpretare și implementare de către autoritățile vizate.

Principalele constatări:

1. Măsurile de protecție a copilului în mediul online și de promovare a siguranței online sunt abordate fragmentar, în diferite documente de politici, fără a exista o legătură logică între acestea. Acest fapt creează impedimente în evaluarea impactului politicilor în domeniul siguranței copiilor online, în determinarea dinamicii pozitive în domeniul de interes, eficientizarea rezultatelor obținute, etc.
2. Se atestă un nivel scăzut de cunoaștere și înțelegere a subiectului de către autoritățile responsabile de implementarea politicilor în domeniul siguranței copiilor online;
3. Modelul actual de coordonare a eforturilor în domeniul siguranței copiilor online este absolut ineficient, fapt ce determină abordarea superficială a problemei;
4. Nivelul de colaborare și implicare a partenerilor în implementarea activităților este minim, limitându-se la acțiuni realizate în contextul unor proiecte;
5. În pofida faptului că a fost aprobat un document de politici tematic în domeniul siguranței copiilor online, lipsește angajamentul ferm al autorităților publice de a implementa acțiunile planificate.



3.

Standarde și abordări internaționale

3.1. Modul de integrare a siguranței copiilor online în politicile internaționale

Strategie distinctă dedicată subiectului

Pe plan internațional, siguranța copiilor online e abordată încă din anii 1999, odată cu aprobarea Planului de Acțiuni pentru un Internet mai Sigur 1999-2004³³. În contextul în care acesta a fost elaborat, la etapa incipientă de dezvoltare a industriei Internetului, prioritățile Uniunii Europene (UE) erau să combată conținutul ilegal și dăunător, să creeze o rețea de servicii Hotline³⁴, să încurajeze măsuri de auto-reglementare, să dezvolte filtre de conținut, dar și să realizeze activități de sensibilizare.

În ultimii 20 de ani, prioritățile UE în acest domeniu au fost revizuite. Cea mai recentă **Strategie Europeană pentru un Internet mai bun pentru copii**³⁵, aprobată de Comisia Europeană în 2012, are următoarele domenii de acțiune:

- **Stimularea conținutului online de calitate pentru tineri**, prin încurajarea producției de conținut creativ și educațional online și promovarea experiențelor pozitive online ale copiilor;
- **Promovarea educației digitale**, de alfabetizare digitală și **predarea siguranței online în școli**;
- **Sporirea gradului de conștientizare** și abilitare prin activități de sensibilizare și implicare a tinerilor,

dar și prin promovarea unor instrumente de raportare a conținutului online;

- **Implementarea unor măsuri tehnice** de setare a opțiunilor de confidențialitate, utilizarea programelor de control parental, clasificare de conținut sau stimularea unor măsuri de auto-reglementare pentru a proteja copiii de conținuturi publicitate nepotrivite;
- **Dezvoltarea cadrului legal și aplicarea legii** în vederea identificării și oferirii suportului victimelor, întreprinderii acțiunilor împotriva abuzatorilor, stopării circulației imaginilor ce reprezintă abuz sexual al copilului prin detectarea și înlăturarea acestora de pe internet și prin prevenirea încălcării acestora.

Această abordare presupune reglementarea diferitor măsuri ce trebuie întreprinse, inclusiv legislative, măsuri de auto-reglementare sau de co-reglementare, măsuri tehnice și educaționale, dar și de sensibilizare. În practică, modul de implementare a acestei Strategii variază în fiecare țară. Niciun stat din UE nu a implementat această Strategie Europeană direct, prin transpunere într-un document de politici separat, focusat doar pe aspecte ce vizează siguranța online. 50% dintre state (12 state) au elaborat o serie de politici separate care abordează direct subiectul siguranței

³³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A124190>

³⁴ Serviciu Hotline – serviciu de raportare a conținutului ilegal pe Internet.

³⁵ <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52012DC0196&from=EN>

online, iar celelalte 12 state abordează subiectul în politici cu profil mai larg³⁶.

Activitățile de sensibilizare și promovarea educației digitale și educației despre siguranța online sunt integrate, de obicei, în politici cu profil mai larg. Iar pilonul 5 din Strategia Europeană ce vizează combaterea abuzului sexual față de copii vizează doar cadrul legal și organele de drept și, de obicei, sunt abordate distinct.

Integrarea siguranței online în documente de politici cu o tematică mai largă

Siguranța copiilor online în contextul promovării drepturilor copilului

Spre deosebire de cadrul de politici la nivelul țărilor UE, care se remarcă prin aprobarea unei politici sectoriale tematice ce vizează protecția copiilor în mediul online, Consiliul European a reglementat măsuri ce vizează siguranța copiilor online în **Strategia Consiliului European pentru Drepturile Copilului 2016-2021** – un document de politici mai comprehensiv, ce abordează măsuri generale de promovare a drepturilor copilului. Așadar, unul dintre domeniile prioritare de intervenție în această Strategie sunt drepturile copilului în mediul digital și anume: participarea copilului în mediul digital, protecția copilului față de riscuri online și educația copilului privind utili-

zarea creativă, critică și sigură a internetului.

Comitetul de Miniștri completează inițiativele UE în domeniu, în următoarele direcții strategice:

- **Protejarea drepturilor copiilor în mediul online** (Recomandarea Comitetului de Miniștri CM/Rec(2018)7 privind Liniile directorii ce vizează respectarea, protejarea și realizarea drepturilor copilului în mediul digital³⁷);
- **Promovarea educației pentru cetățenia digitală**, ce include și dimensiunea siguranței online, în legislația, politicile și practicile din domeniul educației (Recomandarea Comitetului de Miniștri CM/Rec(2019)10 privind dezvoltarea și promovarea educației pentru cetățenia digitală³⁸).

În Recomandarea Comitetului de Miniștri CM/Rec(2018) se menționează necesitatea întreprinderii unor acțiuni de către fiecare stat în vederea protejării copiilor online. Mai mult decât atât, au fost recunoscute necesitatea unei bune coordonări și coerenței politicilor ce vizează copilul online și nevoia de a lua măsuri consistente care să se consolideze reciproc. Aceasta ar putea presupune fie adoptarea unei strategii

³⁶ O'Neill, B. Dinh, The Better Internet for Kids Policy Map, Implementing the European Strategy for a Better Internet for Children in European Member States, March 2018.

³⁷ <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>

³⁸ Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, adopted by the Committee of Ministers on 21 November 2019 at the 1361st (Budget) meeting of the Minister's Deputies.

sau a unui plan de acțiuni integrat care să reglementeze drepturile copilului în mediul online, fie integrarea subiectului în politicile existente.

Cât privește tipul de măsuri ce necesită a fi întreprinse de statele membre, Recomandarea enunțată stabilește necesitatea unei abordări holistice care să reglementeze:

- măsuri de sensibilizare despre subiect;
- măsuri privind materialele ce reprezintă abuz sexual al copilului;
- măsuri de angajare a companiilor private ca parteneri-cheie în promovarea drepturilor omului, prin asumarea angajamentelor de protecție a copilului online;
- dezvoltarea serviciilor și produselor ce țin cont de interesele copiilor;
- crearea unor remedii eficiente în cazurile în care copiii li s-au încălcat anumite drepturi.

Implicarea tuturor actorilor vizați (reprezentanților din domeniul educației, autorităților ce protejează datele cu caracter personal, întreprinderilor de business, membrilor societății civile, organizațiilor de tineret; participarea directă a copiilor, etc.) atât la etapa de elaborare a politicilor, cât și la etapa de implementare reprezintă un principiu-cheie.

Dreptul copilului la protecție și siguranță online rămâne unul dintre domeniile în care e recomandată întreprinderea de acțiuni, în vederea diminuării riscurilor

de contact (exploatare sexuală și abuz, grooming, etc.), riscurilor de conținut (promovarea portretului stereotipizat și hipersexualizat al femeii sau copiilor; promovarea violenței online, etc.), riscurilor de conduită (bullying, distribuirea non-consimțită a imaginilor cu caracter sexual, discursul de ură, etc.) sau riscurilor pentru sănătatea copilului (utilizarea excesivă, lipsa de somn sau dauna fizică).

Siguranța copiilor online în politicile privind securitatea cibernetică

Nu există o definiție standard a securității cibernetică, universal acceptată. În sens larg, securitatea cibernetică presupune măsuri de protecție a sistemelor informaționale de accesul neautorizat, atac și daune, acțiuni care să asigure confidențialitatea, integritatea și disponibilitatea datelor. Totodată, securitatea cibernetică presupune și prevenirea, detectarea, răspunsul și acțiunile de recuperare de după un incident cibernetic.

Definiția securității cibernetică propusă de UIT pune accent pe protecția infrastructurii, dar nu pe protecția persoanei: „colectarea de instrumente, politici, orientări, abordări de gestionare a riscurilor, acțiuni, instruirii, bune practici, asigurări și tehnologii ce pot fi utilizate **pentru a proteja disponibilitatea, integritatea și confidențialitatea infrastructurii aferente guvernului, organizațiilor private și cetățenilor**; aceste active includ dispozitive de calcul conectate, personal, infrastructură,

aplicații, servicii, sisteme de telecomunicații și date din mediul online³⁹. **Așadar, acestea delimitează clar măsurile menite să contribuie la siguranța copiilor online** (pun accent pe bunăstarea emoțională, fizică, sexuală a copilului în mediul online) **și securitatea copiilor online** (vizează protecția sistemelor informaționale, informațiilor, dispozitivelor la care are acces un copil).

În politicile UE, securitatea cibernetică este utilizată în context mai larg, fără a se limita la securitatea rețelelor și informațiilor. Termenul vizează orice activitate ilegală realizată cu utilizarea tehnologiilor digitale în mediul online, cum ar fi: lansarea atacurilor cu viruși computerizați, fraude la realizarea plăților fără numerar sau **diseminarea materialelor ce reprezintă abuz sexual online al copiilor**. La fel, vizează și campaniile de influență a dezbaterilor online și acțiunile de ingerință electorală⁴⁰.

Integrarea siguranței online în politicile privind securitatea cibernetică rămâne un subiect controversat, întrucât practicile statelor sunt diferite, iar reglementarea „pornografiei infantile” în mai multe tratate internaționale creează confuzie în implementare și implică un răspuns fragmentar în domeniu. Totuși, evoluțiile din ultimii ani au determinat necesitatea delimitării unui nou domeniu - „**violența cibernetică**” față de copii și femei, ce se referă la

următoarele forme de infracțiuni reglementate de Convenția de la Lanzarote, Convenția de la Istanbul și Convenția de la Budapesta:

- **abuz și exploatare sexuală online a copiilor;**
- infracțiuni cibernetice;
- infracțiuni motivate de ură;
- amenințări directe și violența fizică;
- încălcări ale vieții private;
- hărțuirea online.

Exploatarea sexuală online a copiilor este un domeniu reglementat de Convenția de la Lanzarote și de Convenția de la Budapesta. Deși ambele fac referință la infracțiunea de pornografie infantilă, Convenția de la Lanzarote e mult mai detaliată și complexă în ceea ce privește cadrul legal material. Cu toate acestea, lipsesc măsuri procedurale sau mijloace de cooperare internațională relevante pentru investigațiile realizate cu utilizarea sistemelor informatice sau pentru asigurarea electronică a probelor. Iată de ce, **Statele ar trebui să implementeze instrumentele și mijloacele puse la dispoziție de Convenția de la Budapesta pentru realizarea investigațiilor** și să încurajeze utilizarea lor pentru combaterea eficientă a dimensiunii online a exploatării sexuale și abuzului sexual față de copii, în special prin aplicarea prevederilor art. 16 și art. 21 din Convenția de

³⁹ https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

⁴⁰ Challenges to effective EU cybersecurity policy, Briefing paper, march 2019, disponibil la https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

la Budapesta în legislația națională, și să faciliteze cooperarea internațională privind probele electronice (art 23 – 35 din Convenția de la Budapesta)⁴¹.

Cât privește conținutul politicilor naționale în domeniul securității cibernetice, Recomandările UIT de dezvoltare a Strategiilor Naționale definesc 7 domenii de intervenție ce necesită a fi abordate: Guvernanța; Managementul riscurilor în securitatea cibernetică la nivel național;

Pregătirea și reziliența; Servicii de infrastructură critică și servicii esențiale; Capacitatea, dezvoltarea de capacități și sensibilizarea; Legislația și normele regulatorii; Cooperarea internațională.

Niciunul dintre aceste domenii nu vizează exploatarea sexuală online a copiilor, care e un subiect mult mai specific și NU ar trebui abordat în contextul unei strategii naționale ce vizează securitatea cibernetică.

Principalele constatări:

1. În documentele de politici internaționale, siguranța copiilor online este fie subiectul unor politici tematice în domeniu, fie e integrată în documentele de politici cu o tematică mai vastă (spre exemplu – în contextul protecției drepturilor copilului);
2. E recomandată delimitarea clară a măsurilor menite să contribuie la siguranța copiilor online și care pun accent pe bunăstarea emoțională, fizică și sexuală a copilului în mediul online, de cele ce se referă la securitatea online și care vizează protecția sistemelor informaționale, informațiilor, dispozitivelor la care are acces un copil;
3. Recomandările și politicile internaționale din domeniul securității cibernetice nu abordează siguranța copilului online. De obicei, măsurile de prevenire și protecție a copilului în mediul virtual sunt reglementate în politicile publice scopul cărora e să asigure protecția drepturilor copilului (Strategia CoE pentru drepturile copilului) sau în politici tematice (Strategia europeană pentru un Internet mai bun pentru copii).
4. Securitatea cibernetică poate fi platformă-umbrelă pentru toate măsurile de combatere a infracțiunilor cibernetice, inclusiv pentru combaterea pornografiei infantile. În aceste politici ar putea fi reglementate acțiunile menite să îmbunătățească răspunsul organelor de drept sau măsurile de investigație în cazurile de abuz sau exploatare sexuală online, conform prevederilor Convenției de la Budapesta.

⁴¹ <https://www.coe.int/en/web/cybercrime/-/t-cy-mapping-study-on-cyberviolence-recommendations>

3.2. Dimensiuni ale politicilor în domeniul siguranței online

O abordare comprehensivă a măsurilor de protecție a copiilor în mediul online, ce derivă din standardele prevăzute de Convenția de la Lanzarote, vizează în mod special doi piloni principali:

prevenirea riscurilor online și protecția copiilor. Conform angajamentelor internaționale asumate odată cu ratificarea acestei Convenții, Statele s-au obligat să întreprindă măsuri pe diferite dimensiuni (a se vedea Figura nr. 4).

Dimensiuni ale politicilor de protecție a copiilor online

Prevenirea riscurilor online

- Plan Strategic la nivel național
- Cadrul de protecție a copiilor online
- Programe de instruire și educație
- Campanii de informare și sensibilizare
- Programe de responsabilitate socială
- Colectare de date și cercetări

Protecția copiilor online

- Instrumente legislative îmbunătățite
- Procese legale oficializate, inclusiv arestări, urmăriri penale și condamnări
- Servicii pentru victime
- Servicii pentru agresori
- Mecanisme de monitorizare și raportare

Figura nr. 4

Sursa: Studiul privind Materialele de Abuz Sexual asupra copiilor: modele de legislație și revizuire globală, ICMEC, 2018

Această abordare e recomandată și de WePROTECT – o inițiativă internațională de îmbunătățire a capacității globale de combatere a exploatării sexuale a copiilor în mediul online⁴². În 2015, 43 de state din întreaga lume, Biroul ONU pentru Droguri și Criminalitate (în continuare – UNODC)

și Interpol și-au asumat angajamentul de a întreprinde acțiuni menite să contribuie la impulsivarea eforturilor naționale de protecție a copiilor online, în baza Modelului de Răspuns Național elaborat în cadrul acestei inițiative⁴³. Acest Model reprezintă un cadru unic de coordonare internaționa-

⁴² Statement of action by Governments to tackle online CSE: Abu Dhabi WeProtect Summit, 16-17 November 2015, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT+-Global+Alliance+Model+National+Response+Guidance.pdf>

⁴³ Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>

lă, având scopul de a evalua răspunsul curent al statelor la această problemă, modul de ierarhizare a eforturilor naționale și identificarea lacunelor politicilor, ce necesită a fi înlăturate, pentru a susține Guvernele să atingă următoarele obiective⁴⁴:

- **Sporirea eforturilor de identificare a victimelor** și asigurarea asistenței, suportului și protecției de care acestea au nevoie;
- **Consolidarea eforturilor de investi-gare a cazurilor** de exploatare sexuală online a copiilor, de identificare și urmărire penală a abuzatorilor;
- **Consolidarea eforturilor de infor-mare și sensibilizare a publicului** în raport cu activitățile riscante ale copiilor în mediul online, inclusiv

groomingul și imaginile cu caracter sexual auto-produse.

- **Reducerea la maxim a accesului către materialele ce reprezintă abuz sexual online al copilului** și, prin urmare, reducerea șanselor de victimizare repetată a copiilor ce au trecut prin experiența unui abuz sexual online.

Standardele setate de către acest instrument vizează următoarele aspecte: măsuri menite să consolideze cadrul de coordonare, politicile publice și legislația; măsuri menite să îmbunătățească modul de desfășurare a investigațiilor, serviciile furnizate victimelor; măsuri menite să contribuie la sensibilizarea societății în raport cu exploatarea sexuală a copiilor în mediul online și altele (Tabelul nr. 5).

Extras din Modelul național de răspuns pentru prevenirea și combaterea abuzului și exploatării sexuale online a copilului, elaborat de Alianța WeProtect

| | | | |
|----------------------|------------------------|----|--|
| Tabelul nr. 5 | Politici și Guvernanța | 1. | Leadership: Un Comitet național de guvernare și de supraveghere funcțional |
| | | 2. | Cercetare, Analiză și Monitorizare: Analiza națională a riscurilor de exploatarea sexuală online și răspunsului față de acestea; Evaluarea situației în baza unor indicatori |
| | | 3. | Legislație: Un cadru legal comprehensiv și eficient, care asigură investigarea co-rispondătoare a abuzatorilor și protecția victimelor |

⁴⁴ Our Strategy to End the Sexual Exploitation of Children Online, WePROTECT Global Alliance, iulie 2016, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/578408b5f7e0ab851b789e14/1479254482761/WePROTECT+Global+Alliance+Strategy.pdf>

| | | |
|-----------|-----|---|
| Justiție | 4. | Structuri de poliție specializate: Structuri cu mandat național, ce dispun de ofițeri instruiți; realizează investigații pro-active și reactive, centrate pe interesele victimelor și cooperează cu structuri internaționale specializate |
| | 5. | Procurori și judecători: Instruiți, demonstrând abordări centrate pe interesele copiilor-victime |
| | 6. | Procesul de abordare a infractorilor: Acțiuni întreprinse în vederea prevenirii recidivei la nivel național și internațional |
| | 7. | Acces la baza de date specializată: Baza de date națională funcțională; acces la baza de date a Interpol (ICSE) |
| Victime | 8. | Suport: Servicii integrate în timpul investigațiilor, urmării penale, dar și după acțiunile procesuale |
| | 9. | Specialiștii în contact cu copilul: Instruiți și disponibili să furnizeze suport victimelor |
| | 10. | Compensații, remedii și proceduri de depunere a reclamațiilor: Proceduri accesibile |
| | 11. | Servicii de consiliere pentru copii: Servicii de raportare și suport pentru victime, referire către alte structuri pentru asistență continuă |
| Societate | 12. | Hotline: Mecanism de raportare a cazurilor de abuz sexual online, ce poate stabili legătura cu organele de drept și sistemul de protecție a copilului |
| | 13. | Programe educaționale: Pentru copii și tineri; părinți și îngrijitori; cadre didactice; practicieni; reprezentanți ai cultelor religioase |
| | 14. | Participarea copilului: Copiii și tinerii au o voce în dezvoltarea politicilor și practicilor |
| | 15. | Sisteme de suport pentru abuzatori: Suport medical, psihologic, auto-ajutor, sensibilizare |

| | | |
|---------------------|-----|---|
| Industrie | 16. | Proceduri de înlăturare a conținutului: Ștergerea sau blocarea conținutului ce reprezintă exploatarea sexuală online a copilului |
| | 17. | Raportarea cazurilor de exploatare sexuală online a copiilor: Prevederi legale ce ar permite companiilor TIC să raporteze în mod eficient cazurile de exploatare sexuală online, inclusiv prin expedierea conținuturilor către organele de poliție sau alte organe competente |
| | 18. | Soluții inovative pentru dezvoltare: Angajamentul industriei de a ajuta în combaterea cazurilor de exploatare sexuală online a copiilor la nivel local |
| | 19. | Măsuri de responsabilitate socială: Programe eficiente centrate pe interesele copilului |
| Media și comunicare | 20. | Abordarea etică și bine documentată a subiectului în mass-media: Sensibilizarea publicului și reflectarea corespunzătoare a problemei |
| | 21. | Terminologie universală: Linii directoare și aplicarea acestora |

Acest Model este implementat de 43 de state din întreaga lume, care au subsemnat această Strategie a Alianței Globale pentru a combate abuzul sexual și exploatarea sexuală online. Pornind de la aceste Standarde, Statele semnatare, inclusiv RM, și-au dezvoltat măsuri de răspuns naționale. Cea mai mare provocare în implementarea acestui Model este identificarea de către fiecare stat a elementelor unice ce definesc vulne-

rabilitatea copiilor la abuzul sexual și exploatarea sexuală online, la nivel național, și identificarea acțiunilor care ar funcționa la nivel național⁴⁵.

RM este membră a Alianței Globale, însă nu a subsemnat această Strategie. Cu toate acestea, în anul 2014, RM a raportat despre realizarea parțială a unor acțiuni în domeniu, conform celor patru obiective enunțate mai sus⁴⁶.

⁴⁵ <https://www.end-violence.org/sites/default/files/paragraphs/download/WePRO-TECT%20Global%20Alliance.pdf>

⁴⁶ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/commitments/ga_commitment_-_moldova_en.pdf

Principalele constatări:

Practica statelor europene în domeniul siguranței copiilor online indică despre faptul că acest subiect nu poate fi abordat doar într-un singur document de politici. Protecția copilului în mediul virtual poate fi asigurată printr-un spectru divers de acțiuni ce vizează domeniile educației și protecției copilului, domeniul de aplicare a legii/justiției, cu responsabilități de combatere a abuzului și exploatării sexuale online. Protecția copilului în mediul virtual presupune asumarea - pentru autoritățile din sectorul educației, protecției copilului, domeniul de aplicare a legii/justiției - de responsabilități pentru combaterea abuzului și exploatării sexuale online.

3.3. Modele de coordonare a eforturilor

Studiile realizate în cadrul Programului EU Kids Online au stabilit unele criterii de evaluare și un clasificator al statelor din perspectiva politicilor naționale în domeniul siguranței copiilor online⁴⁷. Conform acestuia, cele mai dezvoltate politici de promovare a siguranței online sunt în statele în care sectorul public este implicat profund în aceste politici, în colaborare cu Centrele pentru Siguranța Online⁴⁸. Totodată, aceste state alocă resurse financiare în bugetul public pentru implementarea acestor acțiuni și evaluarea rezultatelor, promovează abilitățile digitale ale copiilor și părinților și abordează pro-activ medierea riscurilor.

Cel mai înalt nivel de dezvoltare a politicilor din acest domeniu au fost constatate în Belgia, Franța, Germania, Grecia,

Spania și UK. Aceste state se caracterizează prin:

- Existența unei agenții de profil înalt, specializată în domeniul siguranței copiilor online, cu responsabilități de coordonare;
- Cadru legal și normativ comprehensiv, bine dezvoltat;
- Spectru larg de inițiative de cercetare în domeniu;
- Implicarea pro-activă a sectorului public, care acționează ca un motor puternic în domeniul educației, inițiativelor de sensibilizare și abilitare;
- Un spectru larg de inițiative de politici;
- Centrele de siguranță online⁴⁹ au un rol important în coordonarea efor-

⁴⁷ Policy influences and country clusters. A comparative analysis of Internet Safety Policy Implementation, LSE, London: EU Kids Online, O'Neill, B. (2014).

⁴⁸ Centru pentru Siguranța Online (Safer Internet Center) – structuri funcționale la nivelul statelor din UE ce desfășoară diverse inițiative, servicii și resurse pentru a menține copiii în siguranță online.

⁴⁹ Centru de siguranță online – Servicii ce furnizează informații, sfaturi, asistență copiilor, tinerilor și părinților despre cum să facă față conținutului dăunător, contactelor cu impact negativ (de ex. grooming) sau conduită dăunătoare (de ex. hărțuire online și sexting).

turilor ori activează complementar pentru dezvoltarea politicilor în domeniu.

Un nivel redus de angajamente politice se caracterizează prin lipsa unei structuri responsabile de coordonare a eforturilor, lipsa unor cercetări în domeniu și lipsa unui cadru de evaluare a politicilor. La cel mai limitat nivel de dezvoltare a politicilor în domeniul siguranței online sunt țările din Europa de Est: Bulgaria, Cipru, Cehia, Polonia și România. Aceste țări se caracterizează printr-un nivel înalt de riscuri online și o mediere ineficientă a acestora. În aceste state se atestă:

- Lipsa unei coordonări a politicilor ce vizează siguranța online;
- Evoluții relativ recente ale politicilor;
- Inițiativele noi sunt focusate pe dezvoltarea sectorului TIC;
- Lipsește un cadru de monitorizare și evaluare a politicilor;
- Centrele de siguranță online reprezintă o platformă de coordonare a

activităților despre siguranța online;

- Sectorul public este mai puțin implicat decât în alte regiuni ale Europei;
- Nu sunt alocate resurse financiare din bugetul public pentru implementarea acestor politici.

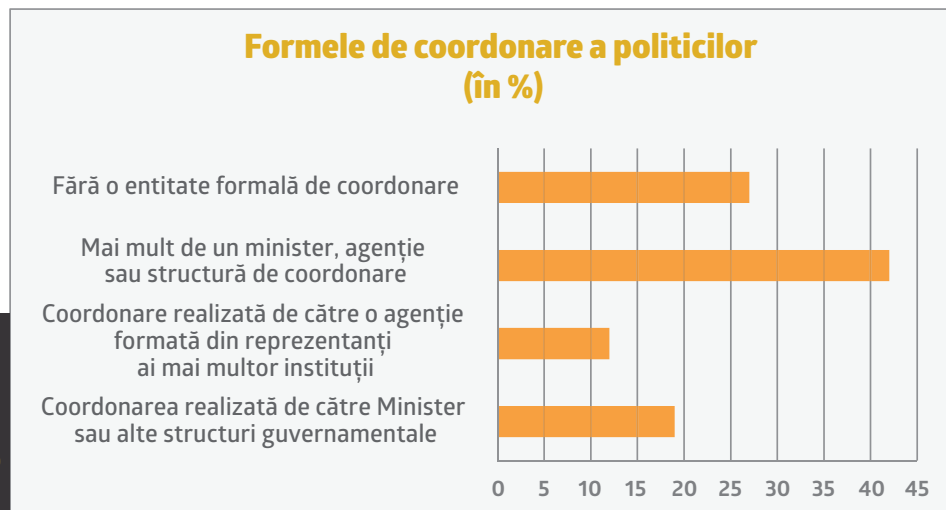
RM nu este unica țară care se confruntă cu probleme în coordonarea eficientă a eforturilor de promovare a siguranței online și de protecție a copiilor față de abuzul și exploatarea sexuală online. Această problemă e influențată și de lipsa unor recomandări clare la nivel internațional, inclusiv din partea Comitetului de la Lanzarote – structură responsabilă de coordonarea acțiunilor de monitorizare a eforturilor de implementare a Convenției de la Lanzarote de către statele membre, dar și de furnizarea suportului explicativ și informațional, pentru o mai bună înțelegere a angajamentelor asumate⁵⁰.

Statele din Europa au diferite practici de coordonare a politicilor în domeniul siguranței copiilor online. În mai bine de 42% dintre state, există mai multe ministere sau structuri de coordonare.

⁵⁰ Studiul privind analiza problemelor sistemice care afectează răspunsul sistemului de protecție a copilului la exploatarea și abuzul sexual al copilului, CoE 2019.

Formele de coordonare a politicilor despre siguranța online în statele din Europa.

Figura nr. 5



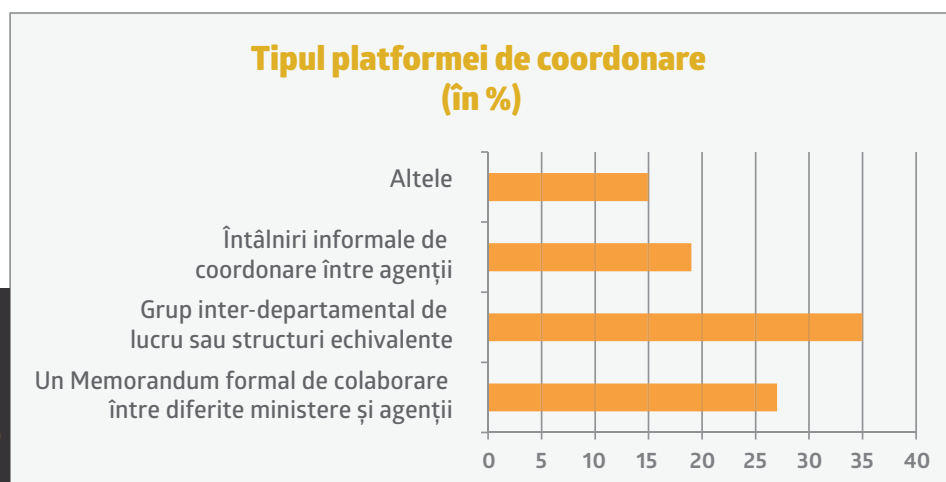
Sursa: Raportul de implementare a Strategiei europene pentru Internet mai bun pentru copii de către statele membre ale UE

Pentru a facilita cooperarea între instituții și agenții în ceea ce privește politicile de siguranță a copilului online, 73% dintre state au creat mecanisme de faci-

litare a cooperării inter-departamentale sau inter-instituționale. Tipurile de platforme de coordonare sunt menționate în Figura nr. 6.

Tipul platformei de coordonare în statele din Europa

Figura nr. 6



Sursa: Raportul de implementare a Strategiei europene pentru Internet mai bun pentru copii de către statele membre ale UE

Principalele constatări:

Setarea unui mecanism de coordonare a politicilor în domeniul siguranței copiilor online este o provocare pentru mai multe state europene. Așa precum nu există unele recomandări de coordonare eficientă a politicilor în acest domeniu, fiecare stat și-a dezvoltat propriile practici de guvernare, fie prin crearea unei agenții specializate de nivel înalt, fie prin atribuirea acestui rol unor structuri specializate (Centrele de siguranță online) sau mai multor ministere cu responsabilități de implementare a politicilor.

Cert este că o condiție a dezvoltării politicilor ce vizează siguranța copilului online este coordonarea eficientă a eforturilor, printr-o implicare activă a sectorului public, monitorizare și evaluare a rezultatelor și o abordare comprehensivă centrată pe interesele copilului.

Concluzii generale și recomandări

1. Siguranța copilului online reprezintă un subiect de interes pe mai multe platforme de politici publice: protecția copilului, securitatea cibernetică, Moldova digitală, securitatea informațională, siguranța online. Astfel, se atestă eforturi paralele și fragmentare întreprinse de autoritățile publice, fără o viziune strategică unică, fără o abordare comprehensivă care să integreze toate eforturile din domeniu într-un cadru unic de monitorizare și evaluare.

Coordonarea politicilor s-a rezumat la solicitarea rapoartelor de implementare a acțiunilor planificate, fără a fi desfășurate ședințe cu autoritățile vizate.
2. Experiența din ultimii ani a indicat despre o dublare a acțiunilor raportate în contextul monitorizării mai multor documente de politici. Unele acțiuni au fost reflectate în rapoartele de implementare a Planului de Acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020 și în Raportul pentru executarea Programului național de securitate cibernetică a RM pentru anii 2016-2020.
3. Determinarea stadiului de implementare a PNA privind promovarea siguranței pe Internet a copiilor este o provocare cauzată de evaluarea contradictorie și de datele inconsistente furnizate de diverși reprezentanți ai autorităților publice. Deși majoritatea activităților au fost raportate ca fiind implementate, datele furnizate sunt insuficiente, pe alocuri sunt contradictorii sau nu coincid cu indicatorii de progres reglementați. Respectiv, nu permit aprecierea progresului și situației faptice, împiedică conturarea priorităților și planificarea următoarelor acțiuni.
4. Lipssește un angajament ferm de implementare a măsurilor menite să promoveze siguranța copiilor online. Aceasta se datorează lipsei resurselor financiare și personalului specializat. O bună parte dintre acțiunile planificate nu au fost realizate, au fost amânate sau stagnate din

varii motive. Chiar dacă RM are angajamente politice asumate prin ratificarea Convenției de la Lanzarote, autoritățile nu au întreprins eforturi în acest sens.

5. Siguranța online este un concept generic, care deseori e confundat cu alți termeni precum „securitatea cibernetică”, „securitatea online” sau „securitatea informațională”. Prin urmare, actorii responsabili de implementarea politicilor deseori se orientează spre aspecte ce vizează securizarea dispozițiilor digitale, păstrarea securității informațiilor sau dezvoltarea abilităților de utilizare a tehnologiilor, iar acțiunile ori-

entate spre prevenirea și diminuarea riscurilor de conduită și contact ale copilului sunt adesea neglijate.

6. Lipsește o abordare centrată pe interesele copilului, ancorată în necesitatea de a diminua din riscurile de conținut, de conduită sau de contact la care se expun copiii prin dezvoltarea abilităților de gândire critică în mediul online și promovarea serviciilor/opțiunilor de raportare a abuzurilor online. Această abordare e specifică nu doar pentru RM, dar pentru mai multe state din Europa de Est, în care se atestă un nivel incipient de dezvoltare a politicilor în domeniu.

Recomandări de ordin strategic

1. Întrucât RM este membră a Alianței Globale împotriva Exploatării Sexuale Online a Copiilor „WeProtect”, e necesară actualizarea parteneriatului și angajamentelor asumate, prin subsemnarea noului Model de politici recomandat pentru prevenirea și combaterea abuzului și exploatării sexuale online. Totodată, e necesară stabilirea unor noi priorități și acțiuni naționale pentru asigurarea implementării graduale a acestui Model.
2. Pentru următorul ciclu de politici, e absolut necesară instituirea unui mecanism de coordonare adecvat în domeniul protecției copiilor față de riscurile în mediul online. A se lua în considerație toate opțiunile care există în domeniu: fie prin capacitatea unui minister, sub egida căruia poate fi creat un grup de lucru tehnic, ce ar asigura atât comunicarea eficientă între autorități pe segmentul de studiu, cât și monitorizarea regulată și continuă a eforturilor în domeniu; fie prin revizuirea competenței CNPDC și atribuirea responsabilității de coordonare și monitorizare a eforturilor întreprinse în domeniul protecției copiilor față de riscurile online.
3. Întrucât măsurile ce vizează siguranța online pot fi incluse în mai multe documente de politici, e necesară coordonarea la nivel inter-instituțional pentru a asigura comunicare între diferite structuri responsabile de dezvoltarea politicilor, dar și asigurarea coerenței politicilor, între diferite măsuri/acțiuni planificate în documente de politici.
4. În contextul expirării mai multor documente de politici publice (Planului Național de Acțiuni privind Promovarea Siguranței pe Internet a Copiilor și Adolescenților pentru anii 2017-2020, Programului național de securitate cibernetică a RM pentru anii 2016-2020 și Planului de acțiuni privind implementarea acestuia, etc.) ce reglementau măsuri de siguranță online, devine imperativă planificarea unor acțiuni în vederea continuării eforturilor în domeniul promovării siguranței copiilor online. Pentru aceasta, e necesară cre-

area unui grup de lucru sub egida MSMPS, care ar planifica întregul set de acțiuni în domeniul promovării siguranței online.

5. În procesul de elaborare a politicilor în domeniul siguranței copiilor online, este important să se țină cont de angajamentele internaționale asumate prin semnarea tratatelor internaționale ce vizează protecția copiilor față de abuzul sexual și exploatarea sexuală online, pentru a asigura o abordare complexă, ce corespunde recomandărilor internaționale (Convenția de la Lanzarote, Convenția de la Budapesta).
6. **E necesară implicarea reprezentanților tuturor autorităților și instituțiilor publice vizate în elaborarea următoarelor politici în domeniu, pentru a asigura același nivel de înțelegere a subiectului**

și asumarea responsabilității prin participare. Totodată, acest fapt ar include promovarea siguranței copiilor online pe agenda MSMPS, MECC, MAI, PG. MEI și altor structuri interesate sau cu responsabilități în domeniu.

7. Preluarea modelului de politici publice în domeniul siguranței copiilor online recomandat pe plan internațional, care distinge clar scopul de prevenire și combatere a abuzului și exploatării sexuale, prin care se asigură protecția bunăstării fizice, psihice și sexuale a copilului în mediul online. Securitatea online, prin care se au în vedere acțiuni menite să contribuie la securitatea dispozitivelor digitale, a informațiilor necesită a fi abordată separat, în politici de vizează securitatea cibernetică sau securitatea informațională.

Recomandări operaționale

Reieșind din principalele constatări și domenii problematice identificate, se recomandă abordarea complexă a riscurilor online la care se expun copiii, bazată pe următoarele obiective-cheie:

1. Abilitarea copiilor și dezvoltarea rezilienței față de abuzul online

Ministerul Educației, Culturii și Cercetării ar trebui să se asigure că, în procesul educațional, copiilor le sunt furnizate informații despre cum să facă alegeri informate, evitând eventualele riscuri online, și să întreprindă acțiuni de răspuns în cazuri de abuz online. În această ordine de idei, sunt necesare:

- Revizuirea curriculei școlare și politicilor educaționale pentru ca acestea să integreze aspecte ale siguranței online în activitățile cu elevii, la toate categoriile de vârstă. A asigura o delimitare foarte clară între aspectele ce vizează bunăstarea psiho-emoțională a copilului în mediul online și aspectele ce vizează securitatea online, etc.
- Integrarea siguranței copiilor online în programele de formare profesio-

nală continuă a cadrelor didactice, în vederea abilitării acestora pentru desfășurarea activităților educative cu copiii, în scopul prevenirii abuzului sexual online;

- Crearea și implementarea unor programe de dezvoltare a competențelor parentale ce ar ține cont de beneficiile și riscurile asociate utilizării TIC, punând accent pe educația copilului despre comportamentele sigure în mediul online, soluțiile și serviciile de suport disponibile în caz de abuz.
- 2. Îmbunătățirea răspunsului sistemului de justiție la abuzul sexual și exploatarea sexuală online a copiilor.

Ministerul Afacerilor Interne, Ministerul Justiției, Procuratura Generală și Inspectoratul General al Poliției ar trebui să asigure ajustarea cadrului legal la standardele internaționale și capacitatea reprezentanților organelor de drept și sistemului judecătoresc pentru a asigura un răspuns corespunzător la cazurile de abuz și exploatare sexuală online. În acest scop, sunt necesare:

- Ajustarea cadrului legal ce incriminează acțiunile ilegale de abuz și exploatare sexuală online la prevederile Convenției de la Lanzarote;
 - Ajustarea cadrului legal ce prevede măsurile procesuale de investigație și urmărire penală a infracțiunilor săvârșite cu utilizarea TIC la prevederile Convenției de la Budapesta;
 - Dezvoltarea unor linii directorii pentru reprezentanții organelor de drept (polițiști și procurori) privind realizarea acțiunilor de investigație și urmărire penală a infracțiunilor ce reprezintă abuz sexual și exploatare sexuală online, din perspectiva protejării intereselor copilului;
 - Dezvoltarea și consolidarea expertizei conținutului ilegal și dăunător online;
 - Formarea profesională a reprezentanților organelor de drept și sistemului judecătoresc în domeniul identificării, investigării și judecării infracțiunilor ce reprezintă abuz sexual și exploatare sexuală online, centrate pe interesele copilului în procesul penal;
 - Menținerea specializării structurilor din cadrul procuraturii și organelor de poliție responsabile de investigarea și realizarea acțiunilor de urmărire penală în cazuri de abuz și exploatare sexuală online și asigurarea desfășurării regulate a activităților de consolidare a capacităților acestora. O astfel de abordare ar asigura centrarea pe interesele victimelor și ar corespunde bunelor practici și recomandări internaționale.
- 3.** Furnizarea serviciilor de suport și asistență pentru copiii - victime ale abuzului sexual online;
- Ministerul Sănătății, Muncii și Protecției Sociale și Ministerul Educației, Culturii și Cercetării trebuie să asigure pregătirea profesională a specialiștilor aflați în contact cu copilul, pentru a identifica și interveni în mod corespunzător în cazurile de abuz în mediul online. În acest scop, sunt necesare:
- Formarea profesională a specialiștilor din sistemul de protecție a copilului - evaluarea riscului abuzului sexual online, acțiunile de intervenție și furnizarea asistenței în baza necesităților identificate;
 - Dezvoltarea capacităților profesioniștilor aflați în contact cu copiii (cadrelor didactice, psihologilor școlari) - evaluarea riscurilor la care se expun copiii, identificarea semnalelor ce indică despre un posibil abuz și acțiuni de intervenție centrate pe interesele copilului;
 - Dezvoltarea unor politici instituționale de promovare a siguranței online printr-o abordare comprehensivă, astfel încât să fie asigurat un răspuns eficient în toate cazurile de abuz online identificate în școală, iar copilul să poată avea acces imediat la servicii de suport sau consiliere specializate.

- Dezvoltarea unor instrucțiuni pentru specialiștii din sistemul de protecție a copilului și sistemul de educație (asistenți sociali, cadre didactice, psihologi școlari) privind identificarea și raportarea cazurilor de abuz sexual online asupra copilului către organele de poliție.
- 4. Realizarea cercetărilor privind ultimele tendințe în domeniul siguranței online;
 - Analiza factorilor de vulnerabilitate a copiilor în mediul online și măsurilor educaționale de prevenire a acestor riscuri;
 - Analiza comportamentului abuzatorului în vederea determinării modului de operare a acestuia, măsurilor eficiente de identificare/investigare/prevenire a acestor infracțiuni reieșind din tendințele constatate;

Ministerul Educației, Culturii și Cercetării, Institutul de Dezvoltare a Societății Informaționale, precum și alte părți interesate ar trebui să ia măsuri pentru a asigura realizarea cercetărilor în domeniul siguranței online, ce ar facilita dezvoltarea următoarelor politici în domeniu, abordând următoarele aspecte:

- Evaluarea riscurilor la care se expun copiii online;

Recomandăm să se țină cont de practicile internaționale care, pe parcursul ultimilor 15 ani, dezvoltă astfel de cercetări cu scopul de a îmbunătăți cadrul de politici publice în domeniu (EU Kids Online, Global Kids Online⁵¹); de metodologia aplicată pe plan internațional, subiectele cercetate și modul în care acestea servesc ulterior la elaborarea politicilor în domeniu.

⁵¹ <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online>

Referințe

- 1) Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, adopted by the Committee of Ministers on 27 September 2006 at the 974th meeting of the Ministers' Deputies, disponibil la https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805af669;
- 2) Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), adopted by the Committee of Ministers on 5 September 2001 at the 762nd meeting of the Ministers' Deputies, disponibil la https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804deb54;
- 3) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children/*-COM/2012/0196 final*/, disponibil la <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0196%3AFIN>
- 4) Council of Europe Strategy for the Rights of the Child (2016-2021), disponibil la [Council of Europe Strategy for the Rights of the Child \(2016-2021\)](#)
- 5) Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, disponibil la
- 6) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGIS-SUM%3A124190>

- 7) Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor, Strategia europeană pentru un Internet mai bun pentru copii, aprobată de Comisia Europeană, 2012, disponibil la <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52012DC0196&from=EN>
- 8) Recommendation CM/Rec(2018)7 of the Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, disponibil la <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>
- 9) Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, adopted by the Committee of Ministers on 21 November 2019 at the 1361st (Budget) meeting of the Minister's Deputies, disponibil la https://library.parlhelp.eu/wp-content/uploads/2019/12/CoE-digital-citizenship-education-recommendations-CM_Rec201910E.pdf.
- 10) ITU, Guide to developing a national cybersecurity strategy, Strategic engagement in cybersecurity, disponibil la https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf
- 11) Challenges to effective EU cybersecurity policy, Briefing paper, march 2019, disponibil la https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf
- 12) Hotărârea Guvernului nr. 257 din 22.11.2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia, publicat la 18.01.2019 în Monitorul Oficial nr. 13-21, art. 80.
- 13) Legea nr. 299 din 21 decembrie 2017 privind aprobarea Concepției securității informaționale a Republicii Moldova.
- 14) Hotărârea Guvernului nr. 811 din 29.11.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, publicat la 13.11.2015 în Monitorul Oficial nr. 306-310, art. 905.
- 15) Hotărârea Guvernului nr. 212 din 5 aprilie 2017 pentru aprobarea Planului de acțiuni privind promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020.
- 16) Hotărârea Guvernului nr. 857 din 31 octombrie 2013 privind aprobarea Strategiei Naționale de dezvoltare a societății informaționale „Moldova digitală 2020”.

- 17) Raportul pentru executarea în semestrul II 2019 a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, disponibil la http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf
- 18) Understanding cybercrime: phenomena, challenges and legal response, ITU, September 2012, disponibil la <http://www.itu.int/ITU-D/cyb/cyber-security/docs/Cybercrime%20legislation%20EV6.pdf>
- 19) WeProtect Global Alliance, Global Threat Assessment 2019, Working together to end the sexual exploitation of children online, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL++Global+Threat+Assessment.pdf>
- 20) The Better Internet for Kids Policy Map, Implementing the European Strategy for a Better Internet for Children in European Member States, March 2018, disponibil la <https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report++Final++March+2018/a858ae53-971f-4dce-829c-5a02af9287f7>.
- 21) Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, adopted by the Cybercrime Convention Committee, Working group on other forms of online violence, especially against women and children, disponibil la <https://www.coe.int/en/web/cybercrime/-/t-cy-mapping-study-on-cyberviolence-recommendations>
- 22) Child Sexual Abuse Material: Model legislation and Global review, ICMEC, 9th edition 2018, disponibil la <https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf>
- 23) Statement of action by Governments to tackle online CSE: Abu Dhabi WeProtect Summit, 16-17 November 2015, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50b-c534a51764e8a4ec/1549388168335/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>
- 24) Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50b-c534a51764e8a4ec/1549388168335/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>
- 25) Our Strategy to End the Sexual Exploitation of Children Online, We-

PROTECT Global Alliance, iulie 2016, disponibil la <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/578408b5f7e0ab-851b789e14/1479254482761/WePROTECT+Global+Alliance+Strategy.pdf>

26) [The WeProtect Global Alliance, Working examples of model national response capabilities and implementation, disponibil la https://www.end-violence.org/sites/default/files/paragraphs/download/WePROTECT%20Global%20Alliance.pdf](https://www.end-violence.org/sites/default/files/paragraphs/download/WePROTECT%20Global%20Alliance.pdf)

27) Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației, Anuar statistic, Dezvoltarea comunicațiilor electronice în Republica Moldova, în anul 2019, disponibil la https://www.anrceti.md/files/filefield/Anuar%20statistic%202019_22aprilie_2020.pdf

28) Centrul Internațional „La Strada Moldova”, Siguranța copiilor pe Internet, 2017, disponibil la http://lastrada.md/files/resources/3/Siguranta_copii-pe_Internet_-_final.pdf

29) [Factsheet Siguronline pentru perioada anului 2019, disponibil la http://lastrada.md/pic/uploaded/ffFactSheet%20siguronline%202019_FINAL.pdf](http://lastrada.md/pic/uploaded/ffFactSheet%20siguronline%202019_FINAL.pdf)

30) [Factsheet Echipa de Asistență a Copilului din cadrul Centrului Internațional „La Strada Moldova”, pentru perioada anului 2019, disponibil la http://lastrada.md/pic/uploaded/EAC%20Factsheet%20sem%202%20_%202019.pdf](http://lastrada.md/pic/uploaded/EAC%20Factsheet%20sem%202%20_%202019.pdf)

31) [Factsheet Siguronline pentru perioada primului semestru 2020, disponibil la http://lastrada.md/pic/uploaded/Siguronline%2520factsheet_1%-2520sem._2020.pdf](http://lastrada.md/pic/uploaded/Siguronline%2520factsheet_1%-2520sem._2020.pdf)

