

2020

SIGURANȚA ONLINE A COPIILOR ÎN ȘCOALĂ

POLITICI ȘI
PRACTICI ÎN
DOMENIUL
EDUCAȚIONAL

Centrul Internațional „La Strada Moldova”



Centrul Internațional „La Strada Moldova”

Siguranța online a copiilor în școală. Politici și practici
în domeniul educațional

Autoare:

Elena BOTEZATU
avocată, Directoarea Programului Copii,
„La Strada Moldova”

Au contribuit:

Cristina VAȘCHEVICI, psihopedagog
Victoria GRIBINEȚ, psiholog

Coordonatoarea studiului: Ana REVENCO

Pentru informații suplimentare despre prezenta
publicație, ne puteți contacta:

MD-2012, CP 259, Chișinău, Republica Moldova

Tel.: +373 22 23 49 06

Fax.: +373 22 23 49 07

E-mail: office@lastrada.md

Web: www.lastrada.md

Cuprins

Introducere	4
Metodologia cercetării	5
1. Cadrul recomandărilor internaționale	7
1.1. Politici și angajamente internaționale	8
1.2. Modelul de abordare comprehensivă a siguranței online în școală	12
2. Problematica siguranței copiilor online	15
2.1. Interese și riscuri la care sunt expuși copiii în mediul virtual	16
2.2. Siguranța online din perspectiva elevilor	18
2.3. Siguranța online din perspectiva părinților	20
2.4. Siguranța online din perspectiva cadrelor didactice	23
3. Politici și practici naționale în domeniul educațional	26
3.1. Cadrul politicilor publice naționale și cadrul normativ	27
3.2. Practicile instituțiilor de învățământ în domeniul siguranței copiilor online	29
a. Guvernarea școlii	29
b. Formarea personalului didactic	31
c. Politici și proceduri	31
d. Implicarea părinților	32
e. Educația despre siguranța online	33
f. Tehnologii și infrastructură securizată	34
Principalele concluzii și recomandări	36

Introducere

Trăim într-o perioadă fără precedent, în care tehnologiile ne influențează modul de viață, relațiile, domeniul de activitate și orice tip de interacțiune socială pe care o avem. În tot acest amalgam al schimbărilor, copiii sunt, probabil, cei mai activi consumatori de tehnologii informaționale și, totodată, cei mai vulnerabili în fața riscurilor online în virtutea vârstei, lipsei de cunoștințe și abilități pe care o au. Tendințele indică că copiii utilizează Internetul și tehnologiile de la o vârstă tot mai mică, iar fără suportul și ghidarea corespunzătoare din partea familiei, educatorilor, comunității, se pot expune unui spectru larg de riscuri pentru bunăstarea lor emoțională.

Contextul național, însă, indică despre un nivel precar de informare a părinților, de pregătire a cadrelor didactice și de sensibilizare a comunității, în general, pentru a putea face față acestor schimbări. Se atestă unele restanțe în adaptarea procesului și conținuturilor educației la necesitățile curente ale copilului, în pas cu tendințele globale. În prezent, procesul educațional este orientat spre activități sau lecții despre utilizarea corectă a dispozitivelor digitale și predarea unor reguli de conduită online, organizate în mod sporadic. Mai mult decât atât, lipsesc proceduri de intervenție în situații de abuz online, iar în fiecare situație, acțiunile sunt întreprinse intuitiv.

Pentru a face față acestor schimbări și pentru a cultiva comportamente online sigure și responsabile la copii, pentru a crește nivelul de reziliență a acestora la violența online, la nivel european, este promovată o abordare comprehensivă a siguranței online în școală, prin implicarea tuturor actorilor din sistemul educațional. Ce înseamnă această abordare complexă a siguranței online? Care sunt provocările și necesitățile actorilor din domeniul educației din RM, ce vizează siguranța copilului online? Cum poate fi îmbunătățit răspunsul sistemului educațional în acest domeniu? La aceste întrebări-cheie ne-am propus să răspundem prin această cercetare, pentru a asigura o mai bună înțelegere a *siguranței online în context educațional, a modelului de abordare comprehensivă a siguranței online în școală și a condițiilor necesare implementării* unui asemenea model în Republica Moldova.

Metodologia cercetării

Acest studiu și-a propus să analizeze răspunsul sistemului educațional în promovarea siguranței copiilor online, prin cercetarea politicilor și practicilor instituțiilor de învățământ, menite să contribuie la prevenirea riscurilor online și protecția copiilor de abuzuri în mediul virtual.

Obiectivele cercetării

1. Studiarea cadrului de recomandări internaționale și naționale care vizează siguranța online a copilului în context educațional;
2. Identificarea, la nivel național, a problemelor ce vizează siguranța copiilor în mediul online și care necesită a fi soluționate prin măsuri educaționale;
3. Elaborarea recomandărilor pentru îmbunătățirea răspunsului sistemului educațional în promovarea siguranței online a copiilor.

Sarcinile cercetării

1. Studiarea politicilor, recomandărilor și angajamentelor internaționale asumate de RM, ce vizează siguranța online în procesul educațional;
2. Studiarea modelului european de abordare comprehensivă a siguranței online a copilului în școală și bunelor practici de implementare a acestui model;
3. Analiza intereselor și riscurilor la care se expun copiii în mediul online;
4. Analiza nivelului de informare și pregătire a elevilor, cadrelor didactice, părinților de a observa și a răspunde acestor riscuri;
5. Analiza măsurilor educaționale de promovare a siguranței online, planificate în documentele de politici naționale;
6. Analiza cadrului normativ național ce vizează siguranța copiilor online și stabilirea deficiențelor care împiedică răspunsul eficient al sistemului educațional;
7. Studiarea politicilor instituționale și modului de coordonare a eforturilor în domeniul siguranței online în școală; studierea disponibilității activităților de formare a cadrelor didactice, procedurilor de intervenție în cazuri de abuz online, parteneriatelor și colaborării cu părinții în promovarea siguranței online; studierea metodelor

de educație a siguranței online și principalelor aspecte abordate și practicilor de securizare a infrastructurii TIC în școală.

8. Formularea propunerilor de politici publice pentru remedierea deficiențelor și lacunelor identificate în practicile educaționale naționale, pentru a asigura condițiile necesare implementării modelului de abordare comprehensivă a siguranței online în școală.

Metodele de cercetare

Pentru atingerea obiectivelor prezentului studiu, au fost folosite următoarele instrumente și metode de cercetare:

1. Analiza documentelor de politici internaționale și recomandărilor privind modul de abordare a siguranței online în procesul educațional;
2. Analiza documentelor de politici și actelor normative ale RM, relevante pentru scopurile acestui studiu;
3. Discuții de tip focus-grup cu 50 de cadre didactice din 48 de instituții de învățământ din 20 de raioane ale țării și din municipiul Chișinău;
4. Discuții de tip focus-grup cu reprezentanții managementului școlar din cinci instituții de învățământ din patru localități din țară;
5. Discuții de tip focus-grup cu 203 elevi din ciclul gimnazial: 104 elevi din clasa a VI-a și 99 elevi din clasa a IX-a;
6. Metoda observației, în timpul activităților despre siguranța online desfășurate cu 69 de psihologi școlari și specialiști din cadrul Serviciilor de Asistență Psihopedagogică;
7. Chestionarul despre siguranța copiilor online (au răspuns 153 de părinți).

Limitări

Domeniul de cercetare al prezentului studiu este limitat la principalele probleme ce țin de siguranța copiilor în mediul online și nu abordează subiecte precum securitatea digitală sau cibernetică. Nu fac parte din obiectul de studiu al cercetării nici următoarele subiecte:

- Digitalizarea sistemului educațional și utilizarea tehnologiilor în procesul educațional;
- Analiza competențelor digitale ale cadrelor didactice, elevilor sau altor actori vizați;
- Modul în care sunt utilizate rețelele de socializare de către angajații instituțiilor de învățământ;
- Siguranța și securitatea procesului educațional la distanță;
- Alte aspecte ce vizează integrarea TIC în educație, decât dacă acestea au legătură directă cu riscurile online la care sunt expuși copiii, conform capitolului II.



1. Cadrul recomandărilor internaționale

1.1. Politici și angajamente internaționale

Comunitatea internațională este preocupată de mai mulți ani de siguranța copiilor online și de modul în care școala poate dezvolta gândirea critică a elevilor, pentru a face față riscurilor online. Măsuri în domeniul educației au fost stabilite în mai multe documente de politici și recomandări internaționale, care au stabilit măsuri educative în acest sens și la care facem referire în cele ce urmează.

Cadrul general de politici și angajamentele internaționale ale RM

Convenția Consiliului Europei pentru protecția copiilor împotriva exploatării sexuale și abuzurilor sexuale (Convenția de la Lanzarote)¹

Convenția de la Lanzarote a fost ratificată de RM în anul 2012 și implementarea acesteia constituie un angajament asumat². Deși stabilește măsuri de protecție a copiilor față de toate formele de abuz și exploatare sexuală, art. 6 din Convenție prevede măsuri de educație pentru copii, ce trebuie întreprinse pentru a ne asigura că toți copiii sunt informați despre riscurile abuzului sexual și mijloacele prin care se pot apăra, în funcție de nivelul lor de dezvoltare. Convenția stabilește că o atenție specială trebuie acordată situațiilor de risc ce implică folosirea noilor tehnologii ale informației și comunicațiilor.

Protecția copiilor față de exploatarea sexuală și abuzul sexual, facilitate de tehnologiile informaționale și de comunicație, reprezintă subiectul runde a doua de monitorizare a implementării Convenției de la Lanzarote, inițiată în anul 2017³. Deși nu a fost încă publicat raportul de monitorizare, datele din chestionarul de monitorizare includ multe întrebări ce vizează sectorul educației și măsurile întreprinse pentru a preveni transmiterea de fotografii

intime sau conținuturi video auto-produse de copii, ceea ce indică despre aspectele ce necesită a fi abordate în programul școlar pentru a preveni riscul abuzului sexual online⁴.

Obiectivele de dezvoltare durabilă

Siguranța copiilor online în instituțiile de învățământ contribuie direct la realizarea Obiectivului de dezvoltare durabilă (în continuare ODD) nr. 4, "Educație de calitate", și ODD 16, Ținta 16.2, "Stoparea abuzului, neglijării, exploatării, traficului și tuturor formelor de violență și tortură a copiilor"⁵.

ODD nr. 4 "Educație de calitate"

În Moldova, Obiectivul 4 prevede realizarea educației integrative și universale, dar și pregătirea tinerilor și adulților pentru o încadrare mai bună pe piața muncii. Țintele sunt: asigurarea dezvoltării și stilului de viață durabile, drepturilor omului, egalității de gen, economiei verzi; promovarea culturii pentru pace și non-violenței, cetățenia globală și aprecierea diversității culturale, toate promovate prin includerea acestora în programul de studii (Ținta 4.7). Una dintre provocări, care, la fel, urmează a fi abordată, este asigurarea instituțiilor de învățământ cu medii sigure, non-violente, integrative și efective de învățământ pentru copii, copii cu dizabilități și fără discriminare pe bază de gen (Ținta 4.a).

Siguranța în instituția de învățământ presupune crearea unui mediu în care copilul se simte în siguranță atât fizic, cât și emoțional, social. Mediul școlar prietenos și sigur presupune mediul care asigură starea de bine a copiilor, le respectă drepturile și le garantează protecția integrității lor fizice și psihice. În contextul digitalizării relațiilor sociale, angajamentele instituțiilor de învățământ de a crea un mediu sigur ar trebui să vizeze și mediul online, nu doar mediul offline.

¹ <https://rm.coe.int/168046e1d9>

² https://www.legis.md/cautare/getResults?doc_id=13045&lang=ro

³ <https://rm.coe.int/thematic-questionnaire-for-the-2nd-monitoring-round-on-the-protection-/168075f307>

⁴ <https://rm.coe.int/thematic-questionnaire-for-the-2nd-monitoring-round-on-the-protection-/168075f307>

⁵ <https://www.md.undp.org/content/moldova/ro/home/sustainable-development-goals/goal-16-peace-justice-and-strong-institutions.html>

ODD nr. 16 “Pace, justiție și instituții puternice”

Acest Obiectiv din Agenda 2030, în Moldova, presupune dezvoltarea instituțiilor eficiente, responsabile și transparente la toate nivelele, care vor asigura un proces decizional receptiv, integrativ, participativ și reprezentativ în dezvoltarea politicilor publice și utilizarea banilor publici. Un accent important se va pune pe reducerea tuturor formelor de violență, în special violența în familie și violența sexuală, precum și pe eliminarea și combaterea abuzului, traficului și violenței împotriva copiilor (Ținta 16.2).

Abuzul și violența împotriva copiilor se pot manifesta atât în instituțiile școlare, unde ar trebui să primească protecție și grijă, acasă, cât și în mediul virtual. „Moldova 2030” este o oportunitate de a elabora politici care să protejeze copiii de toate formele de violență, inclusiv de violența online.

Cadrul de politici tematice ce vizează siguranța online a copiilor în procesul educațional

Strategia europeană pentru un internet mai bun pentru copii⁶

Strategia se ține pe patru piloni principali:

1. Stimularea conținutului online de calitate pentru tineri;
2. Sensibilizare și responsabilizare crescută;
3. Crearea unui mediu online sigur pentru copii și
4. Lupta împotriva abuzului sexual și exploatării sexuale a copiilor.

Strategia propune un șir de acțiuni ce trebuie întreprinse de Comisia Europeană și de statele-membre, precum și de companiile din industria de profil⁷. Strategia a fost aprobată în anul 2012, nu este stabilit un termen de implementare a acesteia și continuă să fie și astăzi documentul-cheie de politici la nivel european, care ghidează statele în elaborarea propriilor politici în domeniul siguranței online a copiilor.

Una dintre acțiunile stabilite pentru stimularea conținutului online și de calitate pentru tineri este

“educația în domeniul digital și media și predarea siguranței online în școli”. Strategia a stabilit obligativitatea statelor-membre de a întreprinde următoarele acțiuni:

- ~ A intensifica aplicarea strategiilor pentru a include în programul școlar unele cursuri pe tema siguranței online, până în 2013;
- ~ A consolida educația informală pentru siguranța online, a dezvolta politici privind “siguranța online” în școală și a asigura formarea adecvată a profesorilor;
- ~ A sprijini parteneriate între sectorul public și cel privat pentru a atinge obiectivele de mai sus.

Totodată, Comisia Europeană și-a asumat următoarele angajamente:

- ~ Să sprijine identificarea și schimbul de bune practici între statele membre, în domeniul educației formale și informale, în materie de siguranță online; să susțină crearea de conținut educațional online relevant și parteneriatele dintre sectorul public și cel privat, care vizează comunicarea eficientă cu copiii, părinții, profesorii și educatorii;
- ~ Să elaboreze, în cadrul Europass, un modul specific privind competența digitală și îmbunătățirea indicatorilor despre utilizarea și impactul TIC în educație.

Agenda digitală pentru Europa⁸

Deși este un document de politici mai complex, ce are ca scop definirea rolului esențial al tehnologiei informației și comunicațiilor în realizarea obiectivelor Europei pentru 2020, reglementează și **obligativitatea statelor-membre de a preda siguranța online în școală**. Conform acțiunilor planificate, statele-membre ale Uniunii Europene urmau să includă siguranța online în programa școlară până în 2013.

Planul de Acțiuni privind Educația Digitală⁹

Prioritatea Comisiei Europene de a “Dezvolta aptitudini și competențe digitale relevante pentru transformarea digitală” face referire și la siguranța online, ca unul dintre domeniile ce descriu competența digitală. Una dintre acțiunile planificate în acest sens este lansarea unei campanii de informare la nivelul UE, care să se adreseze cadrelor didactice, părinților, precum și elevilor/studentilor și care să

⁶ <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52012DC0196&from=EN>

⁷ <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52012DC0196&from=EN>

⁸ <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52010DC0245&from=RO>

⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:22:FIN#footnoteref21>

stimuleze siguranța online, igiena cibernetică și alfabetizarea mediatică.

Acest document de politici **pune în valoare importanța siguranței online și "igienii digitale" în contextul dezvoltării competențelor digitale**. Planul de acțiuni recunoaște necesitatea consolidării gândirii critice și dezvoltarea competențelor copiilor, astfel încât ei să poată analiza și depăși pericolele actuale. Pentru aceasta, trebuie întreprinse acțiuni menite să sensibilizeze educatorii, părinții și elevii privind siguranța online.

Cadrul European DigCompOrg¹⁰

Acest cadru reprezintă un set de măsuri ce ghidează instituțiile de învățământ primar, secundar și profesional, precum și instituțiile de învățământ superior în auto-evaluarea progresului integrării comprehensive și implementării eficiente a tehnologiilor de învățare digitală. Viziunea strategică a acestui cadru de referință vizează integrarea progresivă și eficientă a tehnologiilor în procesul educațional, ca inovație educațională, care implică planificarea schimbărilor pe trei dimensiuni: pedagogică, tehnologică și organizațională.

DigCompOrg are la bază 7 elemente-cheie care sunt detaliate prin intermediul a 74 de sub-elemente. **Siguranța online se regăsește în descrierea mai multor elemente-cheie ale acestui cadru de referință (practici de predare și învățare, practici de guvernare și leadership, infrastructură securizată)**. În linii generale, o instituție de învățământ "competentă digital" trebuie să întrunească următoarele condiții:

1. Să aibă practici de guvernare și leadership în domeniu, fapt care presupune un sistem de management al integrării TIC în educație, bine pus la punct, însoțit de un plan de implementare;
2. Să aibă practici de predare și învățare corespunzătoare, focusate pe dezvoltarea competențelor digitale ale angajaților instituției de învățământ și elevilor, dar și o readaptare a rolurilor și abordărilor pedagogice în procesul de predare-învățare;
3. Să asigure dezvoltarea profesională a tuturor angajaților instituției de învățământ, la orice nivel;
4. Să desfășoare practici de evaluare a eforturilor în domeniu;
5. Să asigure conținut calitativ, inclusiv prin programul curricular ce trebuie reinterpretat și actualizat în vederea asigurării integrării tehnologiilor digitale

în procesul educațional;

6. Colaborare și networking între instituții la subiectul vizat, cu participarea nemijlocită a elevilor și cadrelor didactice la schimbul de cunoștințe și experiențe;
7. O infrastructură digitală planificată, supusă unui plan de gestionare specific, pentru a asigura eficiența, dar și utilizarea optimă a tehnologiilor digitale în procesul educațional.

Cât privește siguranța online, DigCompOrg stabilește că¹¹:

- Practicile de învățare și predare ar trebui să pună pe primul loc siguranța, riscurile și comportamentele responsabile în mediul online;
- Infrastructura digitală ar trebui să respecte măsurile de protecție a vieții private, confidențialitatea și siguranța elevilor. Aceasta ar putea include obligații legale privind protecția datelor, unele ghiduri pentru angajați și elevi privind protecția vieții private, a confidențialității sau a siguranței în mediul online;
- Practicile de guvernare și leadership presupun existența unei politici de integrare a TIC în cadrul instituțional care să definească modul de utilizare pozitivă a TIC în procesul educațional. Această politică organizațională trebuie să includă, în mod obligatoriu, și un capitol despre siguranța online.

Cadrul european al competențelor digitale pentru cetățeni DigComp¹²

Cadrul european prevede cinci domenii ale competenței digitale pentru cetățeni:

1. Educația în domeniul informației și datelor;
2. Comunicare și colaborare;
3. Creare de conținut digital;
4. **Siguranță**;
5. Soluționare de probleme.

În acest cadru de competențe, **siguranța vizează următoarele aspecte:**

1. **Protejarea dispozitivelor**, conținutului digital; înțelegerea riscurilor și amenințărilor în mediul digital. A cunoaște măsurile de siguranță și securitate online și a ține cont de acestea pentru a asigura confidențialitatea și corectitudinea deciziilor luate.

¹⁰ <https://ec.europa.eu/jrc/en/digcomporg>

¹¹ http://publications.jrc.ec.europa.eu/repository/bitstream/JRC98209/jrc98209_r_digcomporg_final.pdf

¹² <https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework>

2. **Protejarea datelor personale și confidențialității**, înțelegerea modului în care trebuie utilizată și distribuită informația personală, astfel încât să ne putem proteja pe sine și pe alte persoane de pericole. A înțelege că serviciile digitale utilizează o politică de confidențialitate ce ne informează despre modul în care datele personale sunt utilizate.
3. **Protejarea sănătății și bunăstării**, ce presupune abilitatea de a evita riscurile pentru sănătate și amenințările în adresa bunăstării fizice și psihice, ca urmare a utilizării tehnologiilor digitale. A te putea proteja pe tine și pe alte persoane de posibile pericole în mediul virtual (de ex. cyberbullying). A fi conștient de modul cum tehnologiile digitale pot fi utilizate pentru bunăstarea și incluziunea socială.
4. **Protejarea mediului digital** prin conștientizarea impactului pe care îl au tehnologiile și utilizarea lor asupra mediului. În DigComp, mediul digital este termenul utilizat pentru a descrie cadrul de realizare a unor acțiuni digitale, fără a avea în vedere o anumită tehnologie sau un anumit dispozitiv digital.

DigComp a stabilit și 8 nivele de eficiență, repartizate în 4 categorii, și exemple de aplicabilitate a competențelor conform unor scenarii descrise¹³:

- Nivel de bază;
- Nivel intermediar;
- Nivel avansat;
- Nivel de calificare înaltă.

Toate aceste standarde fac delimitare între măsurile de siguranță online și măsurile de securitate online.

DigComp a fost implementat diferit în statele europene. Majoritatea au integrat siguranța online în cadrul normativ de competențe digitale, în contextul elementelor ce vizează “Protecția datelor cu caracter personal și confidențialității”, dar și “Protejarea sănătății și a bunăstării”¹⁴.

“Protecția datelor cu caracter personal și confidențialității” sunt competențe ce presupun înțelegerea modului cum sunt utilizare și partajate informațiile ce pot identifica o persoană; înțelegerea faptului că serviciile digitale au “o politică de confidențialitate” menită să-i informeze pe utilizatori despre modul cum sunt utilizate datele personale, pentru a-i ajuta pe elevi să se protejeze pe ei înșiși și pe alții.

“Protejarea sănătății și bunăstării” reprezintă o altă competență din aceeași categorie, scopul căreia este evitarea riscurilor pentru sănătate și amenințărilor față de bunăstarea fizică și psihologică a copilului, la care se poate expune utilizând tehnologiile digitale; dezvoltarea competențelor menite să îi protejeze pe ei înșiși, dar și pe alții de pericolele posibile din mediile digitale (cum ar fi hărțuirea).

Recomandarea Comitetului de Miniștri pentru promovarea educației privind cetățenia digitală¹⁵

Statele membre ale CoE, inclusiv RM, sunt încurajate să își revizuiască legislația, politicile și practicile, pentru a include un cadru de învățare și a asigura că acesta corespunde Recomandării Comitetului de Miniștri pentru promovarea educației privind cetățenia digitală¹⁶.

“Educația pentru cetățenia digitală” este înțelegerea persoanelor de orice vârstă prin educație sau prin dezvoltarea de competențe pentru învățare și participare activă în societatea digitală, pentru a-și exercita și apăra drepturile și responsabilitățile online și pentru a promova și proteja drepturile omului, democrația și statul de drept în mediul online. Educația pentru cetățenia digitală promovează dezvoltarea unui set de valori, abilități, atitudini, cunoștințe ce ar ajuta în participarea activă și responsabilă online, prin folosirea tehnologiilor digitale în mod competent și pozitiv.

Acest program are la bază 3 piloni-cheie:

1. “A fi online” (acces și incluziune, învățare și creativitate, educația pentru media și alfabetizare informațională);
2. “Bunăstarea online” (etica și empatia, sănătatea și starea de bine, prezența online și comunicarea);
3. “Drepturile online” (participarea activă, drepturi și responsabilități, securitatea și confidențialitatea, conștientizarea consumatorilor)¹⁷.

¹³ [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_\(online\).pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_(online).pdf)

¹⁴ https://eacea.ec.europa.eu/national-policies/eurydice/sites/eurydice/files/en_digital_education_n.pdf

¹⁵ https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168098de08

¹⁶ Recomandarea CM/Rec(2019)10 a Comitetului de Miniștri către Statele Membre privind dezvoltarea și promovarea educației pentru cetățenia digitală, adoptat de Comitetul de Miniștri la 21 Noiembrie 2019, la ședința 1361 a Deputaților Miniștri.

¹⁷ <https://rm.coe.int/10-domains-dce/168077668e>

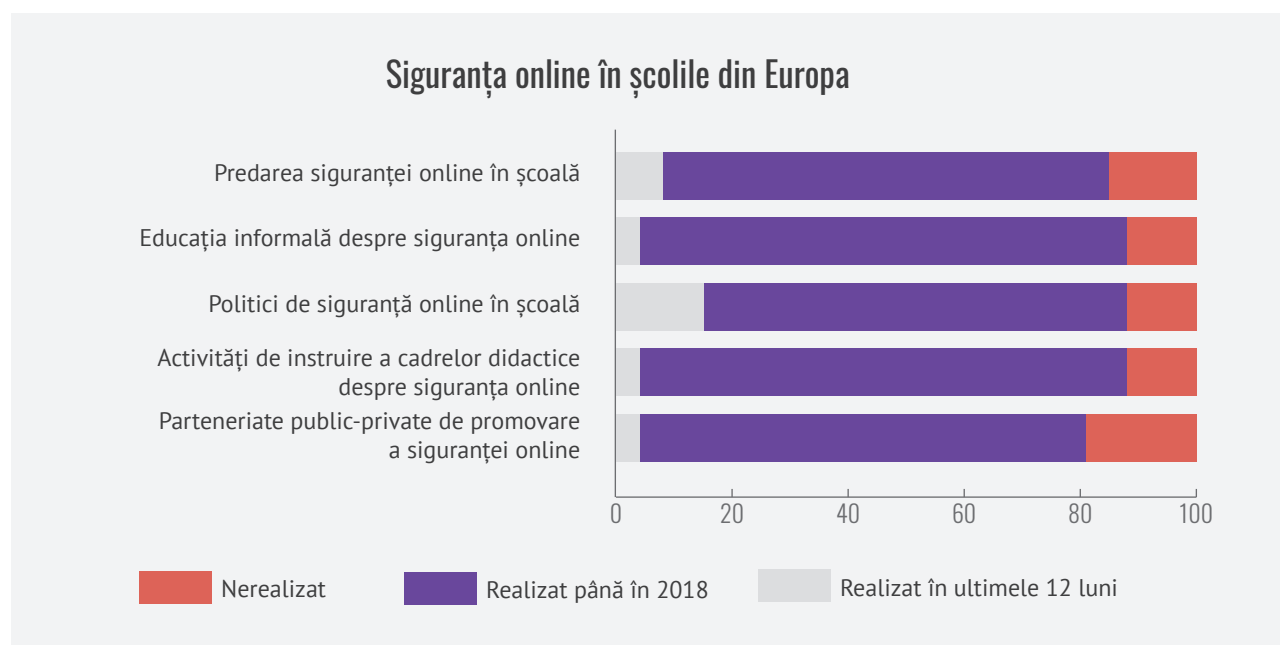
1.2. Modelul de abordare comprehensivă a siguranței online în școală

Politicile și recomandările internaționale, în special Strategia Europeană pentru un Internet mai bun pentru Copii, menționează un șir de acțiuni ce ar trebui întreprinse pentru siguranța online în școală:

- ~ Includerea siguranței online în programa școlară;
- ~ Încurajarea educației informale despre siguranța online;

- ~ Dezvoltarea politicilor de siguranță online în școală;
- ~ Asigurarea instruirii corespunzătoare a cadrelor didactice despre siguranța online;
- ~ Suport al parteneriatelor public-private în domeniul siguranței online;
- ~ Alte activități relevante.

Figura 1: “Siguranța online în școlile din Europa” **Sursa:** Raportul de implementare a Strategiei Europene pentru un Internet mai Bun pentru Copii în Statele Uniunii Europene, 2018¹⁸.



Aceste măsuri au fost practic implementate de către majoritatea statelor europene până în anul 2018. În mai mult de 85% dintre state, siguranța online a copiilor este predată în școală. Pe lângă activitățile realizate cu regularitate conform programului școlar, în mai mult de 88% dintre state se realizează și activități informale de educație despre siguranța online. Totodată, e asigurat un program de instruire pentru cadrele didactice în domeniu, de dezvoltare a politicilor instituționale despre siguranța online și sunt încurajate parteneriatele public-private în domeniul siguranței online¹⁹.

Toate acestea, conform recomandărilor Organizației pentru Cooperare și Dezvoltare Economică (în continuare – OECD) determină o abordare

comprehensivă a siguranței online în școală. Acest fapt presupune depășirea responsabilităților de educație și integrarea siguranței online în toate aspectele activității școlare, în toate politicile, procedurile și procesele din instituția de învățământ. Rolul școlii în acest sens este unul crucial și constă în abilitarea copiilor pentru a diminua din utilizarea negativă a Internetului și a dispozitivelor digitale, încurajând totodată utilizarea TIC în procesul de învățare, predare și stabilire a unor conexiuni sociale²⁰.

Această abordare presupune că, atât cadrele didactice, cât și ceilalți angajați ai instituției de învățământ pot recunoaște, răspunde și ajuta copilul în situații de risc care vizează siguranța online.

¹⁸ <https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7>

¹⁹ <https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7>

²⁰ <https://www.oecd-ilibrary.org/docserver/f21353a9-en.pdf?expires=1589194601&id=id&accname=guest&checksum=990A761AF4E566F8D36E5B29545B2F5B8>

Așadar, reieșind din cele prezentate mai sus, se conturează mai mulți piloni-cheie ai politicii de siguranță online a copilului în școală. În cele ce urmează, e prezentat un exemplu al UK de transpunere a recomandărilor internaționale în practică, prin încurajarea dezvoltării politicilor instituționale în domeniu. Elemente similare se regăsesc și în politicile școlilor din alte state (Australia, Polonia, etc.)²¹:

1. Politici și proceduri ce stabilesc responsabilități pentru întreaga comunitate școlară:
 - ✓ Existența unui coordonator al siguranței online în școală, responsabil de monitorizarea implementării politicilor în domeniul siguranței online;
 - ✓ Politici instituționale ce fac referire la siguranța online, integrate sau conectate la celelalte politici din școală;
 - ✓ Proceduri și politici de intervenție în cazuri de abuz online.
2. Comunicarea cu părinții și îngrijitorii despre siguranța copiilor online;
 - ✓ Implicarea părinților și îngrijitorilor în procesul de dezvoltare a politicilor școlii, ce vizează siguranța online;
 - ✓ Informarea părinților despre măsurile întreprinse de școală pentru a asigura un mediu de învățare cu utilizarea TIC, sigur pentru copii;
 - ✓ Informarea părinților despre siguranța online și punerea la dispoziția lor a unor materiale, informații, resurse, etc.
3. Dezvoltarea capacităților cadrelor didactice în domeniul siguranței online;
 - ✓ Toate cadrele didactice care desfășoară activități despre siguranța online au o pregătire în domeniu și au participat la instruiți despre siguranța online;

- ✓ Siguranța online la nivel pedagogic, tehnologic și organizațional e inclusă în cursurile de calificare a cadrelor didactice, etc.

4. Dezvoltarea abilităților de siguranță online pentru elevi;

- ✓ Includerea subiectului în programul școlar obligatoriu;
- ✓ Abordarea pozitivă în educarea comportamentelor sigure online;
- ✓ Abordarea obligatorie a riscului sextingului în lecțiile cu elevii;
- ✓ Activitățile ar trebuie orientate spre eforturi de reducere a riscurilor sau diminuare a pericolelor, dar și spre discuții despre riscurile unor comportamente online, pentru a dezvolta copilului abilități de gândire critică, etc.

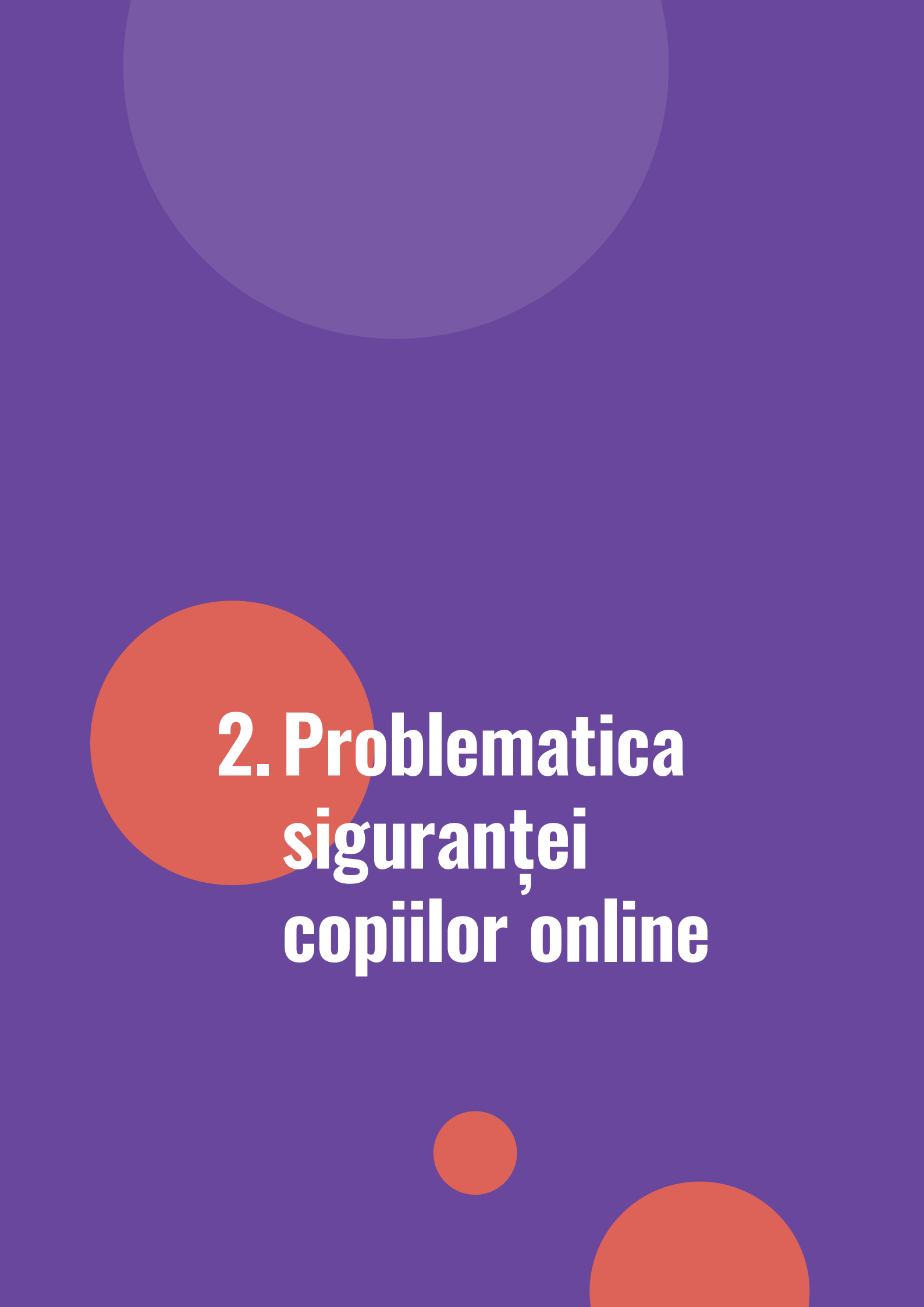
5. Infrastructură securizată, ce ar permite utilizarea tehnologiilor în siguranță;

- ✓ Asigurarea unor sisteme de securitate eficiente, precum sunt programele de filtrare a conținutului, monitorizare și tehnologii firewall sau anti-virus susținute de monitorizarea regulată și detaliată a rețelelor de calculatoare;
- ✓ Documentarea tuturor computerelor ce au acces la Internet în școală. În cazul unor încălcări grave, documentarea rețelei și a dispozitivelor hardware pot ajuta în investigațiile ulterioare. Atenție deosebită trebuie acordată monitorizării echipamentelor mobile sau wireless, etc.

21 https://www.aoc.co.uk/sites/default/files/E_Safety_Developing_whole_school_policies_to_support_effective_practice.pdf

Principalele constatări ce vizează cadrul recomandărilor internaționale:

1. Integrarea siguranței online în procesul educațional este o prioritate a Statelor Europene pe parcursul ultimilor 10 ani.
2. Siguranța online este unul dintre elementele-cheie stabilite de către Comisia Europeană în Cadrul European de Competențe Digitale DigComp. Acest fapt indică asupra necesității de abordare a competenței digitale și impactului tehnologiilor dintr-o perspectivă mai largă: nu doar din punct de vedere tehnologic, dar și din punctul de vedere al impactului utilizării tehnologiei asupra bunăstării psiho-emoționale a copiilor.
3. Digitalizarea procesului educațional nu poate fi percepută ca dimensiune distinctă de asigurare a bunăstării emoționale a copilului în procesul educațional. În contextul evoluției tehnologice și integrării tehnologiilor în procesul educațional, devine necesară și firească stabilirea unor priorități în vederea protejării copilului în mediul virtual. Practicile și politicile europene integrează siguranța online în toate tendințele de digitalizare a educației, iar acesta ar trebui să fie un aspect-cheie în toate inițiativele și politicile educaționale naționale.
4. Principalele acțiuni recomandate în documentele de politici publice internaționale vizează integrarea siguranței online în programul școlar de la o vârstă cât mai mică, realizarea diverselor activități de informare și sensibilizare pentru comunitatea școlară (elevi, părinți, cadre didactice, etc.) și dezvoltarea unor politici instituționale ce ar asigura un răspuns eficient al școlii la provocările copiilor în mediul online.
5. Educația despre siguranța online trebuie să abordeze și subiecte ce vizează transmiterea de fotografii și video cu conținut sexual auto-produse de către copiii.



2. Problematica siguranței copiilor online

2.1. Interese și riscuri la care sunt expuși copiii în mediul virtual

Cel mai recent studiu național în domeniul siguranței copiilor online²² indică despre unele tendințe noi în comportamentul copiilor din Republica Moldova. Un număr tot mai mare de copii de vârstă mică utilizează Internetul încă la etapa preșcolară. În total, 96,5% dintre copiii cu vârsta cuprinsă între 12 și 15 ani au cont/profil pe rețelele de socializare, iar 44% dintre ei sunt prezenți pe rețelele de socializare la o vârstă extrem de fragedă, sub 10 ani. Respectiv, tot mai mulți copii sunt prezenți pe rețele de socializare de la o vârstă tot mai mică, își fac prieteni noi în mediul online, persoane pe care nu le cunosc în realitate, expunându-se tot mai mult riscurilor ce derivă din interacțiunile online cu alte persoane.

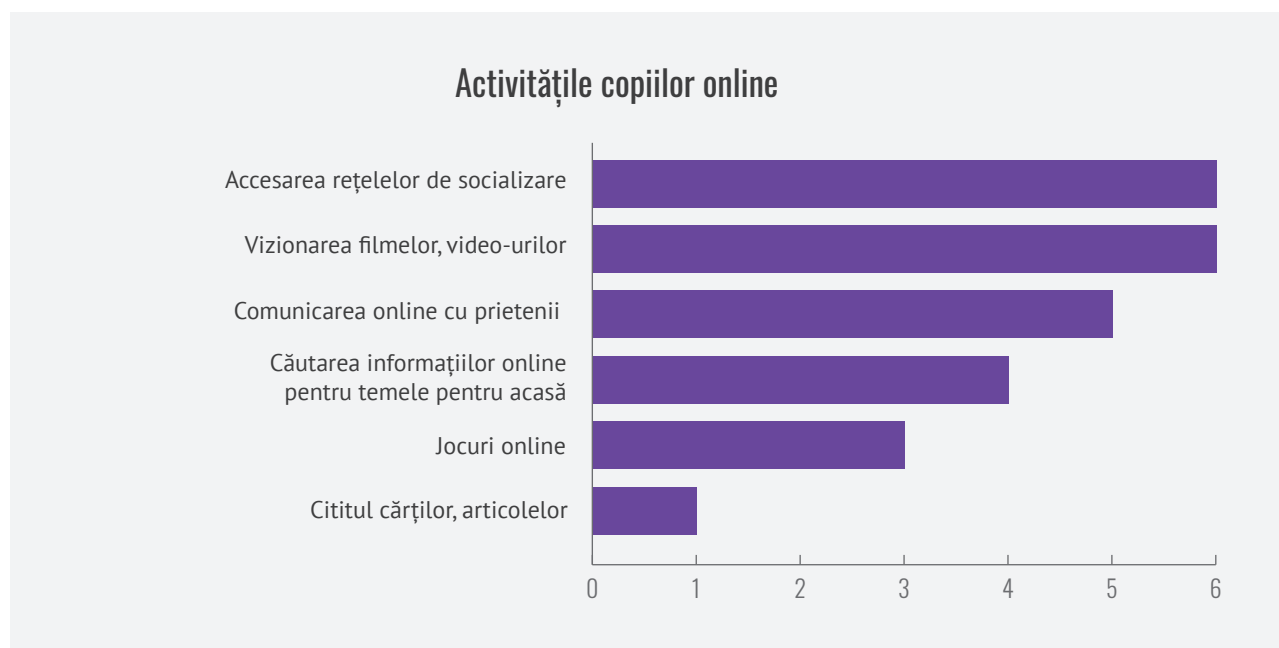
Același studiu arată că copiii de 12-15 ani din RM utilizează Internetul în diferite scopuri²³:

- educațional (pentru a-și face temele pentru acasă, a citi unele materiale informative, cărți, etc.);
- de comunicare și socializare (accesează conturile de pe rețelele de socializare, discută pe forumuri, chaturi, etc.);
- de divertisment (jocuri online, vizionează vloguri, clipuri video, filme, etc.)

Discuțiile de tip focus-grup cu elevii au reconfirmat interesul copiilor pentru rețelele de socializare, filme sau video-uri și comunicarea cu prietenii.

Figura 2: “Cele mai populare activități ale copiilor în mediul online”

Sursa: Rezultatele discuțiilor focus-grup cu elevii



Riscurile la care sunt expuși copiii în mediul online pot fi împărțite convențional în trei categorii²⁴:

- **Riscurile de conținut** sunt acele în care copilul e receptor al conținutului distribuit în masă. Actorii implicați sunt copilul și alte persoane care generează conținut online.
- **Riscurile de contact** presupun interacțiunea copilului cu un adult, care e inițiată și dominată de

către adult. Copilul este participant pasiv, adultul fiind cel care inițiază și controlează contactul

- **Riscurile de conduită** se referă la situațiile între semenii (peer-to-peer). Copilul poate fi atât actorul care inițiază o anumită situație online, cât și cel care agresează.

Cel mai frecvent **risc de conținut** la care sunt expuși copiii din RM este accesarea conținutului ce

²² http://lastrada.md/files/resources/3/sumar_executiv_final.pdf

²³ http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet_final.pdf

²⁴ http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf

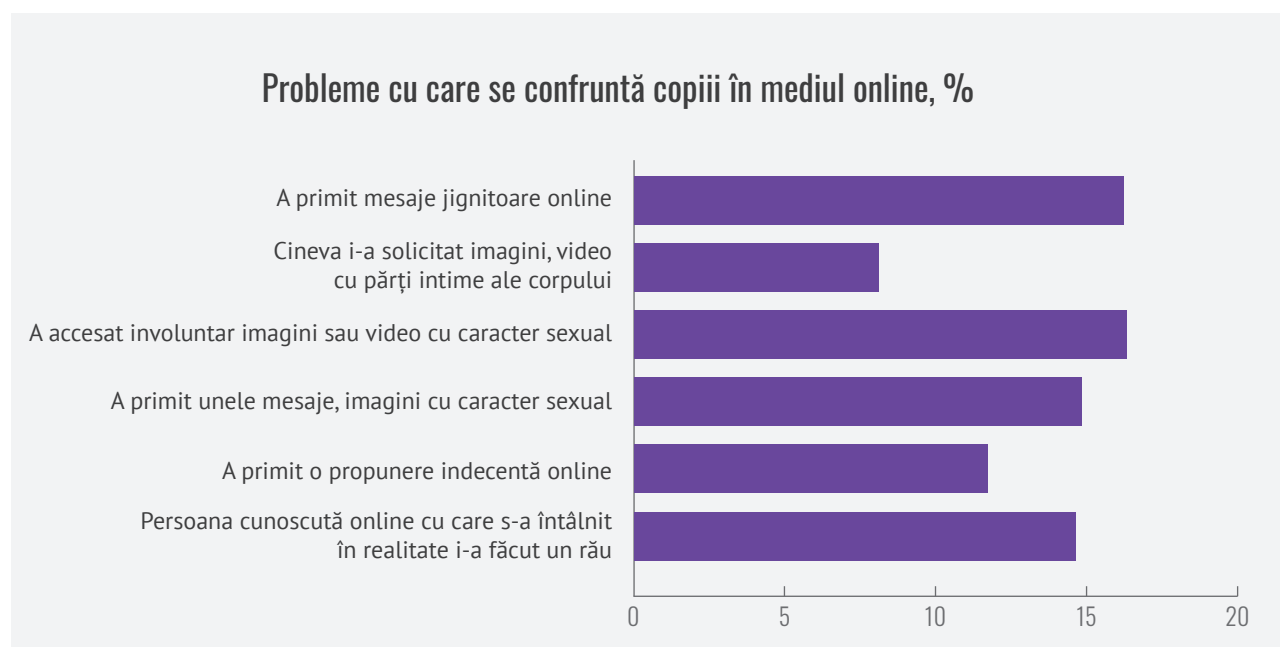
promovează violență ori a conținutului sexual online. Statisticile naționale arată că 16,3% dintre copiii de 12-15 au accesat involuntar un video sau unele imagini cu caracter sexual în timp ce navigau pe Internet și căutau alte informații online. Cu astfel de situații s-au confruntat mai des adolescenții de 15 ani (aproximativ 29,7% din numărul total de copii), riscul fiind mai redus la categoriile mai mici de vârstă (7,4% din numărul total de copii de 12 ani). Totodată, reieșind din tendințele de utilizare a Internetului de la o vârstă tot mai mică, e necesar să ținem cont de aceste riscuri și în raport cu copiii de vârstă mică.

Din categoria **riscurilor de contact**, remarcăm situațiile de grooming²⁵, la care sunt expuși copiii. Fiecare al 5-lea adolescent de 14-15 ani a primit pe Internet

fotografii, înregistrări video cu conținut sexual, iar 16,8% spun că li s-au solicitat astfel de materiale. Datele naționale atestă că transmiterea/solicitarea informațiilor cu caracter sexual pe Internet se face atât de către persoane cunoscute în viața reală, cât și de cele cunoscute doar în mediul online, iar adolescenții care au primit astfel de materiale nu ar fi avut doar o singură experiență de acest fel²⁶.

Riscurile de conduită vizează în special situațiile de hărțuire online, sexting și expunere excesivă a informațiilor cu caracter personal online. Cel mai recent studiu privind bullyingul în RM indică despre faptul că 70,8% dintre elevii din RM s-au confruntat cu o situație de hărțuire, iar 28,9% dintre aceștia au trecut prin experiența cyberbullyingului^{27,28}.

Figura 3: “Probleme ale copiilor în mediul virtual”,
Sursa: Studiul “Siguranța copiilor pe Internet”, La Strada, 2017



În primul semestru al anului 2020, a fost înregistrată o creștere cu 250% (comparativ cu anul 2019) a adresărilor din partea copiilor **ce vizează riscurile de contact și interacțiune online cu alte persoane**. În 54% dintre cazuri, problemele de relaționare sunt cazuri de cyberbullying, în 29% - probleme ce vizează relațiile dintre adolescenți, iar în 17% - situații de sexting (Figura nr. 4). 36 de cazuri de abuz sexual

online au fost raportate de copii în aceeași perioadă - de 3 ori mai mult față de perioada similară a anului trecut. Aceste date indică despre tendința în creștere a numărului de incidente neplăcute prin care trec copiii în mediul virtual²⁹.

²⁵ Grooming – proces de ademenire a copilului, stabilire a unei relații emoționale cu scopul abuzului sau exploatarei sexuale a acestuia (conform definiției Comitetului de la Lanzarote, disponibilă aici: <https://rm.coe.int/168046ebc8>);

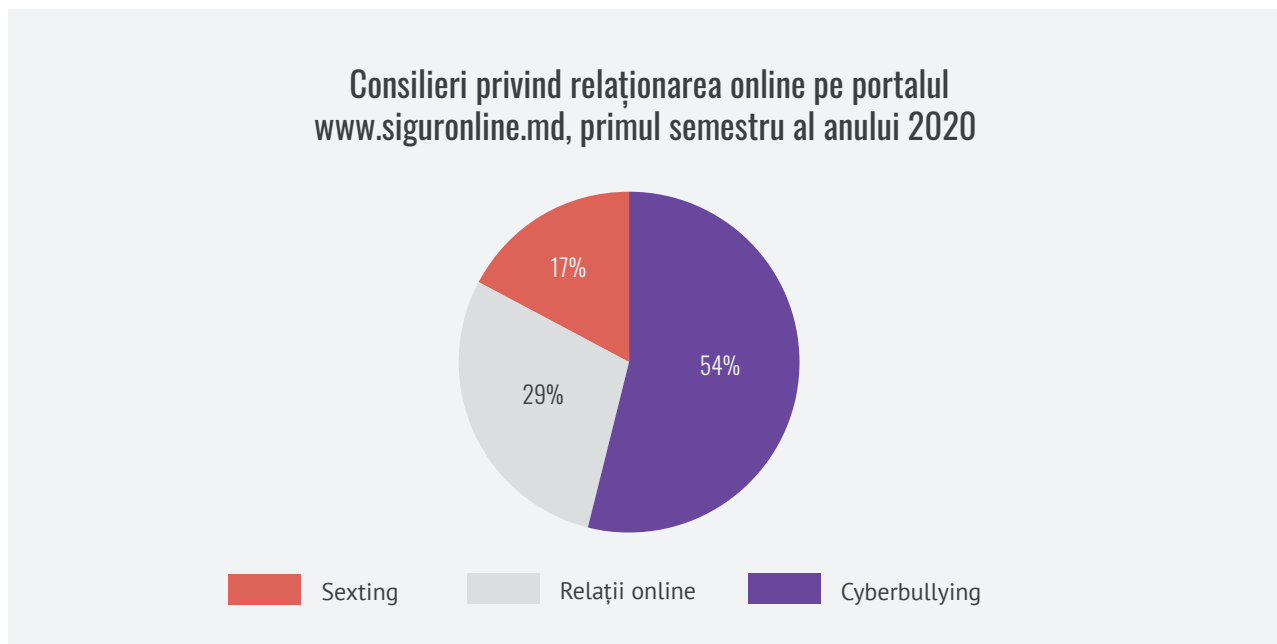
²⁶ http://lastrada.md/files/resources/3/Siguranta_copii_pe_Internet_final.pdf

²⁷ Cyberbullying – hărțuire în mediul online.

²⁸ <https://www.unicef.org/moldova/media/3146/file>

²⁹ http://lastrada.md/pic/uploaded/Siguronline%2520factsheet_1%2520sem_2020.pdf

Figura 4: “Categorii de adresări ce vizează relaționarea online, pe portalul www.siguronline.md, primul semestru al anului 2020” **Sursa:** La Strada Moldova



2.2. Siguranța online, din perspectiva elevilor

Ce cunosc copiii despre siguranța online

Datele cercetării naționale în domeniul siguranței copiilor online atestă că fiecare al 5-lea adolescent cu vârsta de 12-15 ani nu cunoaște nimic despre siguranța online. Din cele relatate de copii, 81,9% cunosc câte ceva despre siguranța online și au aflat despre unele reguli de navigare online de la părinți, prieteni, profesori sau de pe internet. Totodată,

deși s-ar părea că cunosc regulile de siguranță online, copiii nu le aplică în practică și au diverse comportamente riscante în mediul virtual³⁰. Pentru alții, siguranța online se limitează la securizarea dispozitivelor.

Aceste constatări sunt confirmate și de rezultatele discuțiilor de tip focus-grup cu elevii, desfășurate în contextul cercetării. Fiind aplicată metoda discuțiilor în baza unui studiu de caz, copiii au menționat despre acțiuni sau reacții ce contravin regulilor învățate. Răspunsurile elevilor sunt menționate în Tabelul nr. 1.

Tabelul 1: “Subiecte discutate la orele de clasă vs atitudini ale elevilor”,

Sursa: Rezultatele discuțiilor focus-grup cu copiii

Nu trebuie să discutăm online cu persoane necunoscute.	Fiind întrebați cum ar reacționa dacă ar primi un mesaj de la o persoană pe care nu o cunosc în realitate, au răspuns următoarele: “Îi voi scrie și eu, voi încerca să aflu ce vrea”. “Poate el/ea vrea, pur și simplu, să discutăm”. “Îi voi scrie, ca să nu scadă numărul de prieteni online”.
--	--

30 Siguranța copiilor pe Internet, La Strada, 2017.

Pe internet, persoanele se pot prezenta drept altcineva decât în realitate.	Copiii resping ideea că aceste persoane cu identități ascunse ar avea interese dubioase, considerând că nu prezintă niciun risc. <i>“Se poate întâmpla, dar e foarte puțin probabil. Asta se întâmplă doar în filme”.</i>
În situații neplăcute online, trebuie de cerut ajutor de la prieteni, părinți, profesori sau specialiști.	Când sunt întrebați ce ar face dacă ar fi amenințați online, copiii zic că ar bloca acea persoană. <i>“Nu aș cere ajutor de la nimeni, pentru că nimeni nu te poate ajuta, nu pot demonstra nimic și online-ul îți oferă anonim”.</i>
Nu trebuie de expediat fotografii intime.	Fiind întrebați despre modul cum ar reacționa în situații similare, spun că <i>“aș expedia o asemenea fotografie persoanei cu care sunt în relație de iubire”.</i>

Toate aceste situații ne indică despre faptul că în rezultatul activităților realizate cu elevii și discuțiilor despre siguranța online, copiii cunosc regulile de siguranță, însă nu au competențele necesare pentru a rămâne în siguranță online. Prin urmare, continuă să aibă o capacitate redusă de a acționa în mediul online, de a lua decizii responsabile și a evita situațiile periculoase. Pentru a dezvolta competențele copiilor, e necesară o schimbare în modul de abordare a subiectului, astfel încât activitățile despre siguranța online să nu se focuseze doar pe predarea regulilor de siguranță, dar pe abilitarea copilului, pe capacitatea lui de a face alegeri corecte online.

La cine s-ar adresa dacă ar avea o problemă online

Dacă li s-ar întâmpla ceva neplăcut online, copiii de 13-14 ani s-ar adresa după ajutor părinților, întâi de toate, apoi prietenilor. Adolescenții de 15-16 ani însă ar prefera să discute cu prietenii sau cu un specialist.

Aceste diferențe se explică prin specificul de vârstă al copiilor și anume prin faptul că, în perioada adolescenței, este dezvoltată dorința de autonomie și dorința de a deține controlul asupra situației și a soluționa orice problemă fără implicarea părinților. Totodată, acesta ar putea fi rezultatul unei relații precare a adolescenților cu părinții, dar și lipsei comunicării despre subiecte sensibile, legate de sexualitate și relaționare online.

Figura 5: “Persoanele de încredere la care s-ar adresa elevii din cl. a VI-a în situații de abuz online”

Sursa: Rezultatele discuțiilor focus-grup cu elevii

Persoanele de încredere la care s-ar adresa elevii din cl. a VI-a în situații de abuz online

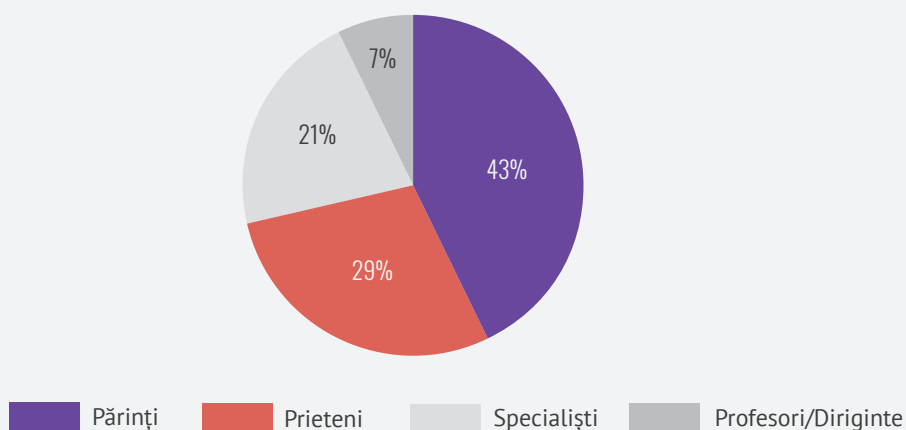
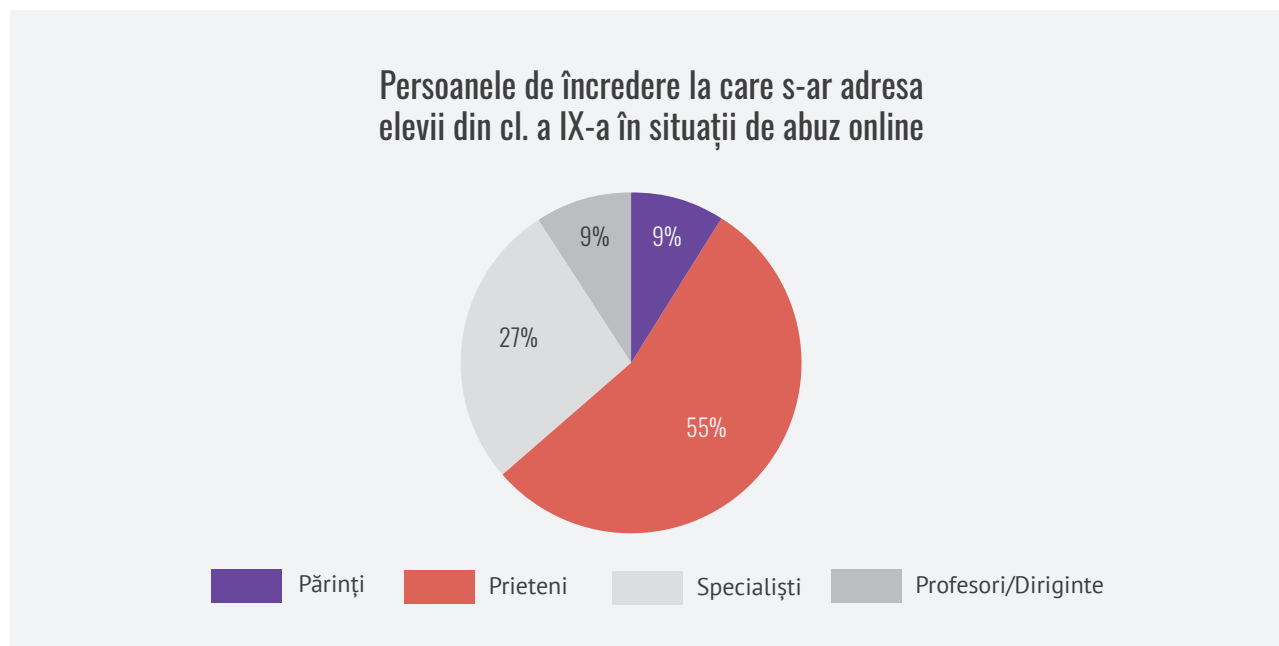


Figura 6: “Persoanele de încredere la care s-ar adresa elevii din cl. a IX-a în situații de abuz online”

Sursa: Rezultatele discuțiilor focus-grup cu elevii



În ultimul rând, copiii ar discuta cu dirigintele sau un profesor. Copiii nu au încredere în cadrele didactice, din următoarele motive:

„Dacă știe profesorul, știe toată școala.”

„Dacă îi spun despre așa ceva, apoi trebuie să ascult o oră de morală după asta.”

„Da' cu ce poate profesorul să mă ajute? Ei știu numai de lecție.”

„Ei deodată o să le spună părinților. Dacă doream, eu singură le spuneam.”

2.3. Siguranța online, din perspectiva părinților

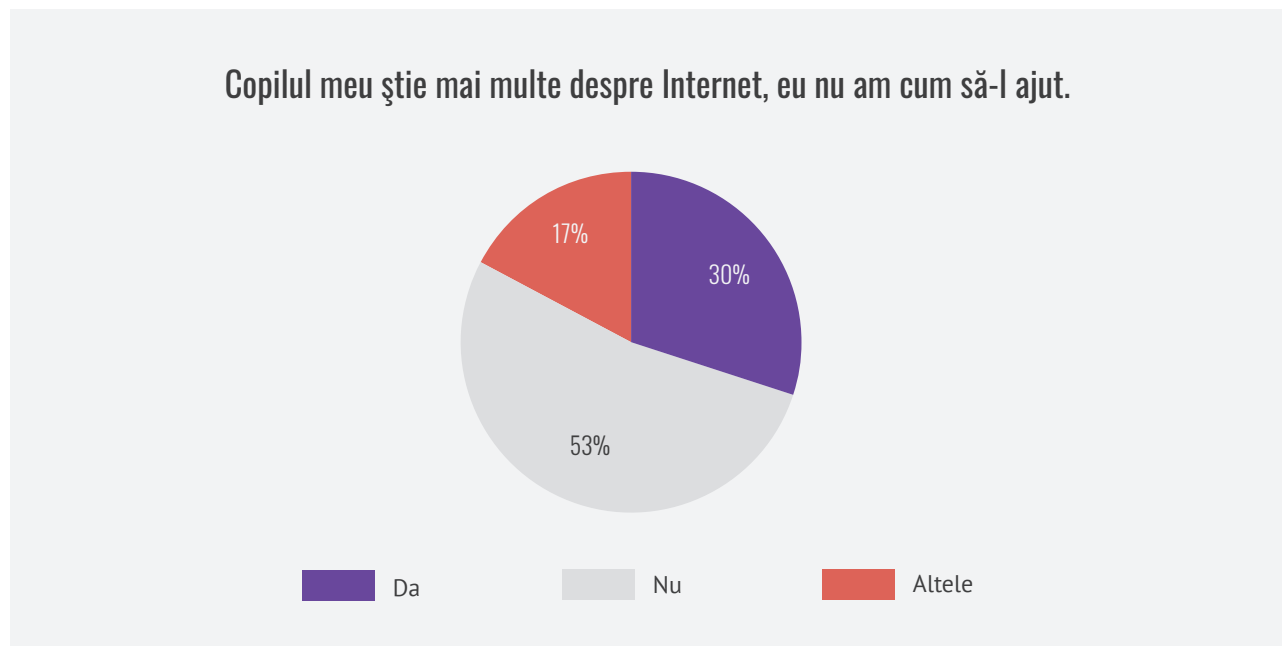
Ce cunosc despre siguranța online

Părinții din RM au o înțelegere vagă despre ce înseamnă siguranța copiilor online și despre ce ar trebui să discute cu copiii lor. Pe de-o parte, părinții consideră că copiii nu sunt informați despre cum

să utilizeze Internetul corect, ceea ce-i motiv de îngrijorare pentru ei. Pe de altă parte, părinții nu cunosc despre ce să le vorbească pentru a preveni eventualele pericole și a-i proteja. Acest fapt determină deseori reacții limitative și abordări restrictive în educație, unii dintre ei considerând că ar fi mai bine dacă copiii nu ar avea acces la Internet.

Figura 7: “Atitudinea părinților față de nivelul de informare al copiilor”

Sursa: Rezultatele discuțiilor focus-grup cu părinții

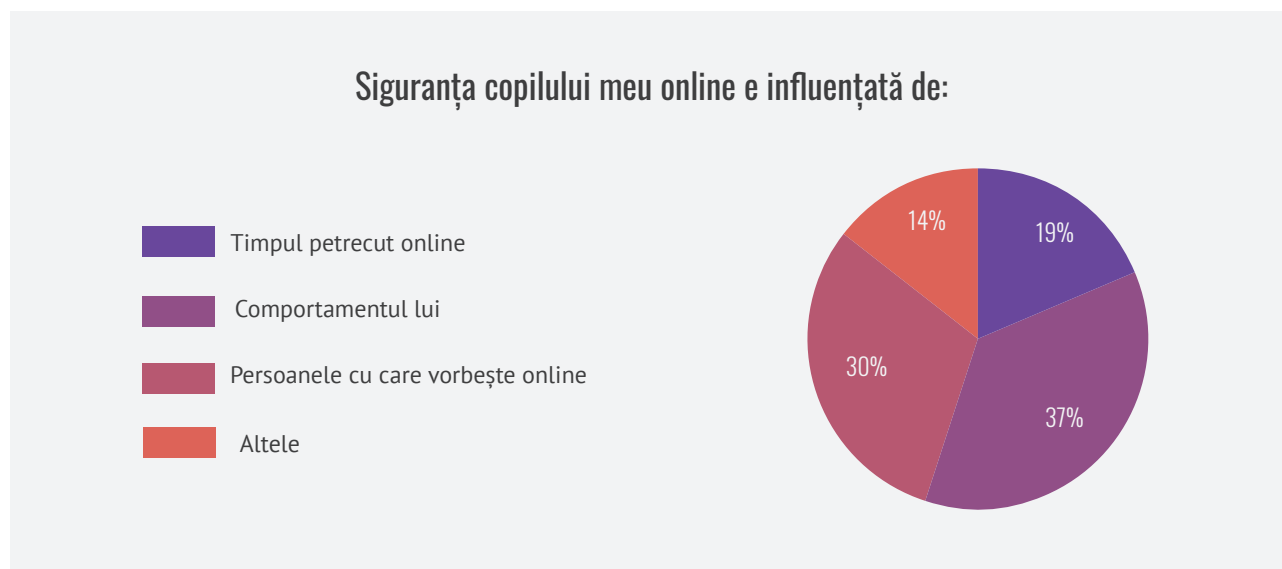


Părinții au atitudini eronate față de timpul petrecut online de către copil, considerând că aceasta este una dintre cele mai mari probleme în relația copilului cu tehnologiile digitale. Această atitudine îi face să limiteze durata activităților online ale copilului, în

loc să se focalizeze pe medierea parentală pozitivă și educarea comportamentelor sigure în mediul online. Alți factori ce influențează siguranța online a copilului sunt mediul (prietenii, colegii, societate) și școala.

Figura 8: “Factorii ce influențează siguranța copilului online”;

Sursa: Rezultatele discuțiilor focus-grup cu părinții

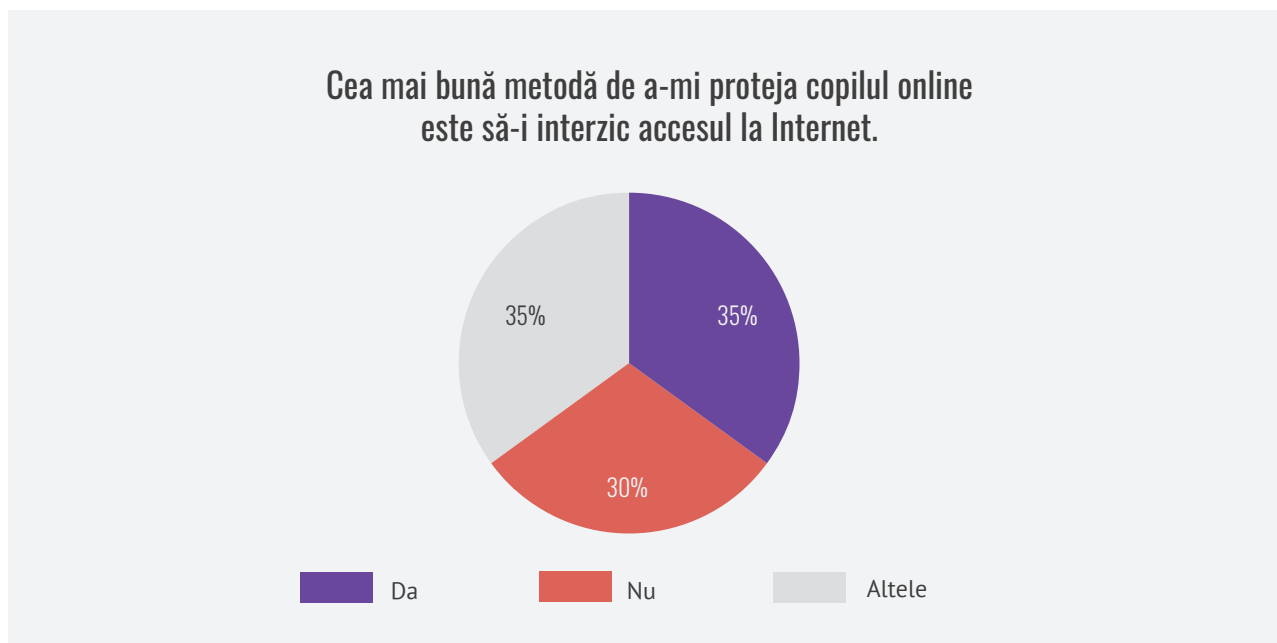


Practicile părinților de educare a comportamentelor sigure online

Rezultatele discuțiilor de tip focus-grup cu părinții indică despre faptul că 35% dintre părinți consideră că cea mai bună metodă de a-și proteja copilul de

pericolele Internetului este interzicerea accesului, 30% sunt categoric împotriva interdicției utilizării Internetului, iar restul 35% consideră că există alte metode mai bune, precum sunt supravegherea, controlul sau interzicerea accesării doar a unor pagini (Figura nr. 9).

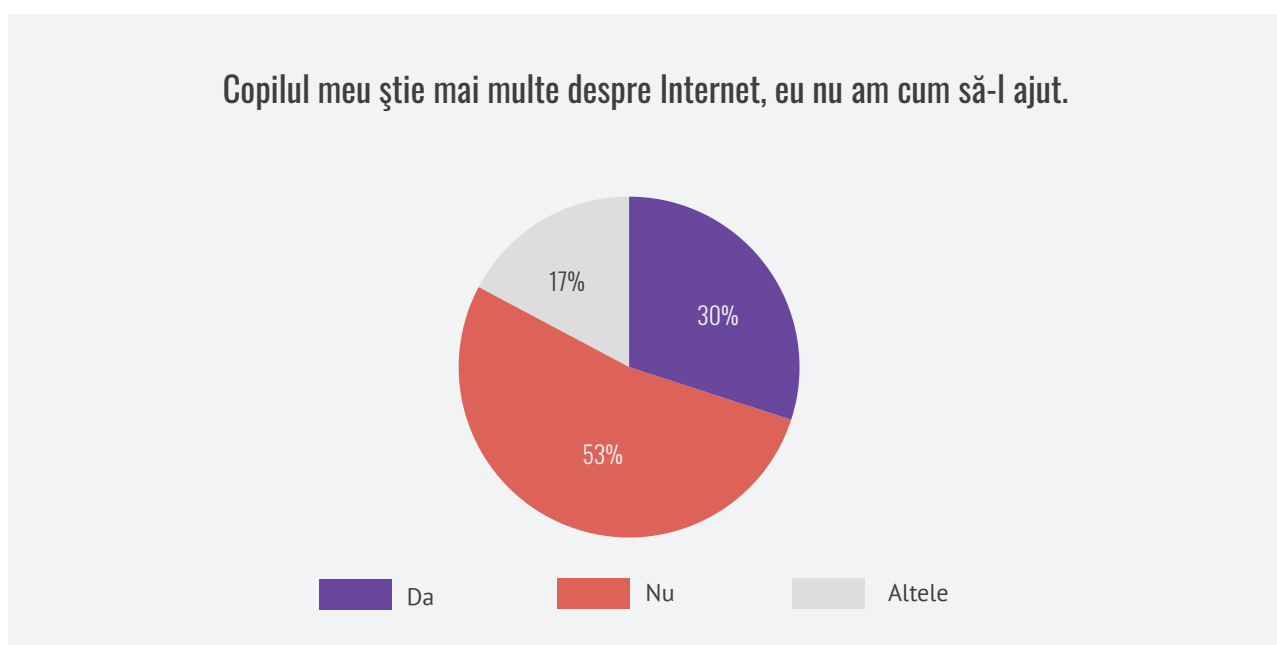
Figura 9: “Cum îmi protejez copilul online?”
Sursa: Rezultatele discuțiilor focus-grup cu părinții



O problemă identificată este “golul dintre generații” ce determină o lipsă de comunicare și înțelegere în relația părinte-copil. Deseori părinții evită să discute cu copilul lor despre Internet și activitățile lui online, din motiv că nu percep acest aspect a fi unul important în educația copiilor lor. Copiii menționează despre neînțelegerile dintre generații din cauza valorilor diferite pe care le au, în special când e vorba de rețele de socializare³¹.

Mai mult decât atât, se constată o percepție greșită în rândul părinților despre nivelul de informare a copiilor despre siguranța online și rolul pe care îl pot avea ei în ghidarea acestora. Mulți părinți consideră că copiii lor cunosc suficient de multe despre Internet, încât să poată face singuri problemelor online (Figura nr. 10). Părinții (care au oferit răspunsuri din categoria “altele”) au recunoscut că nu sunt suficient de informați, însă conștientizează că ar trebui să facă ceva pentru siguranța copilului online.

Figura 10: “Nivelul de informare a copiilor despre siguranța online, în percepțiile părinților”,
Sursa: Rezultatele discuțiilor focus-grup cu părinții



31 Siguranța copiilor pe Internet, La Strada, 2017.

2.4. Siguranța online din perspectiva cadrelor didactice

Ce cunosc despre siguranța online

Rezultatele discuțiilor cu cadrele didactice indică despre faptul că acestea nu delimitează clar măsurile de siguranță online și cele de securitate online. Atunci când desfășoară activități despre siguranța online, deseori fac referire și se limitează la regulile de utilizare a dispozitivelor digitale, de setare a unor parole sigure, de protecție față de virusii informatici, etc.

Nivelul de pregătire profesională este influențat de motivația personală a profesorului. În opinia cadrelor didactice, de obicei, profesorii și învățătorii tineri sunt motivați să participe la formări și instruiți despre siguranța online. Cadrele didactice cu experiență mai mare de muncă nu au abilități digitale de utilizare a tehnologiilor informaționale și de comunicație, utilizează mai rar Internetul și asta îi face să nu perceapă mediul online ca pericol real pentru utilizatori, inclusiv pentru copii.

“Profesorii discută între ei despre acest subiect în cadrul ședințelor. Sunt profesori care fac parte din Consiliul pentru protecția drepturilor copilului. Acolo, tot se abordează subiectul dat.”

Cadru didactic

“Cu profesorii se discută atunci când urmează a fi realizate activități prin clase.”

Cadru didactic

“Profesorii nu sunt instruiți. Este nevoie ca în școală să fie formați mai mulți profesori pe acest subiect, ca să cunoască cum să discute mai corect cu copiii. Ar fi bine ca profesorul să aibă la îndemână un ghid cu termenii principali și explicații și ca acesta să fie pe Siguronline.md, ca fiecare profesor să aibă acces, să-l studieze.”

Cadru didactic

Deși nu au o pregătire profesională corespunzătoare pentru a aborda siguranța online în activitățile didactice, majoritatea cadrelor didactice care au participat la focus-grup au identificat următoarele probleme cu care s-au confruntat elevii în școala în care predau:

Figura 11: “Probleme online ale elevilor din ciclul primar”,
Sursa: Rezultatele discuțiilor focus-grup cu cadrele didactice

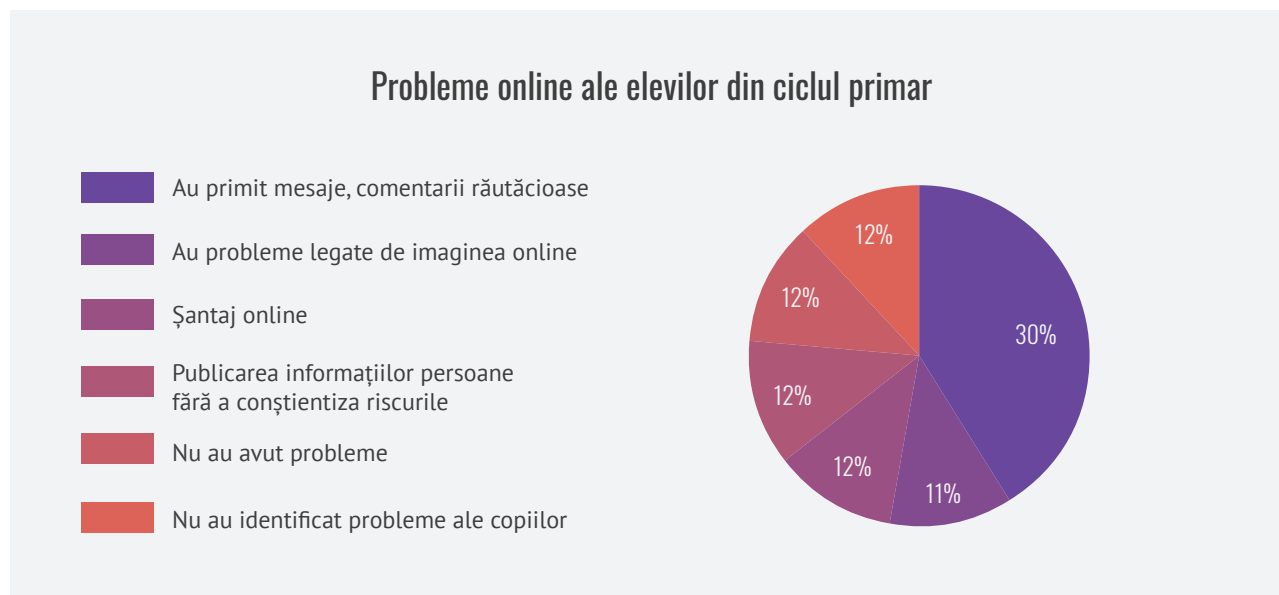
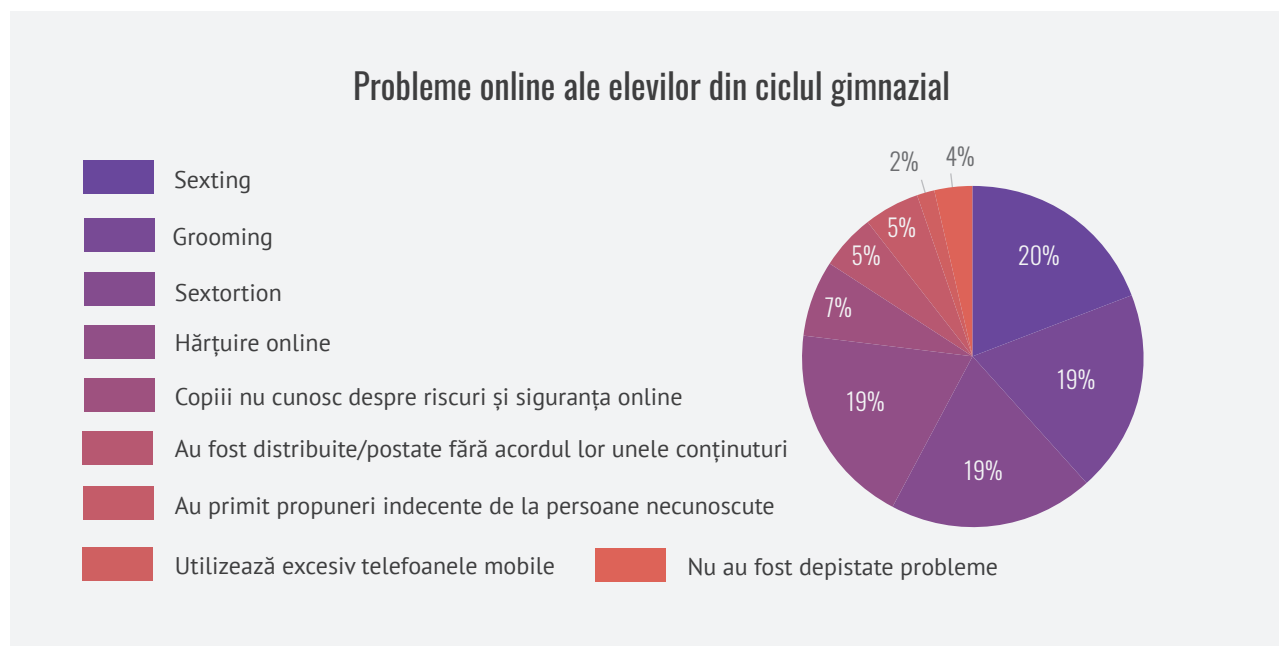


Figura 12: “Probleme online ale elevilor din ciclul gimnazial”,

Sursa: Rezultatele discuțiilor focus-grup cu cadrele didactice



Aceste date indică despre faptul că pedagogii, fiind în prima linie, ar putea cunoaște despre unele cazuri de abuz al copilului în mediul virtual sau ar putea observa unele comportamente riscante sau periculoase ale copilului în mediul online. Cu toate acestea, activitățile didactice cu elevii despre siguranța online pun mai mult accent pe securitatea digitală, iar subiecte precum relațiile online, prietenii online, transmiterea de fotografii intime sau șantajul sexual online deseori nu sunt abordate, deși aceste riscuri există, adolescenții fiind cei mai expuși.

Practicile cadrelor didactice în domeniul siguranței online

Deseori pedagogii evită să abordeze siguranța online în activitățile didactice, preferând să implice specialiști din exterior. Aceasta se întâmplă din următoarele motive:

- ✓ Subiectele care vizează siguranța online sunt complexe și există riscul transmiterii informației eronate sau unui mesaj denaturat elevilor;
- ✓ Subiectele sunt sensibile și e posibil ca unii elevii să se identifice atunci când se discută studii de caz;
- ✓ Lipsesc resurse și informații accesibile în limba română, care să ghideze profesorul atât în procesul de învățare despre siguranța online, cât și în procesul de predare a siguranței online;

- ✓ Programul profesorilor este supraîncărcat, respectiv, nu au timp suficient pentru a se pregăti de lecție și pentru a realiza aceste activități calitativ;
- ✓ Atitudinea negativă a managementului instituției de învățământ față de activitățile extra-curriculare și față de cadrele didactice implicate în diverse inițiative;
- ✓ Nu se simt confortabil să discute despre acest subiect, din motiv că nu cunosc cum să soluționeze toate problemele în domeniul siguranței online și le e frică pentru că nu ar putea răspunde tuturor întrebărilor elevilor.

Fiind întrebate de ce ar avea nevoie pentru a putea face, cu încredere, activități despre siguranța online cu elevii, cadrele didactice au menționat că:

- ✓ Au nevoie de un mentor de la care să afle mai multe informații atunci când se confruntă cu unele probleme sau neclarități în domeniul siguranței online;
- ✓ Au nevoie de mai mult timp pentru a putea realiza activitățile calitativ;
- ✓ Au nevoie de mai multe activități de instruire, ca să fie pregătiți să abordeze subiectul cu elevii;
- ✓ Au nevoie de materiale didactice la subiectul “siguranța online”.

“Pentru ca să fie mai ușor de lucrat cu copiii, ar fi bine să fie cât mai multe materiale vizuale. Diferite postere atractive. Mai multe filmulețe. Alte materiale distributive. Materiale didactice în care să fie studii

de caz reale. Astfel, elevul citește și află că cuiva i s-au întâmplat asemenea situații.”

Cadru didactic

Principalele constatări ce vizează problematica siguranței copiilor online:

1. În mediul virtual, copiii sunt expuși multiplelor riscuri, în funcție de vârstă, interesele, cunoștințele și abilitățile pe care le au, dar și în dependență de prezența ori lipsa unor persoane de încredere ce i-ar putea ghida să navigheze în siguranță online. Aceste riscuri vizează atât conținutul accesat de copil, conduita copilului, cât și persoanele cu care interacționează.
2. Deși, în rezultatul activităților despre siguranța online, copiii cunosc regulile de navigare în mediul virtual, ei nu au competențe de gândire critică, ceea ce îi determină să își asume riscuri și să acționeze contrar regulilor cunoscute.
3. Nivelul de implicare și informare a părinților despre siguranța online a copilului și acțiunile

pe care le poate întreprinde e minim. Acest factor sporește nivelul de vulnerabilitate a copilului în mediul online, întrucât acesta nu este ghidat în experiența pe care o are pe Internet.

4. Nivelul de pregătire profesională e influențat de motivația personală a profesorului. Deși multe cadre didactice evită să abordeze siguranța online în activitățile cu elevii, de cele mai multe ori, anume ei observă comportamentele riscante ale copiilor în mediul virtual și cunosc despre unele experiențe neplăcute ale copiilor. Este un fapt cert, care reconfirmă ipoteza că școala e locul și mediul cel mai propice în care copilului i se pot dezvolta abilitățile de gândire critică și care ar putea interveni și oferi suport copilului în situație de abuz online.

The background is a solid purple color. It features several overlapping circles of different sizes and shades. A large, light purple circle is in the upper right corner. A medium-sized orange circle is on the left side, partially overlapping the text. A smaller orange circle is at the bottom center. Another orange circle is partially visible on the far left edge.

3. Politici și practici naționale în domeniul educațional

3.1. Cadrul politicilor publice naționale și cadrul normativ

Cadrul politicilor publice naționale

Planul de acțiuni pentru promovarea siguranței pe Internet a copiilor și adolescenților pentru anii 2017-2020

Pentru prima dată, siguranța copiilor online a devenit subiect al unui plan național de acțiuni în RM abia în anul 2017. Atunci, la nivel guvernamental a fost recunoscut rolul autorităților și unor structuri publice și private, sectorului asociativ în promovarea siguranței copiilor online. Prin aprobarea Planului de Acțiuni, sectorul educației și-a asumat responsabilitatea pentru organizarea regulată a activităților de informare și sensibilizare a elevilor despre siguranța online, în contextul Zilei Siguranței Online și Lunii Securității Cibernetică. Prin acest document de politici, siguranța online, pentru prima dată, a fost recunoscută oficial parte a programului de activități extra-curriculare, a activităților neformale și informale realizate cu elevii de toate vârstele.

Felul în care au evoluat lucrurile, de fapt, în procesul educațional a determinat abordarea siguranței online și în cadrul curriculumului, nu doar ca activitate extra-școlară. În ultimii 3 ani au fost realizate activități despre siguranța online, atât pentru elevii ciclului primar, gimnazial, cât și pentru elevii de liceu, în cadrul disciplinelor obligatorii și opționale. În mod special, remarcăm dezvoltarea unor programe educaționale menite să contribuie la alfabetizarea digitală a copiilor, precum este disciplina "Educație pentru media" – disciplină opțională pentru ciclul gimnazial și liceal, dar și dezvoltarea disciplinei "Educația digitală", pentru ciclul primar.

Strategia de dezvoltare a educației pentru anii 2014-2020 "Educația 2020"³²

Una dintre direcțiile acestei strategii este integrarea eficientă a TIC în educație. În acest sens, au fost setate următoarele obiective specifice:

~ Obiectivul 3.1. Sporirea accesului la educație de

calitate prin dotarea instituțiilor de învățământ cu echipamente moderne, utile procesului de studii;

- ~ Obiectivul 3.2. Dezvoltarea competențelor digitale prin elaborarea și aplicarea conținuturilor educaționale digitale în procesul de învățământ;
- ~ Obiectivul 3.3. Creșterea eficacității și eficientizarea managementului școlar la nivel de sistem, școală și clasă prin intermediul tehnologiilor informaționale;

Totodată, constatăm că, în contextul digitalizării procesului educațional, acțiuni menite să contribuie la siguranța copilului în mediul virtual nu au fost planificate.

Cadrul normativ

Codul Educației

Art. 135 alin. (1) lit. j) din Codul Educației stabilește obligația personalului didactic de a informa elevii despre toate formele de violență și manifestările comportamentale ale acestora, despre persoanele și instituțiile la care se pot adresa atunci când sunt supuși unui act de abuz. Este o indicație expresă a obligației cadrului didactic de a informa elevii și despre formele de violență online și cele mai noi forme de abuz online, precum sunt groomingul, sextortion, cyberbullying, etc.; despre cum se manifestă acestea și unde pot cere ajutor în aceste situații.

Instrucțiunile privind mecanismul intersectorial de cooperare privind identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului

Cadrul normativ privind protecția copiilor față de violență în instituția de învățământ este unul complex, fiind dezvoltat odată cu aprobarea Instrucțiunilor privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și

³² Strategia de dezvoltare a educației pentru anii 2014-2020 "Educația-2020" aprobată prin Hotărârea nr. 944 din 14.11.2014.

potențiale victime ale violenței, neglijării, exploatării și traficului³³. În baza acestui mecanism intersectorial, au fost dezvoltate ulterior proceduri de organizare instituțională și de intervenție a lucrătorilor instituțiilor de învățământ în cazuri de abuz, neglijare, exploatare, trafic. Aceste proceduri vizează, la general, acțiunile în domeniul prevenirii și protecției copiilor față de violență în instituția de învățământ, **fără a se referi la specificul cazurilor de abuz în mediul online.**

Metodologia de aplicare a procedurilor de organizare instituțională **recomandă desfășurarea activităților cu elevii despre riscurile online, ca parte a programului de prevenție primară, adresate copiilor**³⁴. Cât privește procedurile de intervenție a lucrătorilor instituției de învățământ, acestea nu fac referire la situațiile de abuz în mediul online, nici nu delimitează între formele de abuz în funcție de modalitatea de comitere a abuzului față de copil – cu sau fără utilizarea TIC.

Așadar, deși Hotărârea Guvernului nr. 270 din 8 aprilie 2014³⁵, la pct. 5.4. prin copil-victimă are în vedere copilul căruia, prin acțiuni sau inacțiuni, i s-au adus daune morale, fizice sau materiale ca rezultat al violenței, neglijării, exploatării, inclusiv prin intermediul tehnologiilor informaționale, traficului, etc, acțiuni specifice acestui tip de abuz nu sunt reglementate și nu este definit abuzul online.

Ghidul de implementare a Politicii de Protecție a Copilului³⁶

Ghidul de implementare a Politicii de Protecție a Copilului în Instituția de Învățământ include un capitol separat dedicat regulilor de utilizare a Internetului și TIC în instituție. E recomandată, pe de-o parte, stabilirea unor reguli clare de utilizare a telefoanelor mobile, a tabletelor, computerelor personale, reglementarea unor reguli clare de utilizare a Internetului, dar și stabilirea unor filtre pentru controlul conținutului. Așadar, acest Ghid de implementare stabilește clar că este sarcina Instituției de a se asigura că preocupările legate de protecția copilului sunt abordate în Politicile școlii de utilizare a Internetului și a TIC.

Standarde de competențe digitale ale elevilor din ciclul primar, gimnazial și liceal³⁷

Aceste Standarde descriu 10 competențe-cheie ce ar trebui dezvoltate la elevii din ciclul primar, gimnazial și liceal:

1. Utilizarea sistemelor informatice;
2. Procesarea documentelor de tip text;
3. Crearea și editarea imaginilor;
4. Elaborarea, derularea și difuzarea prezentărilor electronice;
5. Procesarea datelor cu ajutorul mijloacelor de calcul tabelar;
6. Utilizarea Internetului;
7. Comunicarea în medii virtuale;
8. Elaborarea și implementarea algoritmilor;
9. Organizarea și prelucrarea informației cu ajutorul sistemelor de gestiune a bazelor de date;
10. Respectarea normelor de etică și securitate informațională.

Deși punctele 6, 7 și 10 ale acestor standarde ar putea face referire la unele aspecte ale siguranței online, totuși acestea vizează direct utilizarea tehnologiilor și securitatea informațională. Spre exemplu, pct. 6 se referă la următoarele aspecte: navigarea în Internet, accesarea paginilor web, căutarea informațiilor în baza cuvintelor-cheie distincte, căutarea informațiilor în baza criteriilor simple de căutare, organizarea și gestionarea informațiilor descărcate din Internet, etc.

Pct. 7 privind comunicarea în medii virtuale vizează următoarele sub-aspecte: comunicarea prin telefonie digitală, rețelele de socializare și mesagerie instantă, crearea și gestionarea conturilor personale în mediile virtuale de comunicare, utilizarea mijloacelor de creare în spațiile virtuale a propriilor identități digitale.

Pct. 10 “Respectarea normelor de etică și securitate informațională” vizează atât aspectele privind proprietatea intelectuală (definirea noțiunii de proprietate intelectuală, respectarea drepturilor de

33 Hotărârea Guvernului nr. 270 din 08.04.2014 cu privire la aprobarea Instrucțiunilor privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului, publicată la 18.04.2014 în Monitorul Oficial nr. 92-98, art. 297.

34 Metodologia de aplicare a procedurii de organizare instituțională și de intervenție a lucrătorilor instituțiilor de învățământ preuniversitar în cazurile de abuz, neglijare, exploatare, trafic al copilului, aprobată prin Ordinul Ministerului Educației nr. 858 din 23 august 2013.

35 Hotărârea Guvernului nr. 270 din 8 aprilie 2014 privind aprobarea Instrucțiunilor privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului.

36 https://mecc.gov.md/sites/default/files/politica_de_protectie_a_copiluluighid_de_implementare.pdf

37 Standarde de competențe digitale ale elevilor din ciclul primar, gimnazial și liceal, aprobate prin Ordinul Ministerului Educației nr. 862 din 07 septembrie 2015, disponibil la https://mecc.gov.md/sites/default/files/cnc4_final_competente_digitale_elevi_22iulie2015_1.pdf

autor asupra informațiilor digitale, etc.), securitate digitală (definirea noțiunii de securitate digitală, respectarea regulilor de asigurare a securității digitale, utilizarea în situații reale a mijloacelor de asigurare a securității digitale, etc), cât și etica digitală (definirea noțiunii de etică digitală, respectarea regulilor de etichetă digitală, promovarea regulilor de etică digitală, etc.).

Standardele naționale nu abordează aspecte precum protejarea sănătății și bunăstării emoționale a copilului în mediul online sau aspecte precum sunt protejarea datelor personale și confidențialității, înțelegerea modului în care trebuie utilizată și distribuită informația personală, astfel încât să ne putem proteja pe sine și alte persoane de pericole, așa precum e prevăzut în Cadrul european al competențelor digitale pentru cetățeni DigComp.

3.2. Practicile instituțiilor de învățământ în domeniul siguranței copiilor online

Practicile instituțiilor de învățământ din RM, de promovare a siguranței online a copilului, descrise în acest capitol, vor fi analizate din perspectiva corespunderii acestora cu standardele europene ce definesc Modelul de abordare comprehensivă a siguranței online în școală.

a. Guvernarea școlii

Cadrul politicilor instituționale în domeniul siguranței copiilor online

Planurile manageriale

Una dintre bunele practici menționate de participanții la focus-grup este includerea siguranței online în planul managerial al instituției de învățământ, conform Programului de activități extrașcolare elaborat de MECC. Aceasta permite o mai bună organizare a activităților și alocarea timpului suficient pentru pregătirea activităților tematice.

“Este planul managerial. Acesta este întocmit în baza planului de la minister. Când vin circularele, atunci pot fi uneori indicate anumite subiecte care să fie abordate (aceasta se referă la activități, în general). În principiu, se cunoaște de la începutul anului că va fi luna februarie, când vor fi realizate activități care se referă la mediul online.”

Director adjunct pentru educație

Alte instituții de învățământ organizează activități despre siguranța online doar dacă este emisă o circulară în acest sens:

“Desfășurăm activități în perioadele menționate de circulare. Problema este că circularele vin cu 2 sau 3 zile înainte ca activitățile să fie realizate. Nu prea

se reușește o pregătire calitativă. Subiectul este abordat superficial, mai mult pentru bifă. Se face o notă pentru direcție că au fost realizate X activități cu X elevi implicați.”

Director adjunct pentru educație

Politica de Protecție a Copilului

Politica de Protecție a Copilului este un document de politici instituționale ce vizează protecția copiilor față de orice formă de violență în instituția de învățământ. Conform recomandărilor aprobate de MECC, este în sarcina fiecărei instituții de învățământ să asigure reflectarea preocupărilor legate de protecția copilului în politicile școlii de utilizare a Internetului și tehnologiilor de informare și comunicare. La fel, Ghidul de implementare a Politicii de Protecție în Instituția de Învățământ³⁸ prevede un capitol separat dedicat regulilor de utilizare a Internetului și TIC în instituție, cu următoarea structură recomandată:

- ~ Reguli clare de utilizare a telefoanelor mobile, tabletelor, laptopurilor, computerelor personale, consolelor video;
- ~ Reguli clare de utilizare a internetului;
- ~ Stabilirea unor filtre pentru controlul conținutului.

Acestea însă nu au scopul de a abilita copilul să utilizeze tehnologiile în siguranță, nu stabilesc unele repere pentru identificarea cazurilor de abuz online și nu prevăd acțiuni de intervenție timpurie, dar se limitează doar la aspecte ce vizează utilizarea tehnologiilor în școală și securizarea accesului la Internet, prin setarea unor filtre de conținut.

Din toate cele 48 de instituții de învățământ în care activează cadrele didactice ce au participat la discuții focus-grup, doar în una există o politică de protecție a copilului, care are scopul să protejeze copilul față

38 https://mecc.gov.md/sites/default/files/politica_de_protectie_a_copilului/ghid_de_implementare.pdf

de orice formă de abuz și să creeze un mediu sigur în școală. Documentul însă nu include aspecte ce vizează protecția copilului față de abuzurile în mediul online.

Regulamentele instituționale

Regulamentul-tip de organizare și funcționare a instituțiilor de învățământ primar și secundar, aprobat de MECC, nu stabilește măsuri ce vizează siguranța copiilor online. Acest act normativ stabilește niște interdicții generale, menite să asigure o funcționare adecvată a procesului educațional, protejând bunăstarea psihică și emoțională a elevilor și angajaților, cum ar fi:

- ~ La pct. 11 c) “În instituție se interzice implicarea în orice activități ce încalcă normele generale de moralitate și periclitează integritatea fizică și psihică a elevilor și angajaților”;
- ~ Pct. 147 g) “Dirigintele are atribuția de a observa comportamentul elevilor, inclusiv în scopul prevenirii abuzului, neglijării, exploatării copilului și raportării cazurilor suspecte sau confirmate de abuz”;
- ~ Pct. 190 lit. h) “Este interzis elevilor să posede și să difuzeze materiale cu caracter obscen sau pornografic”;
- ~ Pct. 190 lit. i) “Este interzis elevilor să utilizeze telefoane mobile în timpul orelor de curs, examenelor și concursurilor”;
- ~ Pct. 190 lit. k) “Este interzis elevilor să aducă jigniri și să manifeste agresivitate în limbaj și în comportament față de colegi și față de personalul Instituției”.

Acest act normativ nu indică măsuri specifice ce ar viza siguranța copiilor în mediul online, protecția acestora față de riscurile online sau obligația angajaților instituției de a preveni sau interveni în cazuri de abuz online.

La modul practic, Regulamentul intern poate include aspecte ce vizează publicarea imaginilor cu un copil și prevederi despre modul de utilizare a telefoanelor mobile în instituția de învățământ. Rezultatele discuțiilor focus-grup indică despre faptul că alte aspecte ale siguranței online, de obicei, nu sunt reflectate în Regulamentul de organizare și funcționare a instituției de învățământ.

Coordonarea activităților despre siguranța online în instituția de învățământ

Cadrul normativ actual nu stabilește roluri specifice de coordonare a activităților de promovare a siguranței

online în instituția de învățământ. În toate cele 48 de instituții de învățământ, directorul adjunct pentru educație este responsabil de organizarea activităților despre siguranța online în instituția de învățământ, în virtutea responsabilităților pe care le au pentru organizarea tuturor activităților extra-curriculare.

“Vine o circulară de la direcția de învățământ. Directorul adjunct pentru educație anunță diriginții și organizează o ședință. Împreună întocmesc un plan cu activități. Diriginții pregătesc unele activități cu elevii.”

Cadru didactic

Cadrele didactice consultă directorul adjunct pentru educație atunci când se confruntă cu unele probleme în desfășurarea activităților sau când au identificat unele situații problematice ale copiilor în mediul online. La fel, cadrele didactice pot apela și la: psihologul școlar, coordonatorul ANET, profesorul de informatică. Cu toate acestea, cunoștințele pe care le au profesorii de informatică în domeniul colectării, stocării, prelucrării, transmiterii ori difuzării automate a informației cu ajutorul echipamentelor digitale nu sunt suficiente pentru a ghida ceilalți profesori în domeniul siguranței copiilor online, întrucât siguranța online vizează comportamentele online ale copiilor și nu reflectă obiectul de studiu al Informaticii.

În majoritatea cazurilor, directorii adjuncți pentru educație nu au nicio formare în domeniul siguranței online. Siguranța online este subiect al activităților extra-curriculare, respectiv directorul adjunct, chiar dacă coordonează desfășurarea activităților la această temă, nu este obligat să participe la instruirii specifice în domeniu.

“De obicei, este directorul adjunct pentru educație care răspunde de realizarea acestor activități. Problema este că activitățile din fiecare lună sunt diferite. Acestea toate se organizează mai superficial. Directorul adjunct pentru educație nici nu are suficientă pregătire, instruire ca să ghideze cumva și profesorii să abordeze mai interesant pentru copii acest subiect. Copiilor le place când la aceste teme abordate în afara orelor, vin alte persoane din exterior.”

Director adjunct pentru educație

Rolul elevilor în promovarea siguranței online

În discuțiile focus-grup, nu am identificat practici de implicare a elevilor în promovarea siguranței online în școală, din proprie inițiativă, la nivelul consiliilor elevilor. De obicei, copiii se implică în activități despre

siguranța online la inițiativa cadrelor didactice, fiind solicitați să facă unele proiecte. Într-o instituție de învățământ, elevii din clasele de gimnaziu sunt implicați în activități de informare a copiilor mai mici despre siguranța online.

“Copiii mai mari sunt implicați în activități de a informa copiii mai mici despre siguranța online.”

Cadru didactic

Cadrelor didactice au menționat necesitatea implicării elevilor sau unor specialiști din afara instituției de învățământ în realizarea activităților cu copiii despre siguranța online. Profesorii au constatat că elevii au o abordare mai serioasă atunci când despre aceste subiecte le vorbește o persoană pe care nu o cunosc, decât atunci când o face profesorul.

b. Formarea personalului didactic

Formarea cadrelor didactice în domeniul siguranței copiilor online

Siguranța online a copilului nu este abordată distinct în programele de formare continuă a cadrelor didactice. Mai multe module tematice și teme abordează aspecte ce vizează digitalizarea procesului educațional și integrarea TIC în procesul educațional:

- ~ Integrarea TIC în procesul educațional;
- ~ Tehnologii avansate de instruire prin TIC;
- ~ Dezvoltarea competențelor digitale ale cadrelor didactice;
- ~ Inițierea în utilizarea tehnologiilor informaționale în învățământ;
- ~ Tehnologii și resurse educaționale moderne, etc³⁹.

Un modul distinct despre “Etica utilizatorului și securitatea online” este inclus în Planul de formare continuă a cadrelor didactice și a celor cu funcții de conducere din cadrul Universității Pedagogice de Stat “Ion Creangă” din Chișinău⁴⁰. La fel, sunt organizate module specifice de formare continuă la discipline ce includ subiecte despre siguranța online cum ar fi dezvoltarea personală, informatică, învățământ extra-școlar ori educația pentru media⁴¹. Cu toate acestea, nu este clar ce aspecte ale siguranței online sunt abordate în cadrul acestor activități de formare continuă sau dacă acestea vizează doar securitatea online.

“Profesorii discută între ei despre acest subiect în cadrul ședințelor. Sunt profesori care fac parte din Consiliul pentru protecția drepturilor copilului. Acolo, tot se abordează subiectul dat.”

Cadru didactic

“Cu profesorii se discută atunci când urmează a fi realizate activități prin clase.”

Cadru didactic

“Profesorii nu sunt instruiți. Este nevoie ca în școală să fie formați mai mulți profesori pe acest subiect ca să cunoască cum să discute mai corect cu copiii. Ar fi bine ca profesorul să aibă la îndemână un ghid cu termenii principali și explicații și ca aceasta să fie pe siguronline.md, ca fiecare profesor să aibă acces. Să-l studieze.”

Cadru didactic

c. Politici și proceduri

În instituțiile de învățământ în care au fost desfășurate discuții focus-grup lipsesc proceduri de intervenție în cazuri de abuz online. Majoritatea cadrelor didactice au declarat că nu s-au confruntat direct cu cazuri de abuz al copiilor în mediul online, respectiv, nu cunosc ce acțiuni trebuie să întreprindă în astfel de situații.

“Am discutat cu fata. Fata a șters acele fotografii. A înțeles că poate să se ajungă la situații mai urâte și astfel totul s-a liniștit.”

Cadru didactic

Cu părere de rău, însă, aceste situații nu pot fi soluționate doar determinând copilul să-și șteargă fotografiile. Odată expediate, fotografiile au ajuns să fie văzute și de către altcineva sau chiar pot ajunge să fie distribuite pe rețele de socializare, devenind accesibile pentru oricine. Cu fiecare vizualizare, copilul poate fi expus repetat victimizării, asta făcându-l să re trăiască emoțiile negative ale abuzului. Pe de altă parte, odată vizualizate de către colegii de clasă, aceste fotografii pot ajunge să fie distribuite și altor persoane, se pot face glume pe seama copilului sau poate ajunge să fie hărțuit online.

Deși funcționează un mecanism intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor-victime și potențiale victime ale violenței, neglijenței, exploatării și traficului, cadrele didactice au avut păreri

³⁹ <https://mecc.gov.md/ro/content/centre-de-formare-continua-0>

⁴⁰ https://mecc.gov.md/sites/default/files/universitatea_pedagogica_de_stat_ion_creanga_din_chisinau_0.pdf

⁴¹ https://mecc.gov.md/sites/default/files/universitatea_de_stat_din_moldova_0.pdf

contradictorii despre aplicabilitatea mecanismului intersectorial existent⁴² în cazuri de abuz online. Unele cadre didactice consideră că în situațiile de abuz în mediul online trebuie respectate aceleași proceduri ca și în celelalte cazuri de abuz. Alții au respins categoric ideea aplicării acestui instrument, specificând că acestea nu pot fi aplicate în cazurile de abuz online, întrucât procedurile existente nu iau în calcul specificul acestor cazuri și nu furnizează suficiente instrumente și claritate cadrelor didactice în legătură cu acțiunile ce ar trebui să le întreprindă.

“Profesorilor le este mai complicat să discute cu copiii despre astfel de situații. Ei nu prea știu cum să procedeze mai corect.”

Cadru didactic

Cadrele didactice au menționat și alte provocări:

- ~ Indiferența altor colegi (cadre didactice), care îi determină să nu se implice și să nu-i ofere ajutor/suport copilului;
- ~ Atitudinile stereotipizate față de cazurile de abuz sexual online, care îi pot determina să învinovățească copilul pentru ce i s-a întâmplat și să acționeze în detrimentul copilului;
- ~ Necunoașterea semnelor unui posibil abuz sexual online, fie neglijarea situațiilor neplăcute care i s-au întâmplat copilului în mediul online și care nu sunt percepute ca forme de abuz, ceea ce îi poate determina să fie indiferenți în asemenea cazuri.

“Neapărat am avea nevoie de mai multe resurse și o claritate în ce se poate de făcut în situațiile când astfel de situații li se întâmplă copiilor.”

Cadru didactic

Totodată, în discuțiile cu specialiștii din cadrul Serviciilor de Asistență Psiho-pedagogică, dar și cu psihologii școlari, referitor la cazurile de abuz sexual online am constatat că sunt puțin informați la acest subiect. Specialiștilor le este frică să intervină în astfel de situații, întrucât nu cunosc exact ce ar trebui să facă, pentru a nu dăuna copilului.

Specialiștii au recunoscut că motivul inacțiunilor lor vine din lipsa unor instrucțiuni clare în acest sens. Lipsa instrucțiunilor clare o simt și asistenții sociali, și autoritățile tutelare, dar și poliția care întâmpină dificultăți în identificarea cazurilor și realizarea intervențiilor corespunzătoare. La fel, lipsa cunoștințelor despre specificul abuzurilor online, elementele de care ar trebui să se țină cont, modul în care se desfășoară și evoluează abuzul și posibilele consecințe ale abuzului online creează impedimente în asigurarea unui răspuns eficient din partea specialiștilor din domeniu.

d. Implicarea părinților

Lipsește un program de educație parentală în domeniul siguranței copiilor online, ce ar ține cont de evoluțiile din era digitală, riscurile la care se expun copiii și necesarul de informații pe care trebuie să-l cunoască părinții pentru a-și proteja copiii de riscurile online.

Sunt organizate sporadic activități de informare a părinților despre siguranța online. Doar un profesor ne-a menționat despre faptul că nu a discutat niciodată cu părinții despre acest subiect și nu cunoaște dacă s-au făcut activități cu părinții la această temă în școala în care predă.

“La adunări se spune părinților să observe ce fac copiii lor în mediul online.”

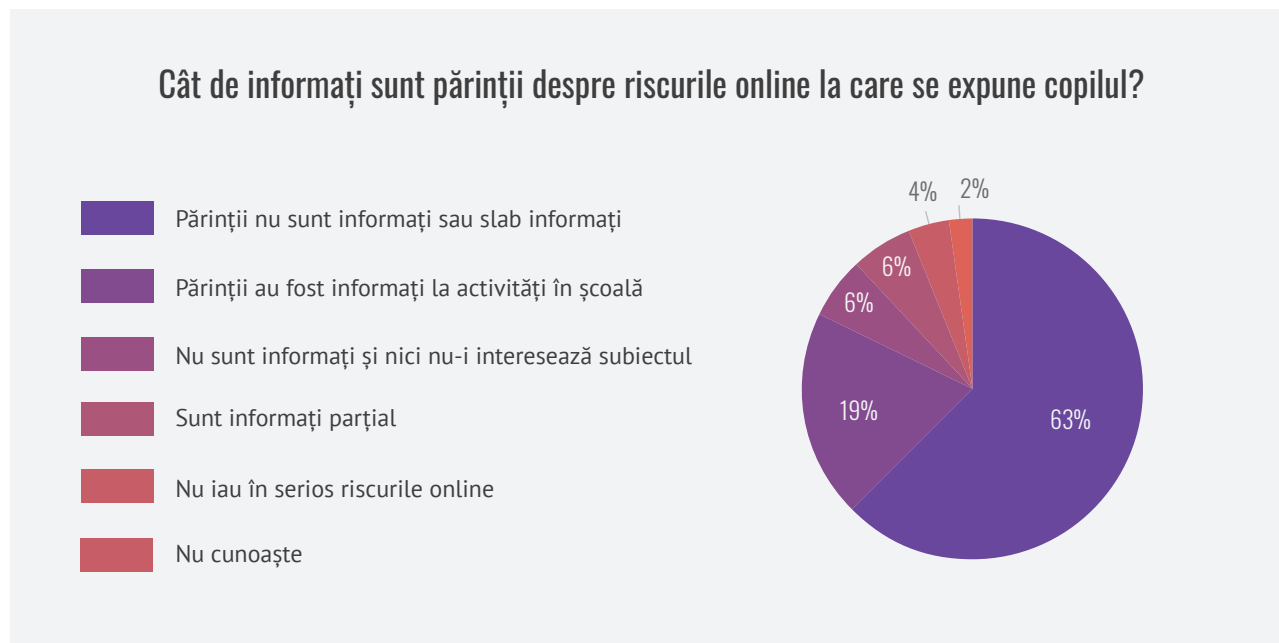
Cadru didactic

Deseori, părinții nu cunosc despre riscurile online la care se expun copiii lor. Prin urmare, nu știu cum să le facă față, dar nici nu fac ceva în acest sens, pasând responsabilitatea cadrelor didactice (Figura nr. 13).

⁴² Hotărârea Guvernului nr. 270 din 08.04.2014 cu privire la aprobarea Instrucțiunilor privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului.

Figura 13: „Nivelul de informare al părinților despre riscurile online”,

Sursa: Rezultatele discuțiilor focus-grup cu cadrele didactice.



Una dintre provocările cu care se confruntă cadrele didactice în organizarea activităților de informare a părinților este lipsa resurselor didactice, pliantelor informative și altor materiale distributive pentru părinți. O altă provocare e faptul că mulți părinți sunt plecați peste hotare, iar copiii rămân în grija bunelor. Nivelul de informare și înțelegere al bunelor despre ce înseamnă Internet și ce face copilul online sau riscurile online e minim. În asemenea cazuri, copilul, de obicei, are libertatea de a naviga online cât își dorește, fără a i se impune anumite limite, fără a-i asigura o experiență sigură online.

Atitudinile și modul de implicare a părinților în educarea unor comportamente sigure online sunt diferite, în funcție de vârsta copiilor. Majoritatea părinților copiilor de vârstă mică (7-10 ani) sunt deschiși și interesați să colaboreze pentru a-și învăța copilul să navigheze în siguranță.

Cât privește părinții copiilor din ciclul gimnazial, aceștia au un nivel înalt de rezistență față de subiect și nu conștientizează riscurile de contact sau conduită la care se poate expune copilul lor online. Mai mulți profesori s-au confruntat cu problema dezinteresului părinților pentru siguranța online la ședințele de clasă, din motiv că ar fi suficient de informați și nu ar avea nevoie de astfel de informații. Unii părinți consideră că copilul lor nu are acces la Internet și astfel nu se expune pericolului.

„Am discutat la adunarea cu părinții despre siguranța online. Dar ei nu sunt interesați și nu sunt atenți. Ei consideră că atâta timp cât nu i s-a întâmplat copilului lor, informația nu-i pentru ei.”

Cadru didactic

e. Educația despre siguranța online

Siguranța online este abordată în discuție cu elevii atât în cadrul disciplinelor obligatorii sau opționale, cât și în contextul Zilei Siguranței pe Internet sau a Lunarului Securității Cibernetică. Subiecte ce vizează siguranța online se regăsesc transversal în cadrul mai multor discipline obligatorii și opționale (a se vedea Anexa nr. 2):

- ~ Dezvoltare personală (ciclul primar, gimnazial, liceal);
- ~ Educația pentru media (ciclul primar, gimnazial, liceal);
- ~ Educația digitală (ciclul primar).

Deseori, subiecte ce vizează siguranța online sunt integrate în module sau teme ce vizează securitatea online sau securitatea cibernetică. Spre exemplu, în cadrul disciplinei „Educația tehnologică”, ciclul primar, clasa IV, la modulul „Educația digitală”, la tema „Bune maniere și corectitudine digitală”, autorii au propus ca unități de conținut următoarele subiecte:

- ~ Resursele digitale pe paginile Web: Cine este proprietarul? Cum avem dreptul să le folosim?
- ~ Comunicăm împreună cu dispozitivele digitale – câteva reguli simple.
- ~ Din nou despre pericole – virușii informatici.

Deși denumirea temei vizează aspecte ce țin de comportamente online, conținutul sugerat vizează securitatea cibernetică, ceea ce creează confuzie între

subiecte și aspecte. În plus, se transmite mesajul că securizarea online este suficientă pentru a evita orice pericole online.

Cadrele didactice desfășoară activități cu elevii și în cadrul Programului de activități extrașcolare⁴³, în contextul Zilei Siguranței pe Internet și Lunarului Securității Cibernetică. Aceste activități sunt recomandate conform Reperelor metodologice privind organizarea procesului educațional la disciplina școlară informatică în anul de studii 2019-2020⁴⁴.

Conform acestor repere metodologice, la disciplina de informatică e recomandată și formarea de atitudini și deprinderi de comportament responsabil ale elevilor în vederea prevenirii unor situații de risc, promovării siguranței în utilizarea tehnologiilor, navigării pe internet, etc. Cu toate acestea, temele din curriculum la ciclul gimnazial și liceal vizează doar aspectele de securitate online și securitate cibernetică⁴⁵.

f. Tehnologii și infrastructură securizată

Standardele minime de dotare a școlilor primare, gimnaziilor și liceelor cu mijloace TIC stabilesc obligativitatea instituțiilor de învățământ de a dispune de un software specializat de filtrare a conținuturilor de pe Internet⁴⁶. Deși este reglementată obligativitatea școlilor primare, gimnaziilor și liceelor de a dispune de un software specializat de filtrare a conținuturilor de pe Internet, despre această normă nu se cunoaște. Discuțiile cu managementul instituțiilor de învățământ indică despre o omisiune în implementarea practică a normelor de dotare minimă de uz general cu TIC.

Mai mult de 50% dintre școli (din numărul total de 48 de școli) au acces la internet prin rețeaua wi-fi. În toate cazurile, accesul este restricționat, ceea ce presupune existența unei parole de acces la Internet. Doar în trei instituții de învățământ copiii au acces la parola de conectare la Internet prin rețeaua wi-fi. Doar într-o singură instituție de învățământ au fost setate măsuri de filtrare a conținutului online. Am constatat că profesorii nu cunoșteau despre posibilitatea setării unor măsuri tehnice pentru filtrarea conținutului, considerând că securizarea accesului presupune setarea unei parole de acces.

„Nu sunt instalate filtre de conținut nici măcar în sala cu calculatoare. Au fost cazuri când pe ecranele calculatoarelor au apărut diferite imagini care nu sunt chiar potrivite pentru vârsta elevilor.”

Cadru didactic

“Nu sunt filtre. Ar fi o opțiune bună, dar, oricum, ei ar accesa, dacă nu în școală, atunci în altă parte.”

Cadru de conducere

“Ministerul trebuie să ia măsuri cu toți prestatorii de servicii, ca să fie obligați să ofere școlilor setările respective.”

Cadru de conducere

“Nu s-a știut. Nu s-a spus. Ar fi bine la nivel de țară să fie responsabilizați cei ce prestează așa servicii.”

Cadru de conducere

⁴³ Ordin MECC nr. 1619 din 10.12.2019 cu privire la aprobarea Programului activităților extrașcolare în învățământul primar și secundar, ciclul II și III.

⁴⁴ Ordinul MECC nr. 1046 din 21 august 2019 privind aprobarea Reperelor Metodologice privind organizarea procesului educațional la disciplina școlară Informatică în anul de studii 2019-2020.

⁴⁵ https://mecc.gov.md/sites/default/files/informatica_gimnaziu_ro.pdf https://mecc.gov.md/sites/default/files/informatica_liceu_ro.pdf

⁴⁶ Ordinul MECC nr. 581 din 24 iunie 2015 cu privire la aprobarea Standardelor minime de dotare a școlilor primare, gimnaziilor și liceelor cu mijloace TIC.

Principalele constatări ce vizează politicile și practicile naționale:

1. Conform Codului Educației, una dintre obligațiunile de bază ale personalului didactic este de a informa elevii despre toate formele de violență, inclusiv despre violența online; despre modul cum se manifestă aceste acțiuni, despre persoanele și instituțiile la care se pot adresa atunci când sunt supuși unui act de abuz online.
2. Siguranța copiilor online nu este o prioritate în documentele de politici educaționale, fiind reglementată ca subiect al programului de activități extra-curriculare, al activităților neformale și informale cu elevii de toate vârstele. Deși subiectul este inclusiv în curriculumul disciplinelor obligatorii și opționale, persistă o confuzie în terminologia utilizată și în abordările despre subiect, deseori termenul de „siguranță online” fiind utilizat în locul „securității cibernetice”, și viceversa.
3. Standardele de competențe digitale ale elevilor din ciclul primar, gimnazial și liceal, aprobate de MECC în 2015, nu corespund Cadrului de referință recomandat la nivel european DigComp. Siguranța online nu este specificată în standardele naționale, deși, pe plan european, aceasta este una dintre sub-competențele digitale-cheie.
4. Cadrul normativ actual nu reglementează modul în care pot fi identificate cazurile de abuz online în școală, dar nici acțiunile de intervenție a personalului didactic. Practica arată o tendință comună în rândurile psihologilor școlari și cadrelor didactice, de a reacționa și interveni intuitiv, în baza propriei experiențe de viață și fiind ghidați de propriile atitudini și percepții față de subiect.
5. Cadrele didactice recunosc actualitatea riscurilor în mediul online pentru securitatea fizică și psiho-emoțională a copilului. Totodată, nu este clar ce ar trebui să facă pentru a reduce din aceste riscuri și care e rolul instituției de învățământ sau personalului didactic.
6. Din lipsa unui program de educație parentală ajustat rolurilor părintești în era digitală, subiectul este abordat sporadic cu părinții. Cadrele didactice au nevoie de resurse și formări tematice despre modul de comunicare și colaborare cu părinții despre siguranța copiilor online.
7. Mai mult de 90% dintre instituțiile de învățământ, în care au avut loc discuții focus-grup în contextul acestei cercetări, nu dispun de softuri specializate pentru filtrarea conținutului, la care ar putea avea acces copiii, accesând rețeaua wi-fi în școală. Instituțiile de învățământ nu sunt informate despre obligativitatea unor asemenea măsuri reglementate de cadrul normativ și lipsesc măsurile de control al implementării acestora, din partea MECC.
8. Nu există o participare autentică a copiilor în inițiativele de promovare a siguranței online în școală. De obicei, implicarea elevilor presupune realizarea unor proiecte, la inițiativa cadrelor didactice. Nu au fost identificate practici de implicare directă a elevilor - prin intermediul consiliilor elevilor sau într-o altă formă - în îmbunătățirea cadrului de politici în școală, care vizează siguranța online ori ameliorarea practicilor în domeniu.
9. Cadrele didactice și psihologii școlari sunt puțin informați despre abuzul sexual online, cum pot identifica asemenea abuzuri și cum pot interveni în astfel de cazuri. Mai mult decât atât, discuțiile focus-grup relevă un nivel înalt de stereotipuri și reticență față de subiect, fapte care stimulează blamarea copilului abuzat.
10. Mecanismele de intervenție existente nu sunt adaptate abuzurilor săvârșite cu utilizarea TIC. Cadrele didactice au constatat necesitatea elaborării unor proceduri specifice pentru cazurile de abuz online, care să explice semnele acestei forme de abuz și recomandările de intervenție, reieșind din riscurile specifice acestor cazuri.

The background is a solid purple color. It features several overlapping circles: a large, semi-transparent light purple circle in the upper right; a medium-sized orange circle on the left side, partially behind the text; a small orange circle at the bottom center; and another medium-sized orange circle at the bottom right.

Principalele concluzii și recomandări

Concluzii

Cu referire la cadrul politicilor educaționale naționale

1. Principalele acțiuni recomandate în documentele de politici publice internaționale vizează integrarea siguranței online în programul școlar, de la o vârstă cât mai mică; organizarea diverselor activități de informare și sensibilizare pentru comunitatea școlară (elevi, părinți, cadre didactice, etc.) și dezvoltarea unor politici instituționale ce ar asigura un răspuns eficient al școlii la provocările copiilor în mediul online.
2. Siguranța copiilor online nu este o prioritate în documentele de politici educaționale, fiind reglementată ca subiect al programului de activități extra-curriculare, al activităților neformale și informale cu elevii de toate vârstele.
3. Standardele de competențe digitale ale elevilor din ciclul primar, gimnazial și liceal, aprobate de MECC în 2015, nu corespund Cadrului de referință recomandat la nivel european DigComp. Siguranța online nu este specificată în standardele naționale, deși, pe plan european, aceasta este una dintre sub-competențele digitale-cheie.
4. Cadrul normativ actual nu reglementează modul în care pot fi identificate cazurile de abuz online în școală, dar nici acțiunile de intervenție ale personalului didactic. Practica arată o tendință comună în rândurile psihologilor școlari și cadrelor didactice, de a reacționa și interveni intuitiv, în baza propriei experiențe de viață și fiind ghidați de propriile atitudini și percepții față de subiect.

Cu referire la practicile instituțiilor de învățământ în domeniul siguranței copiilor online

5. Siguranța copiilor online lipsește din politicile instituționale, din regulamentele de organizare și funcționare ale instituției de învățământ, precum și din politicile de protecție a copilului. În prezent, există doar unele recomandări de integrare a subiectului în politicile de protecție a copilului, însă aceste recomandări nu sunt implementate.
6. Activitățile de educare a comportamentelor

sigure online ale elevilor sunt organizate haotic, sporadic, subiectul fiind deseori confundat cu activitățile de securitate online sau securitate cibernetică. Forma de abordare a subiectului deseori presupune predarea unor reguli de siguranță online, ceea ce nu contribuie la dezvoltarea de abilități și competențe. Aceste activități sunt organizate haotic și superficial, de obicei în contextul „Zilei Siguranței Online” și „Lunarului Securității Cibernetică”.

7. Cadrele didactice recunosc actualitatea riscurilor în mediul online pentru securitatea fizică și psiho-emoțională a copilului. Totodată, nu le este clar ce ar trebui să facă pentru a reduce din aceste riscuri și care este rolul instituției de învățământ sau al personalului didactic. Implicarea cadrelor didactice în promovarea siguranței online depinde de nivelul de motivație și înțelegere a necesității și actualității subiectului. La moment, activitățile didactice despre siguranța online nu sunt percepute ca activitate de prevenire a abuzurilor în mediul online sau de dezvoltare a capacităților de reziliență a copiilor față de abuzuri.
8. Colaborarea cu părinții în promovarea siguranței copiilor online este inefficientă. Deseori, cadrele didactice se confruntă cu problema rezistenței din partea părintelui care nu conștientizează actualitatea temei, care respinge ideea că copilul lui ar fi vulnerabil online ori consideră că nu are nevoie să fie informat la acest subiect. Din lipsa unui program de educație parentală ajustat rolurilor părintești în era digitală, subiectul este abordat sporadic cu părinții. Cadrele didactice au nevoie de resurse și formări tematice privind modul de comunicare și colaborare cu părinții despre siguranța copiilor online.
9. Mai mult de 90% dintre instituțiile de învățământ, în care au avut loc discuții focus-grup în contextul acestei cercetări, nu dispun de softuri specializate pentru filtrarea conținutului, la care ar putea avea acces copiii, conectându-se la rețeaua wi-fi în școală. Instituțiile de învățământ nu sunt informate despre obligativitatea unor asemenea măsuri reglementate de cadrul normativ și lipsesc măsurile de control al implementării acestora, din partea MECC.
10. Nu există o participare autentică a copiilor în inițiativele de promovare a siguranței online în școală. De obicei, implicarea elevilor presupune realizarea unor proiecte, la inițiativa cadrelor didactice. Nu au fost identificate practici de implicare directă a elevilor, prin intermediul

consiliilor elevilor sau într-o altă formă, în îmbunătățirea cadrului de politici în școală, care vizează siguranța online ori ameliorarea practicilor în domeniu.

11. Cadrele didactice și psihologii școlari sunt puțin informați despre abuzul sexual online, cum pot identifica asemenea abuzuri și cum pot interveni în astfel de cazuri. Mai mult decât atât, discuțiile focus-grup relevă un nivel înalt de stereotipuri și reticență față de subiect, fapte care stimulează blamarea copilului abuzat.

12. Mecanismele existente de intervenție nu sunt adaptate abuzurilor săvârșite cu utilizarea TIC. Cadrele didactice au constatat necesitatea elaborării unor proceduri specifice pentru cazurile de abuz online, care să explice semnele acestei forme de abuz și recomandările de intervenție, reieșind din riscurile specifice acestor cazuri.

Recomandări

Revizuirea cadrului național de competențe digitale

- ~ Actualizarea cadrului de competențe digitale pentru elevi, în vederea integrării siguranței online în spectrul de competențe digitale, conform recomandărilor pe plan european în domeniu;
- ~ Preluarea și adoptarea Standardelor Europene de Competențe Digitale – DigComp pentru instituțiile de învățământ.

Integrarea siguranței online în politicile instituționale

- ~ Elaborarea unui model-tip de politică instituțională în domeniul siguranței copiilor online și încurajarea dezvoltării unor asemenea politici de către fiecare instituție de învățământ;
- ~ Elaborarea unor instrucțiuni detaliate care ar răspunde necesităților cadrelor didactice de a înțelege mai bine cum să protejeze copiii de abuzuri în mediul online, prin acțiuni eficiente de prevenire, protecție și asistență;
- ~ Asigurarea dezvoltării politicilor despre siguranța online printr-un proces participativ, cu implicarea elevilor și părinților în dialoguri despre îmbunătățirea politicilor instituționale, procedurilor și proceselor privind siguranța online în școală;
- ~ Crearea unui Comitet specializat în siguranța online în fiecare școală, care ar ghida desfășurarea activităților de prevenire a abuzurilor online în școală, procesul de elaborare a unui plan de intervenție în cazurile de abuz identificate, etc.

Dezvoltarea capacităților actorilor educaționali în domeniul siguranței copiilor online

- ~ Integrarea siguranței copiilor online în programele de formare continuă a cadrelor didactice și psihologilor școlari, precum și a personalului din cadrul Serviciilor de Asistență Psiho-Pedagogică;
- ~ Stabilirea obligativității participării la cursuri de formare în domeniul siguranței copiilor online, pentru toate cadrele didactice care desfășoară activități la acest subiect, în cadrul disciplinelor obligatorii sau opționale;
- ~ Formarea directorilor adjuncți pentru educație în domeniul siguranței copiilor online, pentru a asigura o coordonare și o ghidare eficientă a cadrelor didactice la nivel instituțional, de către un specialist pregătit în acest domeniu;
- ~ Integrarea siguranței copiilor online în programele de educație parentală și desfășurarea cu regularitate a activităților de informare a părinților despre siguranța copiilor.

Încurajarea desfășurării activităților neformale și informale de promovare a siguranței copiilor online

- ~ Continuarea activităților despre siguranța online cu elevii, în contextul Zilei Siguranței Online, prin practica circulelor MECC. Totodată, a se evalua oportunitatea încurajării managementului instituțiilor de învățământ de a include subiectul în planurile manageriale, pentru a eficientiza modul

de organizare și desfășurare a activităților de către diriginții de clasă;

- ~ A include în Programul activităților extrașcolare în învățământul primar și secundar, ciclul I și II, Concursul despre siguranța copiilor online - activitate de încurajare a participării cadrelor didactice și elevilor în promovarea siguranței online în cadrul instituției de învățământ și la nivel național.

Crearea unui mecanism de implementare și monitorizare a securității infrastructurii TIC în școală

- ~ Elaborarea unor repere metodologice, în colaborare cu reprezentanți din sectorul privat TIC, privind modalitatea de implementare în practică a obligativității de instalare a unui software specializat de filtrare a conținuturilor de pe Internet, prin reglementarea responsabilităților fiecărei părți vizate în acest sens.
- ~ Monitorizarea modului de implementare a cadrului normativ ce reglementează obligativitatea școlilor primare, gimnaziilor și liceelor de a dispune de un software specializat de filtrare a conținuturilor de pe Internet, prin crearea unui mecanism de raportare periodică a realizărilor în acest domeniu.

Revizuirea și adaptarea procedurilor de intervenție în cazuri de abuz online în școală

- ~ A analiza în ce măsură procedurile de intervenție în cazuri de ANET⁴⁷ sunt valabile în cazurile de abuz online. În funcție de rezultatele acestei analize, se va recomanda ajustarea instrucțiunilor ANET prin specificarea faptului că sunt aplicabile și în cazurile de abuz online, fie elaborarea unor instrucțiuni distincte pentru cazurile de abuz online.
- ~ A organiza activități de formare a personalului didactic în sensul identificării prompte și intervențiilor eficiente în cazuri de abuz online.
- ~ A desfășura activități de formare continuă a specialiștilor din cadrul Serviciilor de Asistență Psiho-pedagogică în sensul consilierii și suportului psihopedagogic ce poate fi furnizat copiilor - victime ale abuzului sexual online.
- ~ A asigura colaborarea dintre personalul didactic și alți actori din comunitate (organizații neguvernamentale, polițiști, etc.) din momentul identificării unui caz de abuz sexual online în instituția de învățământ, pentru a asigura o intervenție bine coordonată, bazată pe nevoile copilului.

47 Abuz, neglijență, exploatare, trafic