Siguranța online a copiilor în Republica Moldova

www.coe.int/children

Construirea unei Europe cu și pentru copii

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Siguranța online a copiilor în Republica Moldova

Analiza legislației, politicilor și practicilor pentru prevenirea, identificarea, raportarea și eliminarea materialelor online care reprezintă exploatarea și abuzul sexual asupra copiilor

Manual elaborat de:
John Carr
Elena Botezatu

Consiliul Europei

Ediția în limba engleză: Online safety for children in the Republic of Moldova. Analysis of legislation, policies and practices for prevention, identification, reporting and removal of online child sexual exploitation and abuse materials.

Copertă și așezare în pagină: Tipografia Centrală

Fotografie copertă: © Imagine folosită sub licența Shutterstock.com

Prezenta Analiză a fost elaborată în cadrul proiectului Consiliului Europei „Protecția copiilor împotriva violenței și prevenirea acesteia, inclusiv în mediul online în Republica Moldova".

Manualul a fost elaborat de următorii autori, în strânsă colaborare cu proiectul Consiliului Europei „Protecția copiilor împotriva violenței și prevenirea acesteia, inclusiv în mediul online în Republica Moldova".

John Carr, consilier internațional pentru siguranța și securitatea pe internet a copiilor, Regatul Unit licențiat în drept la London School of Economic and Political Science.
În 2021, a scris capitolul privind istoria globală a politicii de protecție a copiilor online în Oxford University Press Handbook on Cyber Security. În 1996, John Carr a fost unul dintre directorii fondatori ai uneia dintre primele linii telefonice de urgență din lume, cea din Marea Britanie, Internet Watch Foundation, iar în prezent este membru al Consiliului consultativ al INHOPE, asociația globală a liniilor telefonice de urgență.

Elena Botezatu, Președintă a Centrului Internațional „La strada". Elena Botezatu este autoarea mai multor cercetări tematice privind siguranța copiilor online și exploatarea sexuală online a copiilor, inclusiv analiza politicilor privind siguranța copiilor online, analiza practicilor educaționale și a răspunsului la riscurile online, cercetări privind experiențele online și riscurile la care sunt expuși copiii din Republica Moldova etc.

Cuprins

1. Introducere și metodologie

Internetul își are originea în comunitatea academică și de cercetare, o lume aparținând integral adulților. Cu toate acestea, internetul a devenit, printre multe altele, un mijloc de comunicare pentru familii, un mijloc de comunicare pentru copii.

În cea mai mare parte a Europei, unul din cinci utilizatori de internet este copil, adică o persoană cu vârsta sub 18 ani.[1] În întreaga lume, proporția este de unul din trei, iar în unele țări, aproximativ cincizeci la sută din toate ființele umane care utilizează internetul sunt copii.

În Republica Moldova nu sunt disponibile date fiabile la nivel macro privind numărul de copii care utilizează internetul și în ce categorii de vârstă. Cu toate acestea, este extrem de probabil ca, în timp, poate chiar foarte curând, nivelurile de utilizare în rândul copiilor din Republica Moldova să reflecte nivelurile de utilizare în rândul copiilor din alte părți ale Europei. În timp ce datele la nivel macro privind utilizarea nu sunt disponibile în acest moment, datorită studiilor individuale orientate, se cunosc totuși foarte multe despre modul în care copiii moldoveni utilizează efectiv tehnologiile digitale, ce beneficii obțin de pe urma acestora, precum și ce probleme întâmpină. Nu este surprinzător faptul că experiența copiilor moldoveni reflectă mai mult sau mai puțin exact experiențele copiilor de pretutindeni în Europa și chiar din întreaga lume.[2]

Extinderea și transformarea pe piețele în care copiii sunt prezenți în număr substanțial nu sunt lipsite de consecințe pentru toate părțile lanțului valoric digital, atât în Republica Moldova, cât și la nivel global.

În timp ce copiii au fost beneficiarii principali ai tehnologiilor digitale care permit conectarea la internet sau utilizarea acestuia, prea mulți au fost, de asemenea, afectați de acestea. Abuzul sexual și exploatarea sexuală a copiilor pe internet continuă să reprezinte un motiv de îngrijorare majoră.[3] Acesta este principalul obiectiv al prezentului raport. Prezentul raport oferă o imagine de ansamblu, orientată spre Europa, a siguranței online pentru copii, cu accent pe prevenirea, identificarea și raportarea abuzurilor sexuale asupra copiilor și a

[1] https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html

[2] https://lastrada.md/pic/uploaded/COS%20Research%202021_summary.pdf

[3] https://www.weprotect.org/global-threat-assessment-21/

exploatării sexuale a copiilor online, adesea denumite „grooming" (ademenire), precum și pe prevenirea, identificarea, raportarea și eliminarea materialelor de exploatare sexuală a copiilor (CSAM), ținând seama de standardele relevante ale Consiliului Europei și internaționale, cum ar fi Convenția Consiliului Europei privind protecția copiilor împotriva exploatării sexuale și a abuzului sexual,[4] Convenția privind criminalitatea informatică[5] și Recomandarea CM/Rec(2018)7 a Comitetului de Miniștri,[6] precum și directivele și regulamentele adoptate de Uniunea Europeană.

Auto-reglementarea internetului a eșuat.[7] În prezent, în numeroase jurisdicții, întreprinderile nu au nicio obligație de a detecta în mod proactiv și de a încerca să prevină sau să devieze comportamentele de ademenire. De asemenea, acestea nu sunt obligate să detecteze CSAM deja stocate pe serviciul lor sau să împiedice încărcarea sau schimbul de CSAM prin intermediul unuia dintre dispozitivele sau serviciile lor. Adesea, nu există nicio obligație de a fi proactivi în ceea ce privește raportarea oricărui CSAM pe care îl descoperă. Așteptarea ca orice CSAM descoperit să fie șters la sursă este un corolar logic al legilor care interzic posesia acestuia, dar și în acest caz noile legi și reglementări care apar acum vor oferi o mai mare claritate în ceea ce privește ceea ce se așteaptă de la întreprinderi în această privință, de exemplu în ceea ce privește termenele operaționale acceptabile.

Toți acești factori sunt în schimbare în multe țări. Direcția politică, în special în cadrul Uniunii Europene, dar și în numeroase jurisdicții din afara UE, este de a impune obligații obligatorii furnizorilor de servicii electronice, atât de a lua măsuri active pentru a detecta materialele de exploatare sexuală a copiilor, cât și de a le raporta autorităților, în așa fel încât să faciliteze identificarea victimei și a editorului. În plus, există un nivel ridicat de așteptări în ceea ce privește detectarea și prevenirea comportamentului de ademenire. A fost dezvoltată o serie de instrumente noi, automatizate, pentru a ajuta furnizorii de servicii electronice să îndeplinească astfel de sarcini la scară largă și cu costuri minime. Aceste instrumente vor fi discutate în acest raport.

Noile medii de reglementare obligatorii la care se face referire și care sunt dezvoltate de guverne și legiuitori de toate culorile politice, în țări de toate mărimile de pe toate continentele, prevăd noi standarde și obligații minime pe care furnizorii de servicii electronice (ESP) vor trebui să le adopte. Aceste standarde și obligații se referă la responsabilități ESP atât în ceea ce privește entitățile cu care au relații contractuale directe care decurg din produsele sau serviciile pe care le vând sau le furnizează, de exemplu, părinții, dar și în ceea ce privește toți utilizatorii finali ai acestor produse

---

[4] Disponibil online la https://rm.coe.int/16800d3832
[5] Disponibil online la https://rm.coe.int/1680081561
[6] ibid.
[7] https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_com-2020-607-commission-communication_en.pdf

și servicii, în special copiii. În această măsură, ESP încep să facă obiectul unor forme de supraveghere reglementară comune în mai multe tipuri diferite de industrii care operează pe o gamă diversă de piețe orientate către consumatori, unde accentul pe siguranța utilizatorului final este de o importanță capitală, mai degrabă decât pe cea exclusivă sau simplă a entității care plătește inițial pentru produsul sau serviciul respectiv sau care îl plătește în mod continuu.

Noile standarde și obligații la care se face referire acoperă mai multe subiecte interconectate, dar, în toate cazurile, se pune un accent puternic pe abordarea abuzului și exploatării sexuale a copiilor.

Prezentul raport se concentrează asupra dimensiunii online a abuzului sexual asupra copiilor și a exploatării sexuale a copiilor; cu toate acestea, în mai multe puncte se face referire și se recunoaște pe deplin importanța vitală a măsurilor luate în lumea offline pentru a reduce incidența abuzului sexual asupra copiilor și a exploatării sexuale a copiilor în primul rând sau pentru a răspunde nevoilor victimelor din lumea fizică. Acestea sunt vitale pentru succesul general al oricărei inițiative. Consiliul Europei a elaborat o serie de recomandări care pot ajuta la orientarea factorilor de decizie politică la nivel național și internațional în ceea ce privește abuzul sexual asupra copiilor și exploatarea sexuală a copiilor, atât online, cât și offline.[8]

Metodologie

Raportul a fost redactat în urma unei consultări și a unei discuții în plen cu o gamă largă de actori importanți din sectorul public și privat, urmate de întrebări structurate și nestructurate și de interviuri individuale cu persoane-cheie din guvernul și din industria moldovenească, completate de o analiză a lacunelor din legislația moldovenească actuală în raport cu standardele internaționale stabilite. Exemple de întrebări utilizate în cadrul interviurilor structurate sunt prezentate în anexa 1.

Analiza lacunelor

Analiza și corelarea cu standardele internaționale au fost efectuate în perioada octombrie-noiembrie 2022 în cadrul proiectului Consiliului Europei privind *prevenirea și protecția copiilor împotriva violenței, inclusiv în mediul digital în Republica Moldova*. Aceasta face parte dintr-un program continuu de sprijin pe care Consiliul Europei îl oferă în legătură cu aceste probleme vitale.

[8] Disponibil online la https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8

2. Concluzii și rezumat executiv

1. Este evident că, în pofida unei perioade susținute de activitate pe aceste teme din partea Guvernului Republicii Moldova, este încă necesară prioritizarea protecției online a copiilor în cadrul industriilor digitale locale.
2. De exemplu, o parte dintre părțile interesate intervievate păreau să nu știe cine, în cadrul companiei lor, avea responsabilitatea de a aborda problemele legate de siguranța online a copiilor. De asemenea, există în continuare un atașament puternic față de ideea că responsabilitățile și relațiile primare ale companiilor de tehnologie sunt mai degrabă cu persoanele care plătesc pentru produsele și serviciile lor decât cu cele care le utilizează. Copiii vor fi rareori clienți plătitori, dar ei constituie un număr substanțial de utilizatori finali. Pe lângă acest punct de vedere, în ceea ce privește copiii, există ideea că este de datoria părinților să asigure siguranța copiilor lor și, într-adevăr, așa este. Dar este, de asemenea, o obligație etică din partea fiecărei întreprinderi active pe o piață de consum care se adresează copiilor, de a ușura cât mai mult posibil sarcina părinților, făcând ca toate dispozitivele și serviciile să fie cât mai sigure posibil la prima utilizare. Este în detrimentul siguranței copiilor să transferăm responsabilitatea pe umerii altor persoane într-o măsură atât de semnificativă.
3. În majoritatea jurisdicțiilor din întreaga lume, ideea de autoreglementare a fost sau este în curs de abandonare. Cu toate acestea, se pare că ea continuă să aibă un număr de adepți în rândul industriilor digitale din Republica Moldova.
4. Din acest motiv, recomandarea cea mai puternică pe care o facem este ca guvernul să își intensifice programul legislativ pentru a stabili tipul de regim obligatoriu care este favorizat acum de UE, de Regatul Unit și de alte câteva jurisdicții. Cu toate acestea, ar putea exista un motiv întemeiat pentru a stabili priorități:
   a. Toate societățile care își desfășoară activitatea în Republica Moldova și care vând sau promovează servicii sau produse online care se pot conecta la internet ar trebui să aibă obligația legală de a desemna un membru al conducerii superioare care să aibă responsabilitatea de a coordona toate aspectele politicii privind utilizarea produselor și serviciilor lor de către copii.
   b. Ar trebui să se adopte o nouă lege care să oblige companiile să raporteze toate cazurile de ademenire (grooming) și toate cazurile în care se descoperă materiale de abuz sexual asupra copiilor către un organism desemnat prin reglementări.

5. Într-un astfel de nou cadru, se sugerează cu tărie să se pună un accent deosebit pe importanța evaluărilor de risc care, la rândul lor, vor conduce la stabilirea unor standarde adecvate vârstei și la obligații mai mari de a include siguranța prin proiectare și securitatea în mod implicit.
6. Pentru a asigura și a menține încrederea publicului în noile acorduri, trebuie să se acorde o atenție deosebită elaborării unor standarde de transparență adecvate care, la rândul lor, sunt legate de obligații solide și obligatorii în materie de confidențialitate, supravegheate de o parte de încredere.[9]

[9] La 15 decembrie 2022, guvernul australian a publicat primele rapoarte majore de transparență din istoria sa, în conformitate cu legislația recent adoptată https://www.esafety.gov.au/newsroom/media-releases/world-first-report-shows-leading-tech-companies-are-not-doing-enough-tackle-online-child-abuse. Acesta arată o imagine foarte inegală în ceea ce privește companiile care abordează sau nu abordează exploatarea sexuală a copiilor online.

3. Contextul din Republica Moldova

Republica Moldova este una dintre cele mai conectate țări din lume, cu o rată de penetrare a internetului de 76,1% din totalul populației la începutul anului 2022. 18,3% din întreaga populație, care este estimată la 4,02 milioane de persoane, sunt copii. Cercetări recente efectuate în țară arătau că 60% dintre copii pot accesa internetul oricând doresc, fără nicio limită, iar, odată cu creșterea vârstei copiilor, numărul de utilizatori de internet devine mai mare.[10]

Situația de pandemie, restricțiile impuse și migrarea procesului educațional pe platforme online i-au determinat pe copii să petreacă mai mult timp pe internet. Din păcate, tendințele globale și datele naționale furnizate de liniile naționale de asistență online, cum ar fi www.siguronline.md, indică un nivel ridicat de vulnerabilitate a copiilor la riscurile online, iar în ultimii trei ani s-au înregistrat mai multe experiențe neplăcute și cazuri de abuz sexual online.

12% dintre copiii cu vârste cuprinse între 9 și 17 ani au primit propuneri sexuale explicite pe chat. 1 din 100 de copii a trimis conținut sexual explicit care îi reprezintă pe ei înșiși unei persoane cu care au discutat online. La nivel mondial, criza COVID-19 a dus la o creștere bruscă a distribuției online de materiale de abuz sexual asupra copiilor, care era deja la niveluri ridicate înainte de pandemie.[11] Potrivit EUROPOL, au existat creșteri semnificative ale activității legate de abuzul sexual asupra copiilor și de exploatarea sexuală a copiilor, atât pe web de suprafață, cât și pe dark web, în perioada de izolare a pandemiei COVID-19. Numărul sporit de infractori care fac schimb de CSAM online poate avea un impact asupra cererii pentru acest tip de materiale online și poate stimula cererea de astfel de materiale online. În același timp, nivelurile constante de activitate ale infractorilor pe dark web în timpul perioadei de izolare reflectă modelul de activitate organizată care a evoluat și nivelul de amenințare pe care îl reprezintă pentru copii.

În perioada 2020 - 2021, procurorul general a instrumentat 105[12] cazuri de abuz și exploatare sexuală a copiilor în mediul online. De asemenea, unitatea de combatere a criminalității cibernetice a poliției a investigat 81 de cazuri, reprezentând diverse forme de abuz și exploatare sexuală online: ademenire (grooming), sextortion, pornografie infantilă etc.

---

[10] https://lastrada.md/pic/uploaded/Studiu_Siguranta_online-comportamente_si_riscuri-FINAL.pdf
[11] ibidem
[12] Date interne comunicate de Procuratura Generală și de unitatea de combatere a criminalității informatice a poliției.

3.1. Contextul politic și coordonarea

Răspunsul național la combaterea exploatării sexuale a copiilor și a abuzului sexual online este încă fragmentar, lipsind o abordare sistemică și cuprinzătoare. În plus, lipsește un organism guvernamental care să fie mandatat să coordoneze politicile, orientările și programele referitoare la drepturile copiilor în mediul digital. Prima încercare de a pune subiectul pe agenda unei anumite autorități a fost în 2016, când, la inițiativa Consiliului Național pentru Protecția Copilului, a fost elaborată prima politică de promovare a siguranței copiilor în mediul online. Anterior, Ministerul Tehnologiei Informației și Comunicațiilor a devenit responsabil de coordonarea implementării Planului național de acțiune.

După reforma de optimizare din 2018, subiectul siguranței online a copiilor a ajuns pe agenda Ministerului Economiei și Infrastructurii. În cadrul reformei administrației publice centrale din august 2021, responsabilitățile în domeniul TIC au fost împărțite între două ministere: Ministerul Infrastructurii și Dezvoltării Regionale - problemele legate de infrastructura de comunicații electronice și politicile de reglementare în domeniu, iar Ministerul Economiei - legislația în domeniul comerțului electronic. Dezvoltarea societății informaționale - e-guvernare - este responsabilitatea viceprim-ministrului pentru digitalizare.

În anul 2022, Guvernul Republicii Moldova a creat un organ de coordonare în domeniul exploatării sexuale a copiilor și a abuzurilor sexuale asupra copiilor - Comisia specializată mandatată să coordoneze și să monitorizeze implementarea Convenției de la Lanzarote[13] . Comisia servește drept mecanism de coordonare între diferite agenții în ceea ce privește implementarea politicilor legate de protecția copiilor împotriva abuzului și exploatării sexuale, online și offline. Fiind co-prezidată de Ministerul Afacerilor Interne și de Ministerul Muncii și Protecției Sociale, aceasta reunește reprezentanți ai autorităților publice, inclusiv ai Ministerului Economiei și Infrastructurii și Dezvoltării Regionale, responsabili de elaborarea politicilor legate de digitalizare și de dezvoltarea industriei tehnologiei informației.

Până în 2022, siguranța online a copiilor era un subiect de interes pe mai multe platforme naționale de politici publice: protecția copilului, securitatea cibernetică, Moldova digitală, securitatea informațională și siguranța online. În plus, lipsea un angajament ferm de implementare a măsurilor menite să promoveze siguranța online a copiilor, din cauza lipsei resurselor financiare și a personalului specializat. Un număr mare de activități/acțiuni planificate nu au fost realizate sau au fost anulate sau amânate din diverse motive.[14]

---

[13] Hotărârea Guvernului cu privire la instituirea Comisiei specializate pentru coordonarea și monitorizarea implementării Convenției Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale și a abuzului sexual și aprobarea Regulamentului acesteia, nr. 66-d din 19.05.2022.

[14] https://lastrada.md/pic/uploaded/A_Research_Child_online_safety_2020.pdf

În prezent, nu există o politică unică la nivel național care să reflecte măsuri care să abordeze mediul digital și responsabilitățile pentru industrie, coduri sau standarde de proiectare. De asemenea, nu există o înțelegere clară cu privire la rolul industriei în asigurarea protecției online a copiilor, deoarece politicile anterioare în domeniu nu au reflectat măsuri cuprinzătoare pentru industrie.

Noul document de politică privind protecția copilului elaborat pentru perioada 2022-2026 trebuia să integreze un set complet de măsuri menite să asigure protecția online a copiilor. Cu toate acestea, Programul național de protecție a copilului pentru 2022-2026 și Planul de acțiuni[15] pentru punerea în aplicare a acestuia, aprobat de Guvernul Republicii Moldova, nu reflectă obiective specifice legate de protecția online a copiilor. Au fost incluse unele acțiuni privind revizuirea cadrului normativ pentru a asigura o intervenție promptă a sistemului de protecție adaptată la necesitățile fiecărui copil și creșterea gradului de conștientizare a impactului negativ al tuturor formelor de violență împotriva copiilor (inclusiv în mediul online), crearea unui mecanism de raportare a materialelor privind abuzul sexual asupra copiilor. În plus, Guvernul a planificat să elaboreze un Plan național de acțiune pentru promovarea siguranței copiilor în mediul online (până la sfârșitul anului 2023).

3.2. Cadrul legislativ

În plus, cadrul juridic național nu este pe deplin aliniat la standardele internaționale. Chiar dacă Republica Moldova a ratificat tratate-cheie privind protecția copiilor împotriva abuzului și exploatării sexuale, cum ar fi Convenția de la Lanzarote, Convenția de la Budapesta și Convenția ONU privind drepturile copilului, se înregistrează blocaje.

În urma ratificării Convenției de la Lanzarote, autoritățile naționale au revizuit legislația pentru a incrimina diferite forme de abuz și exploatare sexuală, inclusiv infracțiunile facilitate de TIC. Cu toate acestea, cadrul juridic național prezintă mai multe deficiențe în ceea ce privește administrarea probelor în format electronic, care nu respectă standardele Convenției de la Budapesta. În prezent, în legislația procesual penală lipsesc măsurile de conservare rapidă a datelor informatice stocate, măsura de punere la dispoziție a datelor care se află în posesia sau sub controlul unei persoane sau a datelor despre abonați, măsura de percheziție și confiscare a datelor informatice, dar și măsura de colectare în timp real a datelor informatice.

În anul 2016, prin proiectul de lege nr. 161 din 13.04.2016, în scopul armonizării cadrului legal național cu reglementările internaționale care vizează securitatea informațională și investigarea criminalității cibernetice și a exploatării sexuale

[15] Hotărârea Guvernului nr. 347 din 01.06.2022 cu privire la aprobarea Programului național de protecție a copilului pentru anii 2022-2026 și a Planului de acțiuni pentru implementarea acestuia.

online a copiilor, au fost propuse modificări la o serie de prevederi legale, și anume: Codul penal, Legea cu privire la Serviciul de Informații și Securitate al Republicii Moldova, Codul de procedură penală, Legea comunicațiilor electronice, Codul contravențional etc. Cu toate acestea, acest proiect a fost criticat, considerându-se că unele prevederi ar fi putut afecta libertatea de exprimare și dreptul la viață privată. La 14 iunie 2018, acesta a fost retras de la examinarea în Parlament.

În anul 2020, Legea nr. 20-XVI din 03.02.2009 privind prevenirea și combaterea criminalității informatice a fost completată cu art. 7 lit. e1) privind eliminarea și blocarea accesului la conținutul infracțional, care este atribuit și materialelor ce reprezintă exploatarea sexuală a copilului. Potrivit legii, furnizorii de servicii se obligă „să oprească" accesul din propriul sistem informatic la toate adresele IP pe care se află pagini web, inclusiv cele găzduite de furnizor, care contribuie astfel la săvârșirea de infracțiuni sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modalitatea de comitere a acestora".

Blocarea conținutului ilegal se realizează la cererea autorităților (Serviciul de Informații și Securitate, Agenția Națională de Reglementare pentru Comunicații Electronice și Tehnologia Informației sau poliția). Legea nr. 20-XVI din 03.02.2009 la art. 7 reglementează obligațiile furnizorilor de servicii legate de prevenirea și combaterea criminalității cibernetice. Una dintre responsabilitățile acestora este de a opri accesul la toate adresele IP pe care se află pagini web, inclusiv cele găzduite de furnizor, care contribuie la comiterea de infracțiuni sau la încălcarea legii.

Industria nu are obligația de a verifica sau de a monitoriza conținutul partajat sau stocat pe serverele sale, deoarece acest lucru este considerat o intruziune în viața privată și o limitare a libertății de exprimare. În conformitate cu Legea nr. 284/2004 privind comerțul electronic, art. 15 alin. 1, furnizorul de servicii nu este responsabil pentru informațiile transmise prin intermediul rețelei de comunicații electronice. Mai mult, furnizorul de servicii nu este responsabil pentru stocarea automată, intermediară și temporară a informațiilor transmise și trebuie să acționeze cu promptitudine pentru a elimina informațiile care au fost stocate sau pentru a bloca accesul la acestea de îndată ce ia cunoștință de faptul că accesul la aceste informații transmise a fost eliminat, accesul la acestea a fost blocat sau că o autoritate publică a autorizat eliminarea sau blocarea informațiilor.

De asemenea, legislația națională stipulează că societățile de găzduire nu răspund la informațiile stocate pe serverele lor, cu excepția cazurilor în care furnizorul de servicii știe că activitatea sau informațiile stocate sunt ilegale sau are cunoștință de circumstanțe care indică faptul că activitatea informațiilor este ilegală. Odată ce compania de găzduire este informată despre activitatea ilegală sau despre informațiile stocate pe serverele sale, este obligată să acționeze prompt pentru a elimina sau a bloca accesul la acestea.

Furnizorul de servicii poate fi informat cu privire la conținutul ilegal stocat pe serverele sale prin intermediul:

- unei dispoziții scrise din partea unei instanțe sau a unei autorități publice care să ateste caracterul ilegal al informațiilor sau al activității stocate pe serverele furnizorului de servicii;
- unei notificări scrise (în original) din partea unei persoane interesate, care declară pe propria răspundere că o activitate sau o informație care este stocată pe serverele furnizorului de servicii este ilegală;

Furnizorii de servicii de internet și companiile de găzduire sunt obligate să informeze Ministerul Afacerilor Interne cu privire la materialele de ademenire (grooming) sau de abuz sexual asupra copiilor realizate prin intermediul serviciilor furnizate. De asemenea, la cererea Ministerului Afacerilor Interne, a Serviciului de Informații și Securitate și a Procuraturii Generale, furnizorii de servicii sunt obligați să furnizeze informații care să permită identificarea utilizatorilor, destinatarii serviciilor cu care acești furnizori au încheiat contracte privind stocarea permanentă a informațiilor. Aceste informații pot fi solicitate numai în cazul în care aceștia dispun de dovezi care conduc la concluzia că serviciile oferite de furnizor sunt utilizate pentru a desfășura activități ilegale.

În ultimii ani, autoritățile naționale au promovat autoreglementarea, ca abordare pentru prevenirea și combaterea abuzului sexual asupra copiilor și a exploatării sexuale a acestora pe internet. Astfel, conform Legii nr. 30 din 07.03.2013, art. 5 alin (8), furnizorii de servicii ar trebui să ofere utilizatorilor posibilitatea de a instala aplicații de filtrare a conținutului cu impact negativ asupra copiilor și ar trebui să includă pe site-urile lor un capitol referitor la siguranța online. De obicei, utilizatorii trebuie să plătească pentru aceste servicii o taxă suplimentară, iar filtrarea nu se face automat pentru toți utilizatorii, implicit.

3.3. Practicile din sectorul TIC

Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației a aprobat un set de recomandări privind autoreglementarea serviciilor de filtrare a conținutului online care poate avea un impact negativ asupra copiilor, furnizate de către furnizorii de servicii de internet sau de servicii de comunicații electronice.[16] De asemenea, ISP au fost încurajați să mediatizeze programele de filtrare pe site-urile lor.

Companiile TIC au oferit mai multe opțiuni pentru filtrarea conținutului și monitorizarea activității copiilor online. Kaspersky safe kids a fost una dintre opțiunile menționate de către industrie. Din păcate, numărul de solicitări din partea

[16] https://www.anrceti.md/files/filefield/HCA%20nr.%2015%20din%2004.05.2018.pdf

părinților a fost foarte mic, ceea ce arată o lipsă de înțelegere a riscurilor specifice la care pot fi expuși copiii lor și a valorii adăugate a programelor de control parental. În prezent, acest program de control parental nu mai este disponibil pentru Moldova, deoarece parteneriatul cu Kaspersky a încetat. Una dintre companiile participante la întâlnirile bilaterale a menționat inițiativa lor de a oferi programe de control parental, care a necesitat autorizarea din partea Centrului Național pentru Protecția Datelor cu Caracter Personal, dar nu a fost autorizată. Din motive de securitate, ISP oferă, de asemenea, software antivirus și aplicații pentru filtrarea conținutului, contra cost, la cererea utilizatorului.

Au fost stabilite obligații specifice pentru instituțiile de învățământ. Standardele minime pentru dotarea școlilor primare, gimnaziale și liceale cu mijloace TIC reglementează obligația instituțiilor de învățământ de a dispune de software specializat pentru filtrarea conținutului de pe internet.[17] Deși este reglementată obligația de a dispune de software specializat pentru filtrarea conținutului pe internet în școlile primare, gimnaziale și liceale, această normă nu este implementată în toate școlile.

Industria din Republica Moldova nu utilizează niciun instrument de detectare a conținutului și a comportamentelor ilegale. Companiile TIC răspund, de obicei, la cererea poliției și nu iau măsuri proactive pentru a combate exploatarea sexuală a copiilor online. Companiile nu dispun de politici de securitate by-design sau de alte orientări care vizează combaterea conținutului ilegal online.

Companiile de telecomunicații nu aplică nicio măsură de siguranță obligatorie în ceea ce privește copiii. Chiar dacă acestea vând dispozitive telefonice, responsabilitatea pentru utilizarea dispozitivului revine părinților sau persoanei care a cumpărat dispozitivul. De asemenea, nu au fost luate inițiative pentru a evalua vârsta clienților sau pentru a colecta date despre utilizatorii finali ai dispozitivelor.

Companiile private de TIC au inclus securitatea clienților, a adulților și a copiilor în politicile lor de responsabilitate socială. Chiar dacă subiectul este perceput ca fiind opțional, fiind mandatul și responsabilitatea departamentului de RSI, nu a întregii companii. În unele cazuri, personalul unei companii TIC private nici măcar nu știa dacă politica sa de RSI reflectă măsuri de siguranță online pentru copii. Cu toate acestea, au fost identificate câteva exemple bune de implicare a sectorului TIC în prevenirea riscurilor online, cum ar fi organizarea de evenimente de sensibilizare cu privire la siguranța online a copiilor sau educația digitală și codarea/robotica pentru copii.

---

[17] MECR nr. 581 din 24.06.2015 privind aprobarea Standardelor minime pentru dotarea școlilor primare, gimnaziilor și liceelor cu mijloace TIC.

4. Definiții

Bariera lingvistică este o problemă frecventă atunci când se încearcă orice fel de discuție sau comparație internațională în numeroase domenii de politici publice. Cu toate acestea, obstacolele lingvistice pot, de asemenea, să reflecte sau să aibă adesea rădăcini în tradiții sau norme culturale și juridice diferite. Domeniul politicii de protecție online a copiilor nu face excepție. Două persoane care au o înțelegere comună și profundă a principalelor caracteristici ale unei probleme pot discuta împreună despre aceasta în cadrul a ceea ce fiecare dintre ele consideră a fi parametri bine definiți, doar pentru a descoperi că există diferențe importante, nuanțate, care pot conta foarte mult atunci când încearcă să folosească cuvântul scris sau vorbit pentru a descrie problema sau concluziile sau rezultatele dorite.

Astfel, un punct de referință cheie pentru orice discuție despre politica viitoare în Republica Moldova în ceea ce privește abuzul sexual asupra copiilor și exploatarea sexuală a copiilor trebuie să fie definițiile oferite de tratatele și convențiile internaționale relevante, unde, în mod obișnuit, se depune mult efort și timp pentru a produce traduceri convenite, menite în mod expres să armonizeze intrările și ieșirile politicii. Aceste tratate și convenții vor fi menționate în diferite puncte ale prezentului raport, în funcție de context.

4.1. Liniile directoare de la Luxemburg

În plus, sub auspiciile și conducerea INTERPOL și ECPAT International, Liniile directoare de la Luxemburg au fost elaborate de o coaliție neobișnuit de largă de agenții de aplicare a legii, de protecție a copilului, de agenții de bunăstare a copilului, de cadre universitare și de organisme guvernamentale și interguvernamentale interesate de sănătatea, siguranța și bunăstarea copiilor în lumea online. Liniile directoare de la Luxemburg oferă un context cuprinzător pentru o mare parte din terminologia utilizată în prezent sau recent. La momentul redactării acestui document (decembrie 2022), Liniile directoare sunt în curs de revizuire și actualizare pentru a ține seama de schimbările recente din domeniul tehnologiei, dar și în legătură cu înțelegerea noastră mai bună a modului în care se manifestă sau se comite abuzul sexual asupra copiilor online. Cu toate acestea, este posibil ca mulți să găsească în continuare utile și informative orientările actuale.

După cum s-a menționat mai sus, prezentul raport se concentrează asupra exploatării sexuale a copiilor sub două forme principale, provocările legate de imagine și manipularea sexuală a copiilor.

4.2. Provocări legate de imagine

Este unanim înțeles și acceptat faptul că CSAM constă în imagini fixe sau video ale oricărei persoane sub 18 ani implicate în activități sexuale reale sau simulate.[18] În mod obișnuit, în prezent, pseudo-imaginile sunt tratate ca și cum ar fi reale.[19] În definiția CSAM pot fi incluse și reprezentări audio și alte tipuri de reprezentări non-fotografice, de exemplu, desene și schițe.[20] De asemenea, este unanim înțeles și acceptat faptul că, indiferent de vârsta de consimțământ sexual, CSAM nu ar trebui să fie publicate sau distribuite[21] și, de asemenea, este o infracțiune deținerea unor astfel de imagini.[22]

Faptul că posesia este o infracțiune are o importanță fundamentală. Dacă simpla posesie este o infracțiune, rezultă că nicio entitate juridică sau de altă natură nu ar trebui să ajute sau să permită cu bună știință ca cineva care utilizează serviciile sau proprietatea sa să le stocheze sau să le transmită. Până în prezent, o provocare majoră a fost modul în care se poate face acest lucru la scară largă. Această problemă a fost rezolvată prin dezvoltarea și implementarea unei serii de instrumente tehnice.[23]

4.3. Imagini autogenerate

Recent, în multe jurisdicții, s-a înregistrat o creștere semnificativă a fenomenului „imaginilor autogenerate", fotografii sau videoclipuri care par să fi fost create în mod voluntar de un copil care acționează singur. Cu toate acestea, este probabil ca cel puțin o parte dintre acestea să fi fost generate în urma unui proces de ademenire sau să fie rezultatul unei coerciții. Din aceste motive, chiar dacă imaginile vor fi totuși ilegale, este important să se țină seama de acest context atunci când se decide cum să se abordeze și să se ajute cel mai bine copilul. Copilul este în continuare o victimă.

---

[18] Articolul 20.2. Convenția de la Lanzarote.
[19] Convenția de la Budapesta Articolul 9,2, c.
[20] ibid.
[21] Sunt permise excepții în scopuri educaționale, medicale sau de aplicare a legii legitime sau în cazul în care persoanele din imagine au depășit vârsta de consimțământ sexual și au consimțit ca imaginea să fie deținută în mod privat. Articolul 3 20.3, Convenția de la Lanzarote.
[22] A se vedea capitolul de mai jos **Cadrul juridic și politic internațional.**
[23] A se vedea capitolul de mai jos **Cadrul juridic și politic internațional.**

4.4. Ademenirea

Exploatarea sexuală a copiilor pe internet nu se limitează doar la aspecte legate de imagine. Există, de asemenea, provocarea reprezentată de „grooming", denumită uneori și „ademenire".[24] Aceasta se referă la procesele prin care, de obicei, un copil care nu are vârsta de consimțământ sexual este ademenit sau presat să intre într-o relație care are ca rezultat întâlnirea în lumea fizică pentru a se angaja într-un comportament sexual ilegal sau pentru a desfășura acte sexuale online. În acest din urmă caz, deoarece aceste acte au loc online, ele pot fi înregistrate și transformate în CSAM care este ulterior publicat sau distribuit fără consimțământul sau chiar fără știrea copilului.[25] Autorul infracțiunii sexuale va fi adesea un adult, dar este, de asemenea, din ce în ce mai frecvent ca acesta să fie un alt copil.[26]

---

[24] Orientările de la Luxemburg, p. 52, H. 4. ii.

[25] În orice caz, un copil nu poate fi niciodată de acord cu crearea, publicarea sau distribuirea de CSAM.

[26] https://defendinnocence.org/child-sexual-abuse-risk-reduction/sexual-development-at-all-ages/concerning-behavior/5-facts-child-child-sexual-abuse/

5. Context istoric[27]

Dacă ar trebui să alegem un „an zero" pentru internetul modern, am putea spune că acesta ar fi 1995.[28] După cum arată multe grafice, în 1995 a început creșterea explozivă a utilizării internetului în țările OCDE.[29] Națiunile mai puțin bogate nu au rămas prea mult în urmă, iar astăzi internetul este din ce în ce mai bine integrat în viața publică, privată și de afaceri a fiecărei țări.

Dar de ce 1995 ca Anul Zero? Acesta a fost anul în care Microsoft a integrat un browser web în Windows, pe atunci de departe cel mai utilizat sistem de operare din lume. Practic, acest lucru a făcut ca browser-ul să pară *„gratuit"*. Browser-ul s-a numit „Windows Explorer". Deoarece folosea o interfață grafică intuitivă, era suficient să dai clic cu mouse-ul pe o pictogramă pentru a face ceea ce majoritatea oamenilor aveau nevoie sau doreau să facă cu ajutorul calculatoarelor sau atunci când intrau pe internet. Nu mai era necesar să ai o diplomă în cibernetică sau să memorezi și să execuți comenzi obscure la o interogare DOS. Totul a devenit mai ușor, deschizând lumea internetului către un grup cu totul nou - publicul larg - și acest lucru s-a întâmplat cam în același timp în care prețurile hardware-ului și costurile de conectivitate au scăzut. La fel de important este faptul că vitezele de conectare s-au îmbunătățit substanțial, pe măsură ce modem-urile dial-up au început să fie înlocuite cu forme de bandă largă[30] . În loc să fie nevoie de o eternitate pentru a descărca o imagine statică, mică și granulată, cu o paletă limitată de culori, în curând, imagini în mișcare de bună calitate, cu sunet hifi, puteau fi vizualizate și stocate în câteva secunde. Acoperirea mediatică inexactă a internetului i-a făcut pe utilizatori să creadă în mod constant că sunt de negăsit,[31] ceea ce, la rândul său, a contribuit la ideea că internetul este un nou „Vest Sălbatic" complex, ale cărui calități aproape magice erau prost înțelese de guverne și de autoritățile de aplicare a legii. Acest lucru, la rândul său, a condus la o încredere în autoreglementare ca fiind cea mai bună modalitate de a face față provocărilor care au apărut după ce internetul a devenit un produs de consum de masă. Marile întreprinderi de internet au promis guvernelor că vor

[27] Pentru mai multe informații în acest sens, consultați Oxford University Press Handbook on Cyber Security, capitolul 23 „Online Child Safety" de John Carr.

[28] Unii ar putea susține 1957, anul în care a fost lansat „Sputnik". Aceasta a declanșat o investiție majoră în inovație tehnologică din partea guvernului american, din care a apărut în cele din urmă internetul.

[29] https://www.internetworldstats.com/emarketing.htm

[30] La început ADSL fiind cea mai comună.

[31] Această întrebare a revenit în actualitate odată cu discuțiile contemporane despre rolul criptării.

„rezolva" toate problemele care deveneau evidente, dacă acestea le vor permite să facă acest lucru. La început, această abordare părea să funcționeze, dar nu a trecut mult timp până când a devenit evident că, deși unele întreprinderi făceau eforturi de bună-credință, nu era cazul tuturor, și chiar și cele care făceau eforturi erau inconsecvente și lipsite de transparență. Dar toate acestea au fost pentru viitor.

„Child Safety on the Information Highway" (*Siguranța copiilor pe autostrada informațională)*[32] a fost publicat în 1994, cu puțin timp înainte de boom-ul care avea să înceapă în anul următor. A fost scrisă de Larry Magid, un jurnalist de tehnologie din Silicon Valley. Acesta avea să înființeze mai târziu „Connect Safely". La acea vreme, se presupunea că părinții vor aduce un singur calculator în casa familiei și le vor permite copiilor lor să îl folosească pentru a-și face temele sau pentru a se bucura de numărul încă limitat de site-uri web care deveneau disponibile.

Deoarece, în acele zile de început, mai mult de jumătate dintre utilizatorii de internet din lume se aflau în SUA,[33] publicația lui Magid s-a adresat în principal părinților americani, cu scopul de a-i ajuta să înțeleagă ce riscuri pentru copii deveneau deja evidente în noua lume virtuală pe care internetul o crea. Cu toate acestea, domeniile, pe care Magid le-a identificat ca fiind îngrijorătoare pentru părinții americani în 1994, sunt încă în atenția părinților din întreaga lume în prezent:

- Bullying (intimidare);
- expunerea la materiale neadecvate vârstei și dăunătoare.

Astăzi am adăuga preocupări legate de:

- utilizarea excesivă;
- exploatarea comercială;
- confidențialitate;
- informare eronată și dezinformare.

Fiecare dintre aceste subiecte continuă să fie extrem de important în contextul elaborării unei strategii sau abordări naționale cuprinzătoare a tuturor aspectelor legate de siguranța și bunăstarea online a copiilor. Un studiu internațional de anvergură, EU Kids Online,[34] realizat de London School of Economics and Political Science, a subliniat, de asemenea, că, din perspectiva copiilor, există o gamă largă de aspecte care îi preocupă pe copii și care depășesc cu mult simpla abordare a conținutului infracțional și a abuzurilor infracționale. Cu toate acestea, cu excepția cazului în care se face referire în mod limitat în text, chestiunile de acest tip depășesc sfera de aplicare a prezentului raport. După cum s-a menționat deja, cercetările efectuate cu copii din Republica Moldova au reflectat foarte mult constatările internaționale din studiul LSE.[35]

---

[32] https://www.safekids.com/child-safety-on-the-information-highway/.
[33] https://www.internetworldstats.com/emarketing.htm
[34] https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online
[35] https://lastrada.md/pic/uploaded/COS%20Research%202021_summary.pdf

Ademenirea (grooming) a fost denumită de Magid *„molestare fizică”,* iar mass-media s-a concentrat atunci foarte mult pe „pericolul străinului”, deşi, de fapt, majoritatea abuzurilor sexuale asupra copiilor sunt şi au fost întotdeauna comise de membri ai familiei sau de alte persoane aflate în contact apropiat şi de încredere cu copilul victimă.[36, 37]

Ceea ce *nu* a figurat în mod proeminent în activitatea de pionierat a lui Magid a fost un accent major pe CSAM. O parte din CSAM a fost creată atunci ca rezultat al activităţii de ademenire, dar ideea este că, la acea vreme, aceasta nu a fost înregistrată ca o problemă majoră sau distinctă în SUA. Acest lucru avea să vină în curând, dar mai târziu. Primele linii telefonice de urgenţă[38] din lume au fost înfiinţate în 1995-1996 în Olanda, Norvegia şi Regatul Unit, unde o serie de cazuri au beneficiat de o acoperire mediatică substanţială. Statele Unite ale Americii şi-au înfiinţat linia telefonică directă în 1998.[39]. Asociaţia internaţională a liniilor telefonice de urgenţă, INHOPE, a fost înfiinţată în 1999 cu finanţare din partea UE.[40] INHOPE joacă un rol important în stabilirea şi monitorizarea standardelor operaţionale şi în colectarea rapoartelor de la liniile fierbinţi din întreaga lume, eliminând dublurile şi transmiţându-le către INTERPOL.

5.1. Creşterea ponderii CSAM şi a altor forme de abuz sexual asupra copiilor online

În primele zile ale internetului, cea mai mare parte a CSAM a fost distribuită prin intermediul grupurilor de ştiri Usenet, FTP, IRC şi tehnologii similare care au precedat web-ul mondial.[41] Bulletin Boards şi e-mailul au jucat, de asemenea, un rol important, iar mai târziu reţelele peer-to-peer au devenit, de asemenea, proeminente.[42] Darknet sau Darkweb este o altă sursă importantă de CSAM,[43] dar, deşi este imposibil de dovedit într-un fel sau altul, este foarte probabil ca orice CSAM care apare sau este distribuit pe Darknet să fi provenit sau să fi ajuns pe internetul „deschis”. Mulţi sunt de părere că investigaţiile privind abuzurile asupra copiilor pe Darknet şi pe reţelele Peer-to-Peer ar trebui să fie în principal de competenţa organelor de aplicare a legii[44] şi nu a furnizorilor individuali de servicii electronice şi, prin urmare, nu intră în sfera de aplicare a prezentului raport.

---

[36] https://www.csacentre.org.uk/resources/key-messages/intra-familial-csa/#the-prevalence-of-intra-familial-csa

[37] https://www.ywca.org/wp-content/uploads/WWV-CSA-Fact-Sheet-Final.pdf

[38] O linie telefonică de urgenţă este un mecanism de primire a rapoartelor privind CSAM şi de asigurare a eliminării acestora de pe internet.

[39] https://www.missingkids.org/gethelpnow/cybertipline

[40] https://www.inhope.org/EN/articles/annual-reports INHOPE are în prezent 50 de linii telefonice de urgenţă în 46 de ţări. O linie telefonică de urgenţă este în curs de înfiinţare în Republica Moldova.

[41] Web-ul mondial a apărut la CERN în 1990, iar primele browser-e web uşor accesibile publicului au apărut în 1993.

[42] https://inhope.org/EN/articles/what-are-peer-to-peer-networks

[43] https://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites

[44] https://www.vice.com/en/article/bvzxww/europol-took-down-dark-web-child-porn-site-boystown

În primele zile, numărul de imagini găsite și raportate era relativ mic. În 2008, de exemplu, numărul de raportări făcute la cea mai mare linie telefonică de urgență din Europa, Internet Watch Foundation din Marea Britanie, a fost de numai 33 947, în ușoară scădere față de anul precedent.[45] Recent, în 2017, INHOPE, cu membri în 43 de țări, a raportat că membrii săi au procesat 259 000 de rapoarte confirmate.[46] Chiar dacă Republica Moldova nu este membră a INHOPE, NCMEC, una dintre cele mai mari linii de asistență telefonică membre ale INHOPE, a înregistrat în perioada 2019-2020 un număr de 16 509 rapoarte care indică încărcarea de CSAM din Republica Moldova. Cu toate acestea, fiecare țară își aplică propriile legi naționale atunci când evaluează conținutul raportat, astfel încât aceste cifre nu indică nivelul de abuz sexual asupra copiilor într-o anumită țară.[47]

În ianuarie 2017 a apărut o schimbare de situație, grație Centrului canadian pentru protecția copilului. Într-o perioadă de șase săptămâni, Proiectul Arachnid a scanat proactiv 230 de milioane de pagini web, identificând 5,1 milioane de pagini web unice care găzduiesc CSAM, detectând în acest proces peste 40 000 de imagini unice.[48] În prezent, canadienii identifică 80 000 de noi imagini unice în fiecare lună.[49] Operațiunile la această scară și cu această viteză au devenit posibile deoarece Centrul canadian a îmbinat tehnologia de căutare pe internet cu o bază de date cu hash-uri de CSAM deja cunoscute.[50] De atunci, pe bază de voluntariat, liniile telefonice de urgență britanice, americane și altele au copiat exemplul canadienilor și folosesc tehnici proactive similare, dar, în mod esențial, la fel au făcut și numeroase companii de tehnologie. În 2021, NCMEC a primit 29 397681 de rapoarte care conțineau încă 39,9 milioane de imagini, dintre care 16,9 milioane erau unice, și 44,8 milioane de videoclipuri, dintre care 5,1 milioane erau unice. 1.800 de companii sunt înregistrate pentru a raporta la NCMEC, iar numele fiecărei companii care face un raport este publicat pe site-ul web al NCMEC.[51]

Este posibil ca măsurile Covid și restricțiile să fi avut un anumit efect în ceea ce privește creșterea acestor cifre, dar este la fel de clar că avem de-a face cu un model de comportament stabilit de mult timp. Din aceste date se poate observa că volumele de CSAM în circulație sunt substanțiale și nu se reduc. Indiferent de ceea ce ar fi trebuit să facă autoreglementarea, este clar că aceasta nu a funcționat suficient de bine, suficient de rapid sau suficient de consecvent, și tocmai de aceea se dezvoltă acum noi abordări politice. Accentul se deplasează spre a face proactivitatea obligatorie.

---

45 https://www.iwf.org.uk/media/wbzeqk2h/2008-annual-report.pdf

46 https://www.inhope.org/media/pages/articles/annual-reports/a90273c07e-1647828763/inhope-annual-report-2017.pdf

47 https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-country.pdf

48 https://www.cbc.ca/news/canada/manitoba/project-arachnid-cybertip-child-sexual-abuse-1.3938998

49 https://www.protectchildren.ca/pdfs/C3P_Arachnid_PressKit_en.pdf

50 Hash-urile au fost create cu ajutorul PhotoDNA. Consultați secțiunea privind instrumentele de detectare și raportare din acest raport.

51 https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

5.2. Victimele

Circulația continuă a CSAM nu este doar o infracțiune în sine, ci și o încălcare gravă a dreptului copilului la intimitate și la demnitate umană. Aceasta expune victima descrisă la riscul de a fi abuzată și în măsura în care încurajează sau susține activitatea sau rețelele de pedofilie, reprezintă, de asemenea, o amenințare pentru alți copii din întreaga lume. În plus, faptul de a ști că imaginile CSAM ale dumneavoastră circulă pe internet, putând fi văzute de oricine și de toată lumea, se adaugă și agravează răul deja provocat de actele abuzive inițiale. Din acest motiv, victimele abuzurilor în cazul în care imaginile au fost publicate online au început să devină mai vocale atât în ceea ce privește natura răului care le-a fost făcut, cât și importanța localizării cât mai rapide a imaginilor și a înlăturării lor de pe domeniul public.[52] Astfel, deși niciun furnizor de servicii electronice nu ar dori să facă nimic pentru a îngreuna identificarea și arestarea de către organele de aplicare a legii a oricărei persoane identificate în lanțul de infractori, aceasta este o chestiune complet diferită de provocarea de a asigura eliminarea inițială cât mai repede posibil. Copiii nu ar trebui să fie obligați să aștepte până când poliția are timp de căutare, pentru a-i face să fie mai în siguranță.

O altă caracteristică esențială a imaginilor găsite online este faptul că victimele sunt din ce în ce mai tinere, unele sunt bebeluși sau copii mici, iar infracțiunile comise împotriva lor sunt din ce în ce mai violente și mai extreme.[53]

După cum s-a menționat mai sus, a existat, de asemenea, o creștere semnificativă a ceea ce pare a fi imagini „autogenerate" care au ajuns pe internet. Deși pare foarte probabil ca o parte din imaginile considerate „autogenerate" să fie, de fapt, produsul unei constrângeri sau manipulări, în special dacă victimele sunt copii foarte mici, nu există nicio îndoială că multe dintre ele au fost produse în mod complet consensual, prezentând forme de comportament offline adecvate din punctul de vedere al dezvoltării, ca o modalitate de a-și arăta dragostea sau afecțiunea pentru cineva care crede că este prietenul sau prietena sa. Astfel, chiar dacă imaginea, din punct de vedere tehnic, este ilegală și trebuie să fie scoasă din domeniul public, copiii implicați nu ar trebui să fie atrași în justiția penală și ar trebui, în schimb, să fie ajutați să înțeleagă riscurile și pericolele asociate cu producerea unor astfel de imagini.

Pe măsură ce disponibilitatea benzii largi a devenit tot mai răspândită, a crescut și numărul de transmisiuni în direct a activităților de abuz sexual asupra copiilor.[54] În acest caz, de obicei, copiii din țara A, unde există un nivel ridicat de sărăcie, sunt plătiți de cineva din țara B, mai bogată, pentru a desfășura acte sexuale în direct, pentru ca persoana din țara B să le vadă sau chiar să le dirijeze. În Filipine, în perioada de izolare din martie până în mai 2020, a fost raportată o creștere de 256% a cazurilor de transmisiune în direct. Întrucât majoritatea transmisiunilor în direct au loc în cadrul unor fluxuri criptate, acest lucru complică substanțial problema detectării și a interdicției.

---

[52] https://projectarachnid.ca/en/phoenix11-advocacy-statement/
[53] https://annualreport2021.iwf.org.uk/trends/
[54] https://www.weprotect.org/issue/livestreaming/

6. Instrumente de detectare și raportare

Există două clase de instrumente care sunt cel mai frecvent utilizate de furnizorii de servicii electronice în ceea ce privește protecția online a copiilor. Una dintre clase se referă la CSAM. Cealaltă se referă la ademenire (grooming).

6.1. Instrumente de abordare a CSAM

Există două tipuri de imagini care sunt de interes în această categorie. Primul este reprezentat de imaginile care au fost deja văzute și clasificate ca fiind CSAM de către o autoritate competentă. Al doilea este reprezentat de imagini care nu au fost încă clasificate, dar care sunt susceptibile de a fi CSAM. În mod obișnuit, este probabil ca acestea să fie imagini mai noi, ceea ce sugerează posibilitatea ca copilul reprezentat să fi fost abuzat recent și, prin urmare, să fie subiectul unui abuz continuu. Acest lucru sporește importanța localizării acelui copil și a obținerii ajutorului de care are nevoie pentru a scăpa de situația abuzivă și pentru a se recupera de efectele negative ale acesteia.

În ceea ce privește imaginile care au fost deja clasificate ca fiind CSAM, în mod tradițional, autoritățile de aplicare a legii și companiile individuale au folosit o varietate de forme de hash-uri[55] pentru a le permite să identifice repetări ale imaginii fără a fi nevoie să intervină manual pentru a căuta din nou. Acest lucru economisește timp și bani și, de asemenea, îi scutește pe indivizi de stresul de a fi nevoiți să caute.

Problema era că, dacă cineva edita sau modifica chiar și cel mai mic detaliu al imaginii sau, de exemplu, îi schimba formatul, aceasta devenea un fișier complet nou. Hash-ul original nu-i mai corespundea. În 2009, Microsoft a lansat PhotoDNA,[56] care folosea o tehnică de distribuire perceptuală pentru a elimina această problemă, cu o rată de eroare estimată la aproximativ 1 la 50 de miliarde.[57] Corelarea PhotoDNA cu tehnologia de crawling este ceea ce a făcut posibil experimentul canadian și a generat volumul substanțial de rapoarte primite de NCMEC menționat mai sus.[58]

---

[55] Orice element care poate fi stocat sau transmis de un computer trebuie să fie digital. Aceasta înseamnă că este alcătuit dintr-un anumit model sau colecție de 1 și 0. Un hash utilizează o formulă matematică pentru a reprezenta analiza și acel model.

[56] https://www.microsoft.com/en-us/photodna

[57] https://www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf

[58] Secțiunea privind *creșterea CSAM și a altor forme de abuz sexual asupra copiilor online.*

Instrumente similare au fost dezvoltate acum de alte companii și organizații.[59] Acestea pot permite companiilor să detecteze la scară largă imaginile ilegale deja cunoscute și clasificate, împiedicând reîncărcarea acestora sau, alternativ, să găsească rapid astfel de imagini în cazul în care acestea s-au strecurat deja prin plasă sau erau deja prezente înainte de lansarea noii abordări.

Înainte ca o imagine să intre într-o bază de date ADN sau în alte baze de date similare, standardul industrial prevede acum că aceasta trebuie să fie verificată de cel puțin trei persoane. Acest lucru este menit să asigure că doar conținutul ilegal ajunge în baza de date, dar a creat o problemă cu o întârziere substanțială.[60] O serie de linii telefonice de urgență și altele colaborează pentru a reduce numărul de întârzieri.

În plus, în fiecare zi apar noi imagini. Acest lucru înseamnă că acestea nu se pot regăsi în nicio bază de date existentă, astfel încât PhotoDNA și altele similare nu le pot detecta. În prezent, au fost dezvoltate instrumente care pot identifica imagini noi și pot determina dacă este posibil să fie sau nu CSAM. Aceste instrumente se numesc „clasificatoare". În cazul în care un clasificator detectează o imagine, aceasta poate fi scoasă din linia de clasificare și trimisă pentru analiză umană, astfel încât să se poată lua o decizie cu privire la posibilitatea de a permite sau nu publicarea sau distribuirea ei. În cazul în care se decide să nu se permită publicarea sau distribuirea imaginii, aceasta va fi trimisă pentru o examinare umană în cadrul procesului „celor trei perechi de ochi" menționat anterior.

6.2. Instrumente de abordare a ademenirii (grooming)

După cum s-a menționat mai sus, ademenirea se referă la procesele prin care, de obicei, un copil care nu are vârsta consimțământului sexual este ademenit sau presat să intre într-o relație care are ca rezultat întâlnirea în lumea fizică pentru a se angaja într-un comportament sexual ilegal sau pentru a efectua acte sexuale online[61]. În acest din urmă caz, tocmai pentru că aceste acte au loc online, ele pot fi înregistrate și transformate în CSAM, care este ulterior publicat sau distribuit fără consimțământul sau chiar fără știrea copilului.[62]

Din cauza diferențelor mari în ceea ce privește definițiile juridice aplicate în ceea ce privește ademenirea, nu există statistici cuprinzătoare care să permită realizarea unor comparații internaționale fiabile. Cu toate acestea, de exemplu, datele NCMEC pentru anul 2021 au arătat că a primit rapoarte privind 44 155 de cazuri de ademenire online în vederea unor acte sexuale și 12 458 de rapoarte privind molestarea sexuală a copiilor.[63]

---

[59] https://www.thorn.org/blog/safer-impact-report/
[60] https://globalnews.ca/news/8517340/online-tool-cracks-down-on-child-sexual-abuse-images/
[61] A se vedea capitolul de mai jos privind **Cadrul juridic și politic internațional.**
[62] În orice caz, un copil nu poate fi niciodată de acord cu crearea, publicarea sau distribuirea de CSAM.
[63] https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

În cadrul legislației aflate în curs de adoptare la nivelul Uniunii Europene, un nou centru european va stabili o listă aprobată de instrumente care respectă viața privată și care pot fi utilizate în mod proactiv pentru a detecta CSAM, pentru a detecta imaginile susceptibile de a fi CSAM și pentru a detecta activitățile de ademenire.[64]

6.3. Implementarea

În mod evident, pentru ca instrumentele de tipul celor descrise mai sus să poată fi utilizate, un ESP trebuie mai întâi să dobândească codul sau programele necesare. Unele dintre acestea vor fi la un cost redus sau chiar gratuit pentru o licență. Costurile mai mari vor fi asociate cu integrarea sistemelor într-o infrastructură existentă sau vor apărea din necesitatea de a adapta această infrastructură, de a forma personalul și de a gestiona procesele asociate cu utilizarea instrumentelor.

O parte din procesele asociate fiecăruia dintre cele trei tipuri diferite de instrumente vor aborda dimensiunile de raportare. Acestea ar putea fi fie în ceea ce privește escaladarea lor pentru a fi analizate și pentru a se lua măsuri în cadrul întreprinderii, fie în ceea ce privește raportarea lor către o agenție externă, de exemplu, către autoritățile de aplicare a legii.

În ceea ce privește în mod specific imaginile, în mod obișnuit, va exista un organism, cum ar fi o linie telefonică de urgență, care va fi autorizat să primească rapoarte, să confirme că imaginile sunt într-adevăr ilegale înainte de a emite o notificare prin care se solicită tuturor ESP-urilor din jurisdicție să le șteargă și, în același timp, să informeze atât rețeaua globală de linii telefonice de urgență, cât și agenția de poliție relevantă. Republica Moldova nu are în prezent o linie telefonică de urgență, dar aceasta este în curs de înființare. Se preconizează că aceasta va fi operațională la începutul anului 2023.

Instrumentele care pot detecta comportamente de ademenire se bazează, de obicei, pe analiza unor anumite tipare de cuvinte sau a altor forme de comportament, de exemplu, cereri neobișnuite de prietenie. În acest caz, măsurile care ar putea fi necesare sunt probabil mai complexe, de la un simplu avertisment adresat uneia sau mai multor părți sau o sesizare a organelor de aplicare a legii, sau chiar ambele. Unele linii telefonice de urgență acceptă, de asemenea, sesizări privind presupusele cazuri de manipulare. Altele nu. În Republica Moldova, o linie telefonică de urgență deja existentă acceptă raportări cu privire la manipularea sexuală.[65]

---

[64] A se vedea capitolul de mai jos privind **Cadrul juridic și politic internațional.**
[65] www.siguronline.md

6.4. Provocarea criptării

Datele NCMEC confirmă faptul că un număr mare de imagini CSAM sunt schimbate prin intermediul aplicațiilor de mesagerie necriptate deținute de Meta, în special Facebook Messenger și Instagram. În schimb, WhatsApp, deținută tot de Meta, nu generează aproape niciun raport, dar, în acest caz, WhatsApp este deja criptat. Principala aplicație de mesagerie a Apple este deja criptată și, de asemenea, nu generează aproape niciun raport de schimb de CSAM. Apple a recunoscut că aceasta este o problemă și a publicat un plan de introducere a scanării pe partea clientului ca modalitate de rezolvare a acesteia. Aceasta ar implica scanarea conținutului de pe dispozitiv înainte de a intra în fluxul criptat. În decembrie 2022, în timp ce anunța o serie de măsuri suplimentare de protecție a copiilor, Apple a anunțat că nu intenționează să pună în aplicare planul său inițial în ceea ce privește scanarea. Motivele acestei decizii rămân neclare, dar poate că cel mai important lucru de remarcat este că Apple nu a spus că soluția lor anterioară nu funcționează într-un mod care să protejeze confidențialitatea.[66]

Nu intră în sfera de aplicare a prezentului raport discutarea provocărilor asociate cu disponibilitatea și utilizarea pe scară largă a criptării în aplicațiile de mesagerie în masă, dar ar putea fi util de remarcat că, de exemplu, abordarea avută în vedere de Regatul Unit și UE ar fi aceea de a lăsa la latitudinea proprietarilor aplicațiilor să demonstreze că au găsit modalități de a permite utilizarea criptării în moduri care, protejând în același timp algoritmii de criptare, nu pun copiii în pericol.

[66] https://www.forbes.com/sites/emmawoollacott/2022/12/09/apple-expands-icloud-encryption-moves-away-from-client-side-scanning/

7. Cadrul juridic și politic internațional

În această secțiune sunt analizate publicațiile și recomandările mai multor organisme internaționale și ale mai multor instrumente juridice sau de altă natură. Gradul de convergență dintre acestea este foarte frapant. Experiența comună a copiilor și a familiilor din întreaga lume în ceea ce privește utilizarea internetului și a tehnologiilor digitale asociate a fost motorul care a produs această convergență.

7.1. Organizația Națiunilor Unite

Convenția ONU cu privire la drepturile copilului este instrumentul juridic fundamental, care a fost semnat de aproape toate țările din lume, inclusiv de Moldova.[67] De când a fost adoptată, nu au existat adăugiri sau modificări substanțiale la CNUDC. Cu toate acestea, în 2021, Adunarea Generală a adoptat Comentariul general 25, care a oferit sfaturi detaliate cu privire la modul de interpretare a CNUDC și a protocoalelor sale în contextul apariției internetului și a tehnologiilor digitale.[68]

7.2. Comentariul general 25 privind CNUDC

În 2009, UIT a publicat o serie de note de orientare, printre altele, pentru factorii de decizie politică și industrie și, cu ajutorul UNICEF, acestea au fost actualizate și revizuite în 2020.[69] Comentariul general 25 înlocuiește notele de consiliere ale UIT.

Printre altele, CNUDC și Comentariul general subliniază responsabilitatea juridică globală a guvernelor naționale de a asigura conducerea în domeniul politicii online privind copiii. Comentariul general subliniază, în special, că interesul superior al copilului este de o importanță preeminentă în stabilirea politicii în acest domeniu. Punctul 14 din secțiunea III C prevede:

„Statele părți ar trebui să ia toate măsurile adecvate pentru a proteja copiii de riscurile la adresa dreptului lor la viață, supraviețuire și dezvoltare. Riscurile legate de conținut, comportament și contract cuprind, printre altele, conținutul violent și sexual, agresiunea și hărțuirea cibernetică, jocurile de noroc, exploatarea și abuzul, inclusiv exploatarea și abuzul sexual..."

[67] UNCRC, semnată în ianuarie 1993, cele trei protocoale opționale în 2004, 2007 și 2010.
[68] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[69] https://www.itu.int/en/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protecion.aspx

În secțiunea B, punctul 24 și următoarele, apare următorul text:

< Statele părți ar trebui să se asigure că politicile naționale referitoare la drepturile copilului abordează în mod specific mediul digital și ar trebui să pună în aplicare reglementări, coduri industriale, standarde de proiectare și planuri de acțiune în consecință, toate acestea trebuind să fie evaluate și actualizate periodic. Astfel de politici naționale ar trebui să aibă ca scop să le ofere copiilor posibilitatea de a beneficia de implicarea în mediul digital și de a le asigura accesul în siguranță la acesta.

Protecția online a copiilor ar trebui să fie integrată în politicile naționale de protecție a copiilor. >.

În plus, secțiunea C, punctul 27, prevede că:

< Pentru a cuprinde consecințele transversale ale mediului digital asupra drepturilor copilului, statele părți ar trebui să identifice un organism guvernamental care să fie mandatat să coordoneze politicile, orientările și programele referitoare la drepturile copilului între departamentele guvernamentale centrale și diferitele niveluri de guvernare.[70] Un astfel de mecanism național de coordonare ar trebui să se angajeze cu școlile și cu sectorul tehnologiei informației și comunicațiilor și să coopereze cu întreprinderile, societatea civilă, mediul academic și organizațiile pentru a realiza drepturile copiilor în legătură cu mediul digital la nivel intersectorial, național, regional și local.[71] Acesta ar trebui să se bazeze pe expertiza tehnologică și pe alte expertize relevante din cadrul și din afara guvernului, după cum este necesar, și să fie evaluat în mod independent în ceea ce privește eficacitatea sa în îndeplinirea obligațiilor sale. >.

[70] Observația generală nr. 5 (2003), alin. 37.
[71] Ibidem, alin. 27 și 39.

8. Consiliul Europei

8.1. Consiliul Europei: Convenția de la Budapesta

Republica Moldova este semnatară a Convenției Consiliului Europei privind criminalitatea cibernetică (***Convenția de la Budapesta***).[72] Articolul 9 folosește un limbaj care acum pare a fi învechit, dar definește „pornografia infantilă" și, de asemenea, interzice utilizarea computerelor pentru producerea și distribuirea acesteia. Posesia de pornografie infantilă este, de asemenea, considerată o infracțiune și, după cum s-a menționat anterior, infracțiunea de posesie este o piatră de temelie a tuturor politicilor din acest domeniu.

8.2. Consiliul Europei: Convenția de la Lanzarote

Convenția Consiliului Europei privind protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale (***Convenția de la Lanzarote***[73]) a fost o convenție de referință de importanță globală, deoarece, pe baza Convenției ONU privind drepturile copilului și a protocoalelor sale adiționale, convenția a codificat și a solicitat statelor părți să incrimineze o serie de comportamente în vederea reducerii violenței sexuale împotriva copiilor. În plus, aceasta a oferit consiliere și îndrumare statelor părți cu privire la modul în care, în detaliu și în practică, acestea ar putea să-și îndeplinească obligațiile mai largi față de copii în contextul sănătății, bunăstării și dezvoltării personale a acestora, în special a copiilor care au fost victime ale violenței sexuale.

Un aviz interpretativ privind aplicabilitatea Convenției de la Lanzarote la infracțiunile sexuale împotriva copiilor facilitate prin utilizarea tehnologiilor informației și comunicațiilor (TIC) a fost adoptat de Comitetul de la Lanzarote în 2017.[74] Acesta stipulează că infracțiunile existente în Convenția de la Lanzarote rămân incriminate de legislația națională în același mod, indiferent de mijloacele utilizate de infractorii sexuali pentru a le comite, fie că sunt sau nu prin utilizarea TIC, chiar și atunci când textul Convenției de la Lanzarote nu menționează în mod specific TIC. De asemenea, la punerea în aplicare a Convenției de la Lanzarote, părțile ar trebui să asigure răspunsuri adecvate la evoluțiile tehnologice și să

[72] https://rm.coe.int/1680081561
[73] https://www.coe.int/en/web/children/lanzarote-convention
[74] https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f

utilizeze toate instrumentele, măsurile și strategiile relevante pentru a preveni și a combate în mod eficient infracțiunile sexuale împotriva copiilor care sunt facilitate prin utilizarea TIC.

Republica Moldova a ratificat Convenția de la Lanzarote în 2012, luându-și angajamentul de a implementa un răspuns holistic la violența sexuală împotriva copiilor, prin intermediul abordării „4 P": Prevenire, Protecție, Urmărire penală *(Prosecution)* și Promovarea cooperării naționale și internaționale. În cadrul celei de-a doua runde de monitorizare efectuate de Comitetul Lanzarote privind protecția copiilor împotriva exploatării sexuale și a abuzului sexual, facilitat de tehnologiile informației și comunicațiilor (TIC),[75] a fost furnizată o gamă largă de recomandări pentru a îmbunătăți punerea în aplicare efectivă a Convenției de la Lanzarote, care ar trebui să fie luate în considerare și de autoritățile moldovenești.

8.3. Manualul pentru factorii de decizie politică privind drepturile copilului în mediul digital

Acest manual este primul și cel mai detaliat document de acest gen publicat vreodată de o instituție guvernamentală internațională. Recomandările conținute în manual sunt în mare măsură aliniate la Comentariul general 25 al CNUDC. În special în capitolul 2, se recomandă ca statele părți să elaboreze un cadru național pentru dezvoltarea politicii și se spune în continuare:

< Un prim pas în punerea în aplicare a recomandării este desemnarea unei autorități sau crearea unui mecanism de coordonare care să urmeze o abordare transversală (de exemplu, Ministerul Educației sau al Familiei (pornind de la ministerele de resort), sau Ministerul Media sau al Agendei Digitale (adoptând o viziune mai largă), autoritățile de protecție a datelor, sau Ombudsmanul pentru copii, sau altele similare). Apoi, este esențial să se cartografieze și să se identifice organismele de stat relevante la nivel național, regional și local. În aceste procese trebuie să fie atrași și alți actori (2.3).

[75] https://rm.coe.int/implementation-report-on-the-2nd-monitoring-round-the-protection-of-ch/1680a619c4

9. Uniunea Europeană

UE a fost deosebit de activă în domeniul protecției online a copiilor și s-a impus ca lider mondial în acest domeniu. Temeiul juridic al politicilor sale în ceea ce privește aspectele discutate în acest raport a fost conținut într-o directivă din 2011[76] privind „Combaterea abuzului sexual și a exploatării sexuale a copiilor și a pornografiei infantile". Printre altele, fiecărui stat membru al UE i se cerea:

- să interzică toate formele de abuz sexual (articolul 3);
- să interzică toate formele de exploatare sexuală (articolul 4);
- să interzică pornografia infantilă și toate activitățile asociate cu crearea, distribuirea și stocarea acesteia (articolul 5);
- să interzică toate formele de solicitare în scopuri sexuale (grooming) (articolul 6);
- să interzică incitarea, complicitatea, instigarea și tentativa la astfel de infracțiuni (articolul 7);
- să promoveze inițiativele educaționale și de formare privind aceste obiective (articolul 23);
- să prevadă dispoziții privind asistența acordată victimelor (articolele 18 și 19);
- să ia măsuri pentru a se asigura că paginile web care conțin pornografie infantilă sunt eliminate și că accesul la acestea este blocat atât în propria jurisdicție, cât și în alte părți (articolul 25).

În urma adoptării directivei, printre altele, în fiecare stat membru al UE a fost înființată una sau mai multe linii telefonice de urgență.

Legislația națională nu este aliniată la directiva din 2011. Directiva 2011/92/UE, art. 5 stabilește o pedeapsă minimă pentru fiecare dintre modalitățile normative ale infracțiunii de pornografie infantilă:

- cumpărarea sau deținerea de pornografie infantilă se pedepsește cu o pedeapsă maximă de cel puțin un an de închisoare;
- obținerea cu bună știință a accesului la pornografie infantilă prin intermediul tehnologiei informației și comunicațiilor se pedepsește cu o pedeapsă maximă de cel puțin un an de închisoare;
- cumpărarea sau deținerea de pornografie infantilă se pedepsește cu o pedeapsă maximă de cel puțin un an de închisoare;
- furnizarea sau punerea la dispoziție de pornografie infantilă se pedepsește cu o pedeapsă maximă de cel puțin doi ani de închisoare;
- producerea de pornografie infantilă se pedepsește cu o pedeapsă maximă de cel puțin trei ani de închisoare.

[76] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

Legislația națională nu delimitează pedepsele pentru modalitățile normative ale infracțiunii de pornografie infantilă. Sarcina individualizării pedepsei este lăsată la aprecierea instanței de judecată, în baza criteriilor generale de individualizare a pedepsei, dar și a prevederilor capitolului VIII, Cod penal.

În prezent, politica emblematică a UE în acest domeniu este gestionată sub titlul „Un internet mai bun pentru copii".[77] În plus, măsurile adoptate recent, cum ar fi Legea privind serviciile digitale[78] și Legea privind pieețele digitale,[79] au, de asemenea, implicații pentru copii în calitate de utilizatori ai internetului. Legea relativ nouă privind confidențialitatea datelor, GDPR, recunoaște în mod specific faptul că copiii sunt un grup protejat în care trebuie să se acorde o atenție sporită pentru a le asigura siguranța.[80] Deși aceste măsuri nu abordează în principal aspecte legate de protecția copiilor, în măsura în care abordează comportamente ilegale sau conținuturi care amenință copiii, ele au o anumită relevanță.

În conformitate cu Legea națională privind protecția datelor cu caracter personal nr. 133 din 08.07.2011, art. 5 alin (3), consimțământul privind prelucrarea datelor cu caracter personal se acordă în formă scrisă de către reprezentantul legal al minorului. Așadar, toate obligațiile legate de GDPR trebuie asumate de către părinții sau reprezentanții legali ai minorilor.

Din punct de vedere istoric, în ceea ce privește comportamentul întreprinderilor, în cadrul directivei din 2011, autoreglementarea a fost baza pe care s-a desfășurat politica privind internetul în UE în general și, în special, în ceea ce privește copiii. Aceasta a fost înțeleasă ca însemnând că întreprinderile nu erau obligate să întreprindă acțiuni specifice pentru a asigura siguranța copiilor, ci astfel de acțiuni erau permise pe bază voluntară. În acest sens, o serie de companii, în special cele mai mari, au anunțat că adoptă în mod voluntar o serie de măsuri care vizează elemente deja clasificate ca fiind CSAM, elemente care ar putea fi CSAM și comportamente de ademenire. Măsurile de acest tip au început să fie puse serios în aplicare în urma lansării în 2009 de către Microsoft a PhotoDNA[81] pe care l-a furnizat la cost zero părților calificate.[82] Toate acestea au continuat fără a fi contestate din punct de vedere juridic până când, în 2018, a reieșit că un nou regulament privind confidențialitatea în mediul electronic va pune sub semnul întrebării funcționarea legală continuă a acestor măsuri.[83] Pentru a ocoli această dificultate și pentru a elimina orice îndoială

---

77 https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2825

78 https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

79 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

80 https://ec.europa.eu/info/law/law-topic/data-protection_en

81 https://www.microsoft.com/en-us/photodna

82 Acest lucru nu înseamnă că implementarea unui sistem care utilizează PhotoDNA nu ar costa nimic, deoarece, pentru a-l implementa la nivel intern, o companie ar trebui să cheltuiască bani pentru integrarea sistemului, formare și gestionare.

83 De îndată ce a apărut această amenințare, iar regulamentul a devenit operațional în decembrie 2020, unele companii, de exemplu Facebook, au încetat orice activitate voluntară de acest tip. Altele, de exemplu Google și Microsoft, nu au făcut acest lucru.

juridică, a fost adoptată o „derogare provizorie”[84] pentru a restabili *status quo ante,* moment în care întreprinderile și-au reluat practicile anterioare sau au răsuflat ușurate și au continuat.[85] Cu toate acestea, derogarea provizorie este limitată în timp. Aceasta va expira în 2024, acesta fiind unul dintre motivele pentru care UE se află în prezent în faza avansată de elaborare a unor noi reglementări.

9.1. Un nou regulament UE privind combaterea abuzului sexual asupra copiilor[86]

Noul regulament va păstra și va dezvolta toate punctele-cheie ale directivei din 2011, dar le va completa în mod considerabil, atât prin crearea de noi mecanisme instituționale la nivel național și la nivelul UE, cât și prin extinderea legislației în mai multe moduri importante. În plus, deoarece este vorba de un regulament și nu de o directivă, se așteaptă ca acesta să fie aplicat în mod uniform în toate statele membre. În special, noul regulament va introduce:

- măsuri obligatorii de evaluare și de reducere a riscurilor, cu noi agenții naționale însărcinate cu examinarea acestora;
- ordine obligatorii de eliminare a conținutului;
- obligații de raportare obligatorie;
- reguli care vor afecta App Stores în ceea ce privește ademenirea.

O parte a noii abordări este menită să încurajeze firmele să gândească în mod sistemic modul în care, în primele etape ale ciclului de dezvoltare a produsului, acestea integrează siguranța prin proiectare și securitatea în mod implicit.

9.2. Un nou Centru European

Va fi înființat un nou Centru European care va deveni un centru de excelență și de expertiză în ceea ce privește prevenirea abuzului sexual asupra copiilor, atât online, cât și în afara acestuia, precum și în ceea ce privește acordarea de asistență victimelor. Unul dintre rolurile sale va fi acela de a disemina cunoștințele privind cele mai bune practici.[87]

Centrul va colabora îndeaproape cu Europol și, printre altele, va contribui la dezvoltarea unor procese și proceduri standardizate pentru raportarea și eliminarea CSAM. Este probabil că va dezvolta o bază de date axată pe UE cu privire la CSAM, care va fi utilizată împreună cu instrumente care pot detecta CSAM.

O altă evoluție importantă este faptul că, în timp ce, în prezent, companiile pot alege ce instrumente folosesc pentru a aborda CSAM sau pentru a detecta practicile de manipulare, în viitor, centrul va evalua și va întocmi o listă de instrumente aprobate.

---

[84] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0568

[85] Facebook a reluat activitatea atunci când derogarea provizorie a devenit lege.

[86] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2976

[87] Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, Strategia UE pentru o luptă mai eficientă împotriva abuzului sexual asupra copiilor, Bruxelles, 24.07.2020.

10. Alianța globală We Protect și modelul de răspuns național

Alianța globală We Protect[88] este o asociație voluntară globală de guverne naționale, companii de tehnologie, ONG-uri și organizații neguvernamentale internaționale. Republica Moldova este membru. Alianța se axează în mod special pe combaterea exploatării sexuale a copiilor pe internet. Prin colaborarea strânsă cu organisme precum UNICEF și cu o serie de donatori filantropici, Alianța este o parte esențială a unei rețele de organizații care oferă fonduri pentru proiecte și pentru cercetare. O publicație cheie a Alianței este „Modelul de răspuns național".[89] Acesta oferă o prezentare foarte succintă a gamei de măsuri pe care o țară ar trebui să aibă în vedere adoptarea ca parte a unei strategii cuprinzătoare de combatere a exploatării sexuale online a copiilor. Recomandările sale sunt, în linii mari, în concordanță cu Manualul Consiliului Europei menționat mai sus, cu CNUDC și cu Comentariul general 25, precum și cu noul regim emergent din cadrul Uniunii Europene.

Republica Moldova este membru al Alianței Globale WeProtect și și-a asumat angajamentul de a proteja copiii împotriva exploatării sexuale și a abuzului online prin intermediul unui răspuns național cuprinzător care ar trebui să fie orientat spre 7 domenii de intervenție:

- Politică și legislație,
- Justiție penală,
- Industria tehnologică,
- Participarea copiilor și a supraviețuitorilor,
- Societate și cultură,
- Cercetare și informații,
- Colaborare internațională.

Modelul de răspuns național oferă o gamă completă de activități privind modul în care industria tehnologică poate contribui la combaterea abuzului sexual asupra copiilor în mediul online, prin intermediul:

- procedurilor de retragere și raportare presupunând: eliminarea și blocarea la nivel local a materialelor online privind abuzurile sexuale asupra copiilor, proceduri pentru eliminarea în timp util a materialelor privind abuzurile

[88] https://www.weprotect.org/
[89] https://www.weprotect.org/framing-the-future/

sexuale asupra copiilor atunci când o companie confirmă prezența acestora, protecții legale pentru ca industria să raporteze abuzurile sexuale asupra copiilor, inclusiv transmiterea conținutului către autoritățile de aplicare a legii sau către o agenție desemnată, colaborare globală și intersectorială;

- soluțiilor tehnologice pentru prevenirea și combaterea exploatării sexuale a copiilor și a abuzurilor sexuale online;
- conduitei comerciale responsabile, prin politici de protecție și de salvgardare a copiilor, prin măsuri de precauție și de remediere care să abordeze problema exploatării sexuale a copiilor și a abuzurilor online.

11. Concepte-cheie și recomandări pentru furnizorii din sectorul privat

11.1. Siguranță prin proiectare, siguranță implicită

Acest concept presupune ca orice întreprindere care construiește sau furnizează un produs sau un serviciu să aibă în vedere, încă din primele etape ale ciclului de proiectare sau de furnizare, întregul spectru de nevoi ale utilizatorilor finali, în special, în acest caz, ale copiilor. Astfel se vor evita costurile inutile legate de „stabilirea ulterioară" a unor caracteristici de siguranță și, de asemenea, se vor evita costurile și impedimentele legate de retragerea sau rambursarea produselor, sau ambele.

Astfel, pe lângă furnizarea de note explicative și sfaturi de siguranță ușor de înțeles pentru oricine, cumpără produsul sau serviciul, la prima utilizare, dacă există opțiuni sau alegeri care trebuie făcute, acestea ar trebui să fie activate la niveluri maxime de siguranță. Părinții nu trebuie să se confrunte cu dificultăți pentru ca un dispozitiv sau un serviciu să fie cât mai sigur posibil pentru copilul lor. În cazul în care există modalități de relaxare sau de liberalizare a setărilor de siguranță, acestea ar trebui să necesite o autentificare puternică din partea unui adult responsabil.[90]

11.2. Importanța evaluării riscurilor

Evaluările de risc ridică probleme similare, în sensul că impun ca oricine vinde sau furnizează un anumit produs sau serviciu să fi efectuat o analiză completă a tuturor riscurilor inerente utilizării acestuia și să acționeze pentru a minimiza orice risc identificat. Acest lucru presupune cunoașterea clienților și a utilizatorilor finali. În unele jurisdicții, este posibil ca evaluările de risc să trebuiască să fie prezentate unui organism de reglementare sau cel puțin să fie disponibile pentru a fi inspectate de către acesta, indiferent dacă a apărut sau nu un caz. În unele jurisdicții există o sugestie conform căreia evaluările de risc sau un rezumat adecvat al acestora ar trebui să fie documente publice, pe site-ul web al fiecărui furnizor. Modele de evaluare a riscurilor sunt disponibile în numeroase sectoare, deși, din cauza naturii unice a spațiului online, nu a apărut un formular standard pentru evaluările de risc. Acesta ar trebui să fie foarte strâns legat de produsul sau serviciul individual[91] .

[90] https://www.esafety.gov.au/industry/safety-by-design/principles-and-background

[91] https://www.taylorwessing.com/en/interface/2022/the-online-safety-bill---the-uks-answer-to-addressing-online-harms/dl-risk-assessments-under-the-online-safety-bill pentru o discuție despre modul în care se va dezvolta probabil evaluarea riscurilor în Regatul Unit, deși este foarte probabil ca UE să dezvolte modele similare.

11.3. Transparența

Transparența a devenit un domeniu critic de dezbatere, nu doar în ceea ce privește modul în care algoritmii gestionează sau manipulează o mare parte din viața noastră online, ci și pentru că există o lipsă de încredere măsurabilă în întreprinderile online în sine. Din aceste motive, dar și din altele, se va pune din ce în ce mai mult accent pe elaborarea unor regimuri de transparență, gestionate de părți terțe de încredere, pentru a reasigura publicul că spațiul online nu mai este ca un fel de „Vest Sălbatic" nereglementat[92] . Multe dintre instrumentele de protecție a copiilor la care se face referire în corpul principal al prezentului raport utilizează algoritmi și diverse instrumente de învățare automată. Nici acestea nu vor scăpa și nu ar trebui să scape controlului. „Lumina soarelui este cel mai bun dezinfectant".[93]

11.4. Recomandări pentru factorii de decizie politică

Coordonare

Guvernul ar trebui să instituie un cadru național de coordonare, cu un mandat clar și suficientă autoritate pentru a coordona toate activitățile legate de siguranța copiilor online și măsurile de prevenire și combatere a exploatării sexuale a copiilor sau a abuzului sexual online. Subiectul trebuie să se afle pe agenda unei platforme multilaterale care să reunească reprezentanți ai autorităților relevante din sectoarele educației, TIC, justiție, sănătate sau social, instituții naționale pentru drepturile omului, societatea civilă, industria și alte asociații relevante. Comisia recent înființată pentru monitorizarea Convenției de la Lanzarote ar trebui explorată ca o platformă potențială pentru coordonarea agendei digitale pentru copii.

Politici

Guvernul trebuie să acorde prioritate elaborării unui nou plan de acțiune pentru promovarea siguranței online a copiilor, care să includă priorități-cheie menite să echilibreze oportunitățile online ale copiilor și potențialele riscuri online. Această politică ar trebui să integreze măsuri care vizează sectorul industrial și revizuirea cadrelor legislative și de reglementare. Planul de acțiune trebuie să țină seama de inițiativele și reglementările UE care stabilesc un regim de monitorizare obligatorie pentru industria TIC și obligația de a întreprinde procese de diligență în ceea ce privește drepturile copilului. În cadrul acestui nou cadru, se sugerează cu tărie să se pună un accent deosebit pe importanța evaluărilor de risc care, la rândul lor, vor conduce la stabilirea unor standarde adaptate vârstei și la obligații mai mari de a include siguranța prin proiectare și securitatea implicită. Pentru a asigura și a menține încrederea publicului în noile dispoziții, trebuie să se acorde o atenție

[92] https://www.weforum.org/agenda/2022/06/eu-digital-service-act-how-it-will-safeguard-children-online/

[93] Cu mulțumiri către judecătorul Brandeis de la Curtea Supremă a SUA.

deosebită elaborării unor standarde de transparență adecvate care, la rândul lor, sunt legate de obligații puternice și obligatorii în materie de confidențialitate, supravegheate de o parte de încredere.

Legislație

Legislația națională trebuie să prevadă dispoziții clare cu privire la responsabilitățile furnizorilor de servicii și la modul în care aceștia fac schimb de informații cu autoritățile de aplicare a legii. Legislația actuală este neclară și poate genera numeroase interpretări. O posibilitate ar fi ca Ministerul Economiei să preia inițiativa de a asigura alinierea legislației naționale privind implicarea sectorului TIC la standardele internaționale reflectate în Convenția de la Budapesta, Convenția de la Lanzarote și alte orientări. De asemenea, ar trebui revizuită legislația privind blocarea conținutului ilegal online.

Mecanisme

Ar trebui dezvoltat un mecanism național de raportare a materialelor de abuz sexual asupra copiilor, consolidând cooperarea națională între autoritățile de aplicare a legii și industrie și cooperarea internațională cu alte linii telefonice de urgență din întreaga lume. Guvernul trebuie să se asigure că există procese naționale care să garanteze că toate CSAM-urile găsite în țară sunt canalizate spre o resursă națională centralizată, care are puterea legislativă de a determina companiile să elimine conținutul. În plus, este necesar să se asigure un număr suficient de funcționari de aplicare a legii care să fie instruiți în investigarea criminalității informatice și să se confrunte cu accesul la instrumente criminalistice care să le permită să extragă și să interpreteze în mod eficient datele digitale.

De asemenea, industria ar trebui să le ofere utilizatorilor posibilitatea de a raporta preocupări și probleme utilizatorilor și de a răspunde în consecință.

Guvernul trebuie să ia măsuri pentru a încuraja întreprinderile comerciale să își stabilească propriile mecanisme de remediere și de soluționare a plângerilor, în conformitate cu criteriile de eficacitate stabilite în Principiile directoare ale ONU privind întreprinderile și drepturile omului. Agenția Națională de Reglementare trebuie să aprobe orientări specifice pentru sectorul TIC în ceea ce privește măsurile pe care ar trebui să le ia aceste întreprinderi pentru a preveni și a combate abuzul sexual asupra copiilor și exploatarea sexuală a copiilor online.

Implicarea în sectorul TIC

Ar trebui organizate mai multe activități de sensibilizare pentru sectorul TIC cu privire la riscurile cu care se confruntă copiii online și la măsurile care ar trebui luate pentru a le preveni, în conformitate cu standardele internaționale. De asemenea, factorii de decizie politică trebuie să fie informați cu privire la rolul Guvernului în implicarea sectorului TIC și la acțiunile care pot fi întreprinse în conformitate cu

angajamentele asumate de Republica Moldova, prin ratificarea Convenției de la Lanzarote, a Convenției de la Budapesta, a Modelului de răspuns național elaborat de Alianța Globală WeProtect sau prin calitatea de membru al UIT.

Guvernul trebuie să ia măsuri pentru a se asigura că întreprinderile TIC aplică listele hash și iau prompt toate măsurile pentru a asigura disponibilitatea metadatelor referitoare la materialele privind abuzurile sexuale asupra copiilor, pentru a le pune la dispoziția organelor de aplicare a legii, pentru a le elimina sau pentru a restricționa accesul până la eliminare. Autoritățile trebuie să ia toate măsurile pentru a se asigura că întreprinderile TIC efectuează evaluări periodice ale riscurilor legate de drepturile copilului și iau măsuri rezonabile pentru a reduce riscurile.

Anexa 1. Întrebări și părți interesate intervievate

Ghid de interviu

Companii TIC

1. Operați doar în Republica Moldova sau sunteți o filială a unei alte persoane juridice cu sediul în străinătate?
2. În ceea ce privește operațiunile dumneavoastră din Republica Moldova, normele pe care le aplicați sunt identice cu cele aplicate în alte jurisdicții în care își desfășoară activitatea societatea dumneavoastră? Gestionați aplicații sau programe a căror proprietate intelectuală o dețineți și o controlați dumneavoastră înșivă? Au fost luate în considerare aspectele legate de siguranța copiilor în cazul funcționării aplicației sau programului? Aveți reguli declarate cu privire la tipul de materiale pe care utilizatorii au voie să le posteze sau să le schimbe prin intermediul serviciilor dumneavoastră?
3. Cum încercați să puneți în aplicare aceste reguli, de exemplu, angajați moderatori de conținut? În caz afirmativ, cine îi gestionează, unde își au sediul, cine îi instruiește și le supraveghează sau verifică activitatea?
4. Implementați în rețea instrumente pentru a detecta CSAM sau imagini care ar putea constitui CSAM?
5. Folosiți instrumente în rețeaua dumneavoastră pentru a detecta eventualele activități de ademenire a copiilor?
6. Aveți un singur punct de contact cu autoritățile de aplicare a legii pentru raportarea activităților suspecte și au autoritățile de aplicare a legii un singur punct de contact cu compania dumneavoastră?
7. Considerați că în cadrul companiei dumneavoastră există o înțelegere și acceptare suficientă a importanței protecției copilului atât din punctul de vedere al legislației moldovenești, cât și din punct de vedere etic?
8. Sunteți la curent cu resursele disponibile pentru a vă ghida în luarea deciziilor în cadrul companiei dumneavoastră în ceea ce privește problemele legate de protecția online a copiilor? Aplicați limite de vârstă sau restricții similare pentru orice parte a serviciilor pe care le furnizați în calitate de întreprindere (problema furnizării accesului la aplicațiile și serviciile altor persoane ridică probleme diferite)?
9. Aveți vreun mecanism de control sau de aplicare a acestor restricții de vârstă?

Ministerul Infrastructurii și Dezvoltării Regionale și Ministerul Economiei

1. Care sunt politicile actuale implementate în domeniu legate de tehnologia informației și comunicațiilor, infrastructura de comunicații, securitatea cibernetică?
2. Cum este inclusă protecția online a copiilor în politicile naționale legate de TIC?
3. Care este rolul ministerelor pe care le reprezentați în domeniul protecției online a copiilor?

4. Care sunt provocările legate de implicarea sectorului TIC în prevenirea și protecția copiilor împotriva exploatării sexuale online a copiilor?
5. Care sunt prioritățile actuale ale ministerului pe care îl reprezentați în domeniul protecției online a copiilor?
6. Care sunt următoarele acțiuni planificate în acest domeniu și de ce tip de sprijin aveți nevoie pentru a asigura o dezvoltare/implementare mai eficientă a politicilor în domeniul protecției online a copiilor?

Ministerul Afacerilor Interne

1. Care sunt politicile actuale implementate în domeniu în ceea ce privește protecția online a copiilor/infracțiunea cibernetică?
2. Care sunt provocările legate de implicarea sectorului TIC în prevenirea și protecția copiilor împotriva exploatării sexuale online a copiilor?
3. Care sunt lacunele legislative/inițiativele legislative menite să faciliteze cooperarea dintre autoritățile de aplicare a legii și sectorul TIC?
4. Care sunt prioritățile actuale ale ministerului pe care îl reprezentați în domeniul protecției online a copiilor?
5. Care sunt următoarele planuri/acțiuni planificate în acest domeniu și de ce tip de sprijin aveți nevoie pentru a asigura o dezvoltare/implementare mai eficientă a politicilor în domeniul protecției online a copiilor?

Direcția de investigare a criminalității informatice

1. Cum colaborați cu sectorul TIC în cadrul investigațiilor privind exploatarea sexuală a copiilor online?
2. Care sunt provocările actuale legate de cooperarea dintre sectorul TIC și autoritățile de aplicare a legii în cazurile de exploatare sexuală a copiilor online?
3. Care sunt barierele identificate în cooperarea cu sectorul TIC în cadrul investigațiilor privind cazurile de exploatare sexuală a copiilor online?
4. Care sunt lacunele legislative în domeniu?
5. Care sunt măsurile necesare pentru a asigura o colaborare mai eficientă între sectorul TIC și autoritățile de aplicare a legii?
6. Cum ar putea contribui sectorul TIC la o investigare mai eficientă a infracțiunilor de exploatare sexuală a copiilor online?

Asociație a sectorului TIC

1. Cum activați în țară și care este mandatul Asociației sectorului TIC?
2. Aveți o politică corporativă și cum integrați protecția copilului în această politică?
3. Cum vedeți rolul sectorului TIC în combaterea CSAM (sau în prevenirea abuzului sexual asupra copiilor online)?

4. Aveți vreun standard de protecție a copiilor online recomandat pentru toți membrii Asociației sectorului TIC?
5. Care sunt măsurile luate pentru a asigura protecția copiilor de către companiile TIC?
6. Care este rolul Asociației sectorului TIC în promovarea/asigurarea protecției online a copiilor? (sau cum vedeți rolul dumneavoastră)

Părțile interesate intervievate

1. Ministerul Infrastructurii și Dezvoltării Regionale
2. Ministerul Economiei
3. Ministerul Afacerilor Interne
4. Moldcell
5. Orange
6. Asociația sectorului TIC

Anexa 2. Acronime și abrevieri

TIC – Tehnologia informației și comunicațiilor
CSAM – materiale privind abuzul sexual asupra copiilor
ONU – Organizația Națiunilor Unite
CNUDC – Convenția Națiunilor Unite privind drepturile copilului
ISP – Internet Service Provider – Furnizor de servicii Internet
OCDE – Organizația pentru Cooperare și Dezvoltare Economică
ESP – Electronic Service Providers - Furnizori de servicii electronice
GDPR – Regulamentul general privind protecția datelor
ONG – organizație neguvernamentală
OING – organizație internațională neguvernamentală

RON

www.coe.int

Consiliul Europei este cea mai importantă organizație europeană pentru drepturile omului de pe continent. Aceasta cuprinde 46 de state membre, inclusiv toți membrii Uniunii Europene. Toate statele Consiliului Europei sunt semnatare ale Convenției Europene a Drepturilor Omului, un Tratat menit să protejeze drepturile omului, democrația și statul de drept. Curtea Europeană a Drepturilor Omului supraveghează punerea în aplicare a Convenției în statele membre.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE