Children's Safety in the Digital Environment

Republic of Moldova

USAID FROM THE AMERICAN PEOPLE

DATA FOR impact

Children's Safety in the Digital Environment

Republic of Moldova

Data for Impact
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC 27516 USA
Phone: 919-445-6949
D4I@unc.edu
http://www.data4impactproject.org

This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of the Data for Impact (D4I) associate award 7200AA18LA00008, which is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill, in partnership with Palladium International, LLC; ICF Macro, Inc.; John Snow, Inc.; and Tulane University. The views expressed in this publication do not necessarily reflect the views of USAID or the United States government. TR-24-588

September 2024

USAID FROM THE AMERICAN PEOPLE

DATA FOR impact

Acknowledgments

We appreciate the invaluable contributions of all children who participated in the survey, their parents/caregivers, and school administrations. Their participation was crucial for the success of our research.

We would also like to thank the Ministry of Education and Research for facilitating the field work and to representatives of the Psychopedagogical Assistance Services, National Center for Child Abuse Prevention, Child Helpline, Center for Assistance and Protection, Prosecutor's Office for Combating Organized Crime and Special Cases, and the Center for Investigating Cyber Crimes who provided crucial insights during interviews.

We would like to thank the National Center for the Prevention of Child Abuse (CNPAC) for their review of the study questionnaires.

We thank the Health Media Lab IRB for carefully reviewing the research protocol and offering essential suggestions to ensure the implementation of high ethical standards in research.

We thank International Center “La Strada” and Sociopolis Consultancy SRL, which conducted the data collection, analysis, and report writing.

We are grateful for the financial support from the United States Agency for International Development (USAID).

Cover photo credit:

Contents

Figures

Tables

Abbreviations

AI	artificial intelligence
CNPAC	National Center for the Prevention of Child Abuse
D4I	Data for Impact
FGD	focus group discussion
GATU	Gagauzia Autonomous Territorial Unit
IC La Strada	International Center "La Strada"
IDI	in-depth interview
LEA	local education authorities
MoER	Ministry of Education and Research
OECD	Organization for Economic Cooperation and Development
PAS	Psychopedagogical Assistance Service
SEN	special educational needs
UNDP	United Nations Development Programme
UNICEF	United Nations Children's Fund
USAID	United States Agency for International Development
YFHC	Youth-Friendly Health Center

Executive Summary

The study "Children's Safety in the Digital Environment" was conducted by Data for Impact (D4I) in partnership with the International Center "La Strada" and Sociopolis Consultancy SRL, with funding from the United States Agency for International Development (USAID). The results of this study are intended to assist policy makers in making decisions to ensure a safe and inclusive digital environment for children in the Republic of Moldova.

The connected world in which children and young people grow up offers limitless access to information and services, including positive educational experiences. Even though most Moldovans have access to the internet and smart devices, there is a digital divide across socioeconomic groups, rural-urban populations, and gender. Ensuring connectivity for the most vulnerable Moldovans is needed to create a more inclusive digital space. Moldova's Digital Readiness Analysis recommended that digital exclusion is further researched to ensure that digital transformation does not exacerbate current inequalities but acts as a driver of opportunities for the whole country (UNDP, 2021). At the same time, it is important to be aware of the potential negative aspects of information technologies to help inform risk mitigation efforts. Harmful activities can include bullying and harassment, identity theft, and online abuse, including sexual abuse. Children who are at risk offline are usually at risk online, and the potential for digital harm among children is embedded in complex social issues (Internet Matters/Youthworks, 2019).[1]

There is a major gap in evidence related to preventing and responding to the risks of digital harm among vulnerable children in the Republic of Moldova, and more extensive studies are needed to explore the dynamics of online risks and develop tailored interventions. To promote inclusion of vulnerable children and families with children in the country's digital transformation and inform policy and practice, D4I conducted research aimed at providing actionable recommendations to the government and its partners.

The **goal of the study** was to provide a comprehensive understanding of the way children, in particular vulnerable children, access and use the internet, their knowledge and experiences in the digital environment, and risks and protective factors to inform the improvement of measures aimed at fostering evidence-based children's safety in the digital environment.

The **objectives of the study** were the following:

- Identification of methods used by children to access and use the internet
- Analysis of children's behaviors, practices, and experiences in the digital environment
- Assessment of children's knowledge and awareness of risks in the digital environment
- Identification of risks children face online and factors that could reduce their online vulnerability
- Analysis of measures taken by parents and specialists to maintain children's online safety
- Development of recommendations for authorities to ensure a safe, inclusive digital environment

[1] See also: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/02/20/vulnerable-offline-and-at-risk-online and http://globalkidsonline.net/pathways-to-risk/

Methodology

The research applied a mixed methodology that combined quantitative methods used with students from 5th to 11th grade (ages 10–17 years old) and qualitative methods used with parents and specialists. The quantitative component of the research included a national, non-representative sample of 1,412 children from 35 educational institutions. The qualitative component of the research included two focus group discussions (FGDs) with a total of 22 parents/caregivers and 11 in-depth interviews (IDIs) with specialists from the educational, social protection, and law enforcement systems.

A key objective of the research was exploring online risks for children from vulnerability categories. Therefore, it was critical to define child vulnerability specific to this research and strategies to reach vulnerable children. The definition of a vulnerable child used in this research was informed by the provisions of Article 8 of Law No. 140/2013 regarding the special protection of children at risk and children separated from their parents, the provisions of Articles 1 and 7 of Law No. 547/2003 on social assistance, and the criteria used by the Ministry of Education and Research (MoER) for designating vulnerable children in its management information system. Four categories of socially vulnerable children were established based on these legal provisions, data, and information**:** (i) **children from low-income families**; (ii) **children with limited parental communication and support**; (iii) **children with disabilities or special educational needs (SEN)**; and (iv) **children who speak a different language at home than at school**. Data analysis was carried out using the above-mentioned categories.

Key findings are presented below.

Children in the Digital Environment

- Almost all children in the Republic of Moldova have access to the internet and mobile devices, regardless of their background. An estimated 99% of students without social vulnerability and 96% of students from vulnerability categories are online daily. On their days off or when on vacation, the number of children with restricted access is insignificant (1%).
- A greater proportion of children without social vulnerability access the internet at home (92%) and school (35%) compared to children from vulnerability categories (89% and 33%, respectively). Children from vulnerability categories, to a greater extent than non-vulnerable children, access the internet via Wi-Fi in public spaces and mobile internet.
- Ninety-three percent of all children have at least one social media account or profile. Children's favorite social networks are diverse. Children from 5th to 9th grade prefer TikTok to a greater extent, those from 10th to 11th grade opt more for Instagram, and children from vulnerability categories primarily choose TikTok.
- Children use social media for communication (64%), socializing (59%), or spending free time (46%), and less for personal development, including homework (27%). There are differences in the way children use the internet depending on their school grade/age, gender, and vulnerability category.

Children's Behaviors, Practices, and Experiences in the Digital Environment

- Actions taken by children in the digital environment differ according to sociodemographic characteristics. In the last three months of internet use, 72% of girls have sent photos and video sequences about themselves via Messenger, Viber, WhatsApp, Discord, forums, or chat rooms to a

person they know in person, compared to 58% of boys. However, 31% of boys bought online games, game credits, bonuses, etc. via Google Play, AppStore, or other ways online, compared to only 9% of girls.

- Potentially risky actions are almost twice as prevalent among vulnerable children versus those not classified as vulnerable. A greater proportion of vulnerable children reported looking for new friends in the digital environment (32% to 38% compared to 21% of the non-vulnerable), buying games online and game credits (21% to 22% compared to 14% of the non-vulnerable), sending photos or video sequences with them to strangers (17% to 19% compared to 9% of the non-vulnerable), or exchanging personal data with people they only know online (8% to 12% in comparison with 5% of the non-vulnerable).
- An estimated 36% of children accepted friendship or connection requests from people they did not know in real life, 30% chatted with people they did not know in person and met them for the first time on social networks, and 29% sent friendship or connection requests to people they haven't met in real life. Children from vulnerability categories frequently undertook such actions in the digital environment (for example, 38% to 43% of them accepted friend or connection requests from people that they did not know offline compared to 27% of non-vulnerable children).
- 57% of children faced unpleasant online experiences, such as being blocked on social networks**,** having their social media accounts hacked, receiving inappropriate images or messages with sexual content, or being asked to send personal images or videos containing intimate parts of their body. Negative incidents were experienced to a greater extent by boys (62%) and children from low-income families (67%).

Children's Knowledge and Awareness of Online Risks

- The main information sources for children about online safety are parents (54%), education staff (45%), and offline friends (35%). Parents and education staff represent the main sources of information to a greater extent for girls (62%), younger students (64% of 5th grade students), and children from families that are not socially vulnerable (65%).
- One in 10 children knows nothing about online safety and has no source of information. Fifteen percent of boys reported knowing nothing about online safety and having no source of information, as well as 16% of children whose mother tongue is different from the language of instruction and 16% of students in the 5th grade.
- Specialized websites on the subject of preventing and combating online risks are less known by children participating in the research. Only 6% of children are familiar with the site www.siguronline.md and have accessed it a few times, and 2% know about it and use it often to get information. Similarly, only 3% of children are familiar with the site www.12plus.md and have accessed it a few times, and 1% know it and use it often.
- 63% of children reported feeling safe or very safe online. Children from low-income families, children with limited parental communication and support, as well as children with disabilities or SEN, reported a higher self-perception of level of safety in the digital environment.

Risks Children Face in the Digital Environment

- Twenty-one percent of 1,312 children with a social account or profile have their date and year of birth publicly displayed. Between 22% and 24% of vulnerable children have publicly displayed their date and year of birth, compared to 14% of children with no social vulnerability.
- The date and year of birth posted online were reported to be true by 41% of children. In 60% of cases, children's accounts reveal their real name and surname. Fifty-five percent of boys posted their real names and surnames, compared to 64% of girls. Fifty-five percent of the 5th grade students displayed their real names compared to 75% of the 11th grade students.
- Five percent of children publicly displayed contact information on their social account, while 9% did not know if this information was available. The share of boys that publicly displayed contact information was 6% in comparison with 3% for girls. A higher percentage of vulnerable children publicly displayed their contact information (5% to 6%) versus those classified as non-vulnerable (3%).
- In 43% of cases, the photo on a child's social media account clearly shows the face of the profile owner. This is more typical for girls (53%) than boys (31%). A smaller proportion of younger students (40% of the 5th grade students) posted a clear picture with their face compared to older students (59% of 11th grade students). Forty-five percent of non-vulnerable children posted a photo of their face, compared to 40–42% of those from the vulnerability categories.
- The school a child attends was made public on social media by 21% of children. A higher proportion of girls (25%) posted such information compared to boys (18%). Younger students were more likely to share information about their school, with 27% of 5th grade students doing so, compared to just 15% of 11th grade students. Additionally, 23% of children with limited parental communication and support publicly shared their school information.
- Nineteen percent of children revealed that the internet affected their school results (very often, often, or sometimes). Between 21% and 25% of children from the four vulnerability categories faced such challenges, compared to those without vulnerability (13%).
- Thirteen percent of children reported that the internet affected their nutrition or sleep. Fourteen percent to 19% of vulnerable children reported that the internet affected their nutrition and sleep, compared with 8% of non-vulnerable children. Once the school grade increases, the number of children with poor nutrition and sleep due to the internet increases from 10% in the 5th to 23% in the 11th grade.
- The risks related to content on the internet affect a greater percentage of children classified as vulnerable: 10% to 17% accidentally viewed or accessed sexual content online (8% of the non-vulnerable), 12% to 14% involuntary watched videos or photos (6% of the non-vulnerable), and 11% to 14% received inappropriate photos, sexually explicit messages, or images (7% of the non-vulnerable).
- Children engage in various activities with people known only online. Within the last three months, 34% of children shared personal photos, 19% were asked to go out in town/village, park, or other

locations, and 15% shared their contact information with a person known only online. There are also 6% of children who received propositions that made them feel uncomfortable.

- Children face various conduct risks from peers online. Twenty-nine percent of children with disabilities or with SEN were excluded from social media, and 19% received offensive messages. On the other hand, 15% of children from low-income families faced social media hacking, 13% were subject to cyberbullying, 9% experienced hate speech from peers on social media, and 7% experienced situations when peers posted photos and videos modified in an insulting way.
- During the last three months, one in 10 children unknowingly spent money online for games. These risks were most often experienced by boys (8%) compared to girls (5%). Such situations confronted children from low-income families (9%) and children with disabilities or with SEN (9%) even more commonly.
- Sixty-nine percent of children sought help when they faced online challenges and negative experiences, while 31% preferred not to discuss such experiences with anyone. Most who do not seek help are boys (36%) and children who speak a different language at home than at school (39%).

Measures Taken to Ensure Children's Safety Online

- Desk research and interviews showed that various activities are carried out in schools, based on MoER's *Online child/student safety standards*. These are (i) providing information to students during class hours, personal development classes, informatics, and media education; (ii) conducting extracurricular activities on online safety; (iii) engaging students in the promotion of the subject; and (iv) informing parents and caregivers about online risks.
- Online safety is promoted through annual activities in the school community during Safer Internet Day and Cybersecurity Awareness Month.
- There are few specialized services in the Republic of Moldova providing services to children affected by abuse and sexual harassment online. The survey, focus groups, and interviews indicated that siguronline.md (IC La Strada) and 12plus (National Center for the Prevention of Child Abuse [CNPAC]) are among the most well-known web-based resources by children, parents, and specialists. Some children, parents, and specialists use the Child Helpline, which records cases of online abuse and refers them to specialized services.

Key Recommendations

Research findings informed strategic and operational recommendations for central and local authorities, governmental agencies, the private sector, and educational and child protection professionals. Key recommendations are summarized below. More details on the addressee and timeframe for these recommendations are presented in the last chapter of this report.

- Develop specific strategies for the digital inclusion of vulnerable children with limited access to digital devices and online connections to ensure equal access to development and learning opportunities in the digital environment.
- Approve the *Online children's safety action plan*, which will set forth the commitment of all relevant stakeholders to ensure a child-safe online environment through an interdisciplinary approach.

- Embed a comprehensive and constructive approach by the MoER in all initiatives to assess, amend, and review curricular programs through embedding online safety as a cross-cutting subject.
- Develop guidelines on the practical implementation of the intersectoral cooperation mechanism stipulated by Government Decision No. 270/2014 in online abuse and exploitation cases for specialists engaged with social protection, education, healthcare, and the police.
- Integrate activities for the development of transversal competencies into digital education programs, such as skills related to social interaction, communication, collaboration, online content creation, problem-solving, and critical thinking in schools.
- Regulate information to the educational staff about technological innovations and trends linked to young people's use of digital resources, organize activities to develop teachers' digital literacy, and integrate the sub-competency on online safety.
- Carry out thematic awareness-raising campaigns for parents, caregivers, child protection specialists, and community members about online child abuse to change attitudes and combat stereotypes.
- Develop parenting programs adjusted to various child age categories, aimed at improving communication with children about online safety and shifting the approach from a restrictive to an informative and educational one, based on trust and respect.
- Carry out national evidence-based information and awareness-raising campaigns about how specific risks might affect children, including lesser-known ones, such as exposure to abusive or sexual content, online risks from peers, and online shopping safety risks.
- Empower youth in the field of online safety to be able to engage them in peer-to-peer communication, raise other students' awareness of online risks, and provide successful examples of coping with these.
- Develop children's critical thinking and ability to recognize online risks through practical activities and case studies within the compulsory school curriculum as well as through informal education activities.
- Provide information about mechanisms for reporting illegal content on service providers' platforms that are available to users.
- Promote child protection principles in the digital environment, including in consuming digital products and services, as well as the development of services applying safety measures in the design and corporate policies of digital service providers.

Introduction

The connected world in which children and young people grow up offers limitless access to information and services, including positive educational experiences. Even though most Moldovans have access to the internet and smart devices, there is a digital divide across socioeconomic groups, rural-urban populations, and gender. Ensuring connectivity for the most vulnerable Moldovans is needed to create a more inclusive digital space. Moldova's Digital Readiness Analysis recommends that digital exclusion is further researched to ensure that digital transformation does not exacerbate current inequalities but acts as a driver of opportunities for the whole country (UNDP, 2021).

At the same time, it is important to be aware of the potential negative aspects of information technologies to help inform mitigation efforts. Harmful activities can include bullying and harassment, identity theft, and online abuse, including sexual abuse. Children who are at risk offline are usually at risk online, and the potential for digital harm among children is embedded in complex social issues (Internet Matters/Youthworks, 2019).[2]

There is a major gap in evidence related to preventing and responding to the risks of digital harm among vulnerable children in the Republic of Moldova, and more extensive studies are needed to explore the nuanced dynamics of online risks to develop tailored interventions. Thus, the Government of the Republic of Moldova has established among its priorities in the field of child protection the mitigation of child abuse and exploitation, including online abuse and exploitation (General Objective 2 of the National Programme on Child Protection for 2022-2026). Additionally, beginning with the 2022–2023 school year, the Ministry of Education and Research (MoER) approved the implementation of *Online children/students' safety standards.*[3] These represent a comprehensive document focused on critical areas: (i) school management, (ii) educational staff training, (iii) availability of particular policies and procedures, (iv) parent engagement, (v) online safety education, and (vi) safe technologies and infrastructure.

The *Online children/students' safety standards* aim to support the education system to develop and implement measures to secure children/students' safety online by committing to online safety at the local level, empowering the academic environment to communicate positively online with no risk to the security and well-being of children. These standards aim to ensure minimum actions that general education institutions should take to strengthen efforts in promoting online safety, creating a safe and secure environment for children/students, and ongoing training for educational staff, parents, and children/students. The *Online children/students safety standards* were developed to comply with the Recommendations of the Council of Europe on promoting digital citizenship education, Recommendations of the Organization for Economic Cooperation and Development (OECD), European Digital Competence Framework, and Digital Education Action Plan, developed and approved by the European Commission.

Moreover, the Government of the Republic of Moldova is committed to preventing and combating child sexual abuse and exploitation according to the Council of Europe Convention on the Protection of Children

[2] See also: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/02/20/vulnerable-offline-and-at-risk-online and http://globalkidsonline.net/pathways-to-risk

3 MoER Order no. 985 of 07.10.2022 on the approval and implementation of Online children/students' safety standards.

against Sexual Exploitation and Sexual Abuse , signed at Lanzarote on October 25, 2007, as well as integrating into national law the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography. Currently in the Republic of Moldova, there is no evidence regarding the online risks in vulnerable children that allows for planning specific information measures as well as appropriate assistance for these children.

The Data for Impact project (D4I), funded by the United States Agency for International Development (USAID), helps countries generate strong evidence for health and child protection programming and policy decision making. D4I, in partnership with the International Center "La Strada" and Sociopolis Consultancy SRL, conducted this study in the Republic of Moldova on the safety of vulnerable children in the digital environment to close the information gap and inform decision making.

This study generated evidence at the national level about children's online safety, particularly vulnerable children, as well as the opinions of various actors on this subject (such as children, parents, specialists in education, social protection, and law enforcement). These findings could be used to develop child protection policies in the digital environment, digital education, and combat online sexual abuse and exploitation of children. The research findings could be instrumental in developing evidence-based programs for training professionals engaged in child protection and education, providing guidance in organizing community awareness campaigns, and developing tools required to foster children's safety in the digital environment. Finally, the research outcomes could contribute to the development of strategies and practices targeted to protect children from the most vulnerable groups against various forms of online abuse and exploitation.

The study is ultimately targeted to policy makers and other actors that develop and implement education and child protection policies; educational staff, school psychologists, child protection specialists, and other professionals dealing with children, especially vulnerable children; parents who need to stay informed and provide support to their children; the community in general, to be able to understand various aspects of digital inclusion and online safety to provide support; and lastly, to children who stand to benefit from program and policy approaches informed by the protective and risk factors in the digital environment.

I. Research Framework

1.1. Study Goal and Objectives

The goal of the research study, "Children's safety in the digital environment," was to identify specific online risks faced by vulnerable children in the Republic of Moldova and develop recommendations to improve the response of national authorities in securing a safe and inclusive digital environment for all children. The research study aimed at supporting a comprehensive understanding of the way children, particularly vulnerable children, access and use the internet, their knowledge and experiences in the digital environment, risk factors, and protective factors to improve measures to foster evidence-based children's safety in the digital environment.

Objectives of the research were the following:

- Identification of methods used by children to access and use the internet
- Analysis of children's behaviors, practices, and experiences in the digital environment
- Assessment of children's knowledge and awareness of risks in the digital environment
- Identification of the risks children face online and factors that could reduce their online vulnerability
- Analysis of measures taken by parents, educational staff, and other specialists to maintain children's online safety
- Development of recommendations for the authorities from the Republic of Moldova to ensure a safe and inclusive digital environment

1.2. Conceptual Framework and Research Hypothesis

The research study was conducted in five phases: (i) development and approval of the research protocol by the HML IRB Research & Ethics board based in the United States of America (Appendix 6); (ii) data collection (April 22–June 10, 2024); (iii) monitoring and data quality assurance; (iv) analysis and development of the research report; and (v) validation and dissemination of the outcomes and key recommendations of the research.

The research was based on primary and secondary data sources. During the initial stage, the research team conducted the analysis of concepts related to online safety, vulnerability criteria in children, relevant national and international studies (Appendix 1), and techniques used to assess this phenomenon. Important sources for the conceptual framework were *EU Kids Online* and the 3C / 4C which helped differentiate the key areas of risk children face online: content, contact, conduct, and contract. Thus, the risks of the digital environment referred to in this report include:

- Inappropriate, toxic, or illegal content that is available (i.e., the child, as the recipient, engages with or is exposed to potentially harmful content that could cause emotional or psychological harm).
- Harmful contact children could experience, including being targeted by adults that would attempt to abuse them or share inadequate and/or sexually explicit images (i.e., the child, as the participant, experiences or is exposed to potentially harmful contact).

- Abusive conduct from peers or their harmful conduct (i.e., the child as witness, participant, and/or victim of a potential harmful conduct).
- Potentially harmful contracts or commercial interests (such as gambling, exploitative, or age-inappropriate marketing). This includes risks linked to ill-designed or insecure digital services that leave the child open to identify theft, fraud, or scams.

The initial classification of risks (3C) suggested by the *EU Kids Online in 2015* emphasizes three dimensions related to the position of children in the digital environment, and shows how these interact with the type of risk (aggressive, sexual, value, and commercial) (see Table 1).

Table 1. Initial classification of risks suggested by the *EU Kids Online*, 2011

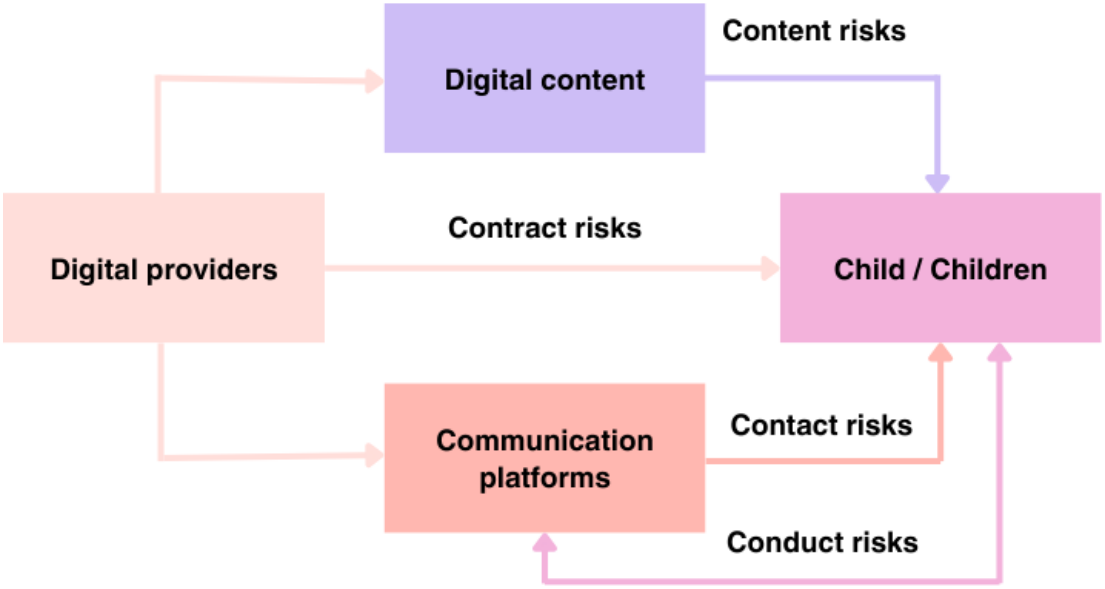
Type of risk	Content (receiving mass produced content)	Contact (participating in online activity)	Conduct (perpetrator or victim in peer-to-peer communication)
Aggressive	Violent content	Harassment, stalking	Bullying/cyberbullying, hostile activity
Sexual	Pornography	Grooming, sexual abuse or exploitation	Sexual harassment, sexting
Value	Racist/hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Embedded marketing	Misuse of personal data	Gambling, copyright infringement

Source: Livingstone, Mascheroni and Staksurd, 2015

Digital technologies have developed significantly in recent years. New opportunities and risks have emerged in the online environment for children, in particular, related to selling data and datafication.[4] To cope with these circumstances and to reintroduce the commercial dimension of online risk more prominently, the initial classification was completed with the fourth "C" (contract). The fourth "C" is conceived not as a commercial risk but as a "contract" risk that directly or indirectly connects children and digital providers. This risk reflects the alarming rise in the commercialization of children's personal data, a form of datafication (Mascheroni, G., 2020). Thus, researchers emphasize and caution policy makers on child rights, the presence of a digital ecosystem within the digital environment, and the various risks children face and how these risks increasingly interact with one another (Figure 1) (Livingstone, S., Lievens, E., & Carr, J., 2020). Contract risks arise when children use digital services and when they are impacted by digital transactions conducted by other people (O'Neill, B., 2014). There are legal difficulties related to contract risks involving children, as well as the fact that users of all ages, not just children, can be unaware of the contractual nature of their relationship with a digital provider. At the same time, researchers emphasize that these risks may not be with a child but with parents or schools, service providers, and other third parties, thus involving a complex digital ecosystem. These risks are currently escalating and require special attention.

4 Datafication is widely used in the Big Data industry and represents a process that transforms social aspects into online quantifiable data, thus enabling real time tracking and predictive analysis. It involves taking previously invisible processes/activities and transforming them into data that can be monitored, tracked, analyzed, and optimized. The latest technologies we use have enabled a wide range of new ways to "update" our daily and main activities.

Figure 1. The 4C classification of risks proposed by EU Kids Online, 2020



Source: Livinstone and Stoilova, 2021

The United Nations Children's Fund (UNICEF) highlighted technological issues and parental intrusion in children's online lives, risks that are not integrated into the classification proposed by *EU Kids Online* in 2011 and 2020 (UNICEF, 2017). The OECD has also pointed out specific risks related to data privacy, advanced technologies (e.g., artificial intelligence [AI], etc.), and children's health and well-being (OECD, 2021). As a result, the 4C classification was completed with transversal risks reflecting the violation of data privacy, risks linked to physical and emotional health, inequality, or discrimination of children (Table 2).

Table 2. Risks for children in the digital environment: revised typology of risks

Risk categories	Content risks	Conduct risks	Contact risks	Contract/consumer risks
Transversal risks	Privacy risks (interpersonal, institutional and commercial)			
	Advanced technology risks (AI, predictive analytics, biometrics)			
	Risks on health and well-being			
Risk manifestations	Hateful content	Hateful behavior	Hateful encounters	Marketing risks
	Harmful content	Harmful behavior	Harmful encounters	Commercial profiling risks
	Illegal content	Illegal behavior	Illegal encounters	Financial risks
	Disinformation	User-generated problematic behavior	Other problematic encounters	Security risks

Source: OECD, 2021

The development of this research relied on the *Global Kids Online Research Toolkit* and all subsequent amendments of the typology of risks for children in the digital environment, with particular adjustments to reflect the circumstances of the Republic of Moldova and its research objectives.

A key objective of this research was exploring the online risks faced by children from vulnerable groups in the Republic of Moldova. Therefore, a critical aspect of the research design consisted of defining child vulnerability and developing strategies to reach these children. An analysis of the factors contributing to vulnerability was carried out by the research team to differentiate vulnerable children from non-vulnerable ones, and several categories of vulnerable children were established. The definition of the vulnerable child used in this research complies with the provisions of Article 8 of Law No. 140/2013 regarding the special protection of children at risk and children separated from their parents, as well as the provisions of Articles 1 and 7 of Law No. 547/2003 on social assistance (Appendix 2) and the criteria used by the MoER for recording vulnerable children in its Management Information System, which is the provider of data on the number of children at risk in primary, secondary, and high school education. **Four categories of vulnerable children** have been established based on these legal provisions, data, and information (Annexes, Appendix 3):

1. **Children from low-income families**
2. **Children with limited parental communication and support** (this includes children living with only one parent or other family members, as well as children that reported that their caregivers did not speak with them about their experiences at school)
3. **Children with disabilities or special educational needs (SEN)**
4. **Children who speak a different language at home than school**

The following definitions are integral to the research:

- Children—represents individuals ages 10–17 years old and students from 5th to 11th grades of the educational institutions from the Republic of Moldova.
- Digital environment/online environment—any digital platform, channel, or social network used to create, store, and share digital content (such as photos, videos, podcasts, etc.).

- Internet—the worldwide network of computers connected to various social networks that enable the interconnection of local and global networks, facilitating data and information exchange in various fields.
- Social networking—digital platforms consisting of communities of individuals that share interests, activities, and relationships that enable the communication between people and work as a means of communication and information exchange.
- BeReal—a social media app that encourages authenticity by prompting users to take and share a photo at a random time each day, capturing what they are doing at that moment. It aims to create a more genuine and less curated social media experience.
- Discord—an instant messaging and digital distribution platform designed for creating communities. Users can communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities called "servers."
- Facebook—a social networking site where users can create profiles, share photos and videos, send messages, and keep in touch with friends, family, and colleagues. It offers a wide range of features including news feeds, events, groups, and pages for businesses and public figures.
- Instagram—a photo and video sharing social networking service. Users can upload media, which can be edited with filters, organized by hashtags, and tagged with locations. Posts can be shared publicly or with pre-approved followers.
- Messenger—a messaging app and platform developed by Facebook. It allows users to send text messages, make voice and video calls, and share photos, videos, and other media. Messenger can be used as a standalone app or integrated with Facebook.
- Snapchat—a multimedia messaging app known for its disappearing messages and stories. Users can send photos and videos that are only available for a short time before they disappear. Snapchat also offers various filters and augmented reality features.
- Telegram—a cloud-based instant messaging app that offers end-to-end encrypted messaging, video calling, file sharing, and several other features. It is known for its speed, security, and support for large group chats and channels.
- TikTok—a social media platform where users can create and share short videos, typically ranging from 15 to 60 seconds, set to music or other audio. It is known for its viral trends, dance challenges, and diverse range of content.
- Viber—a cross-platform voice over IP and instant messaging app. Users can send free messages, make voice and video calls, share images, videos, and other multimedia. Viber also offers end-to-end encryption for secure communications.
- VKontakte (VK)—a Russian online social media and social networking service similar to Facebook. It allows users to send messages; create groups, public pages, and events; share and tag images, audio, and video; and play browser-based games.
- WhatsApp—an instant messaging app that allows users to send text messages, voice messages, make voice and video calls, and share images, documents, user locations, and other media. It uses end-to-end encryption to ensure privacy and security.

The general hypothesis of the research is that children who face difficulties offline are also more prone to risk online.

More specifically, the study used the following **working hypotheses:**

1. Vulnerable children have less access to digital devices and the internet.
2. Vulnerable children are more prone to risk in the online environment.
3. Online behaviors of vulnerable children and their response to online risk situations are influenced by the specific characteristics of their vulnerability (low income, lack of parental care, SEN, etc.).
4. Adults (i.e., parents/caregivers, teachers, etc.) may not always be reliable sources of information and support for vulnerable children due to their lack of information, knowledge, and skills to cope with online challenges and difficulties.

1.3. Methodology

Overall Design

The research methodology was designed to facilitate understanding of children's behaviors in the digital environment, as well as the knowledge, practices, and experiences of children, parents, and specialists about risk factors, protective factors, and actions taken to prevent and combat digital risks, thus enabling data triangulation[5].

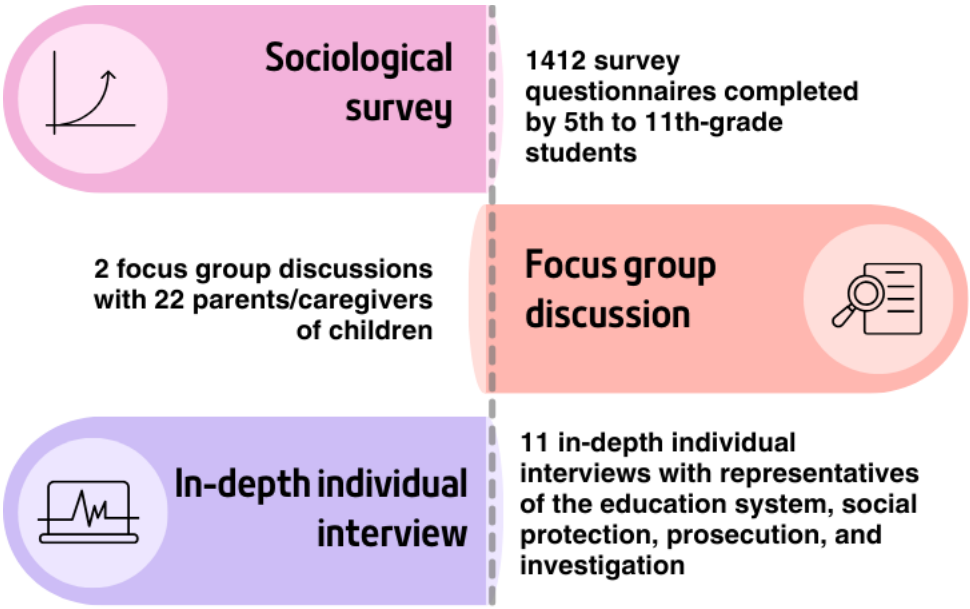
The research was based on a mixed methodology that combined quantitative methods used in the case of students and qualitative methods used with parents and specialists (Figure 2). The methods are as follows:

- Questionnaire for students in 5th to 11th grade
- In-depth interviews (IDIs) with specialists engaged in education, social protection, and law enforcement systems
- Focus group discussions (FGDs) with parents/caregivers of students in 5th to 11th grade

The quantitative method, which was the questionnaire-based sociological survey used with children, enabled the characterization of children's online behaviors, identification of the main areas of risks children face online, and identification of categories of children vulnerable in the digital environment. The qualitative methods of FGDs with parents and IDIs with specialists engaged in education, social protection, and law enforcement systems provided the opportunity to deepen the information obtained from children regarding the risks they face online. FGDs with parents provided information about parents' knowledge and awareness of children's risks online, measures or practices taken by them to ensure safe browsing for their children, and their needs for improving children's safety in the digital environment. IDIs revealed measures taken by educational institutions, the Psychopedagogical Assistance Service (PAS), child protection services, specialized services for children affected by online abuse, and prosecutors and investigation officers in charge of preventing and combating online risks in children, including the intervention and collaboration between various professionals.

5 Validation technique combining several data collection methods to reduce inherited distortions. Triangulation enables the accuracy and stability of results to be checked.

Figure 2. Research methods



Source: D4I

Target Participants

Participants in the research included children ages 10–17 years in gymnasium (5th to 9th grade) and high school (10th to 11th grade), parents or caregivers of children, and specialists in education, social protection, and law enforcement systems.

Quantitative Survey

Geography: The research was conducted throughout the territory of the Republic of Moldova, excluding the Transnistrian region. The sample covered five regions (Northern, Southern, Center, Chisinau municipality, and the Gagauzia Autonomous Territorial Unit [GATU)], including schools in both urban and rural areas.

The sampling strategy was designed to be by school grade rather than age specific. The sample was designed for the lower secondary cycle (5th to 9th grade) and upper secondary cycle (10th to 11th grade), including children with Romanian and Russian languages of instruction.

Purposive sampling was used to ensure a final sample with a high percentage of vulnerable children and to promote similarity to the country's schools overall on other characteristics (e.g. region, urban/rural designation). Specific schools within a geographic region that met one of the following criteria were preferentially sampled first: (i) small rural communities with a high poverty rate; (ii) localities where there are placement centers for children; (iii) localities with a large number of children in alternative family-type care (i.e., foster care); (iv) villages with a high percentage of Roma people; and (v) localities that have accommodation centers for Ukrainian refugees. If insufficient schools in the geographic area were identified to meet these criteria, additional schools were randomly selected from the MoER database. The proportion of urban/rural schools in the study sample is the same as in the MoER statistics. Similarly, the proportion of schools across each region matches the MoER statistics (see Appendix 4).

Within the educational institutions, questionnaires were administered in 5th to 11th grades. In the case of institutions with multiple classes in the same school grade, such as classes 8A, 8B, and 8C, class B was

selected. Because there is no reason to expect that class lettering is related to our outcomes of interest, this approach approximates random selection. In schools with only one class per grade, the questionnaires were administered in that single class.

First, all parents of students in the selected class were asked to provide their informed consent. Based on informed consent from parents, students with prime order numbers in the class register were sampled: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41. They were then asked to provide their written assent. Only students that had provided their parents' informed consent and their written assent participated in the research. Larger classes had more students selected as they had more prime numbers. Within each school, the proportion of students sampled per class matches that classes' proportion of the student body. For example, if 15% of children in a school were in 5th grade, then 15% of the sample was from 5th grade. The total sample comprised 1,412 children from 35 educational institutions[6] (Table 3). Response rates were not collected due to time constraints during data collection.

Table 3. Sociodemographic characteristics of the sample of children

		Number	%
Total		**1,412**	**100**
Gender	Boys	629	45
	Girls	783	55
Vulnerability Category[7]	Children without social vulnerability	264	19
	Children from low-income families	642	45
	Children with limited parental communication and support	604	43
	Children with disabilities or with SEN	507	36
	Children who speak a different language at home than at school	434	31
School grade	Grade 5	221	16
	Grade 6	228	16
	Grade 7	232	16
	Grade 8	232	16
	Grade 9	217	15
	Grade 10	160	11
	Grade 11	122	9
Age	10 years old	6[8]	0
	11 years old	152	11
	12 years old	224	16

6 Six educational institutions from the southern region, 2 from GATU, 8 in the North, 8 in the Center, and 13 in Chisinau, according to the data of the NBS and MoER for the 2023-2024 school year.
7 19% of children are not vulnerable. The other 81% of children experience one or more vulnerabilities. A child can be integrated in one or more vulnerability category/ies, as they may experience several vulnerabilities as is explained in Appendix 3. 58 children (4%) fit in all four vulnerability categories, 239 (17%) fit in three. 387 (27%) fit in two, and 467 (33%) fit in only one vulnerability category.
8 There are very few children aged 10 as the large majority of 5th grade students have already turned 11 years old.

		Number	%
	13 years old	227	16
	14 years old	224	16
	15 years old	251	18
	16 years old	183	13
	17 years old	145	10
Geographical area where the school is located	Northern	342	24
	Center	303	21
	Southern (including GATU)	199	14
	Chisinau	568	40

IDIs and FGDs

IDIs were conducted with 11 specialists, experts, and service providers in the field of online safety, child psychology, and education to ensure a comprehensive exploration of perspectives from professionals actively engaged in child well-being and education. Participant selection was purposive as it helped to prioritize diversity and ensure the inclusion of professionals with varied backgrounds and perspectives in the research. It included both national and local-level participants possessing specific knowledge, expertise, and information about online safety for children; the digital inclusion of vulnerable children; and the provision of services to children who are victims of digital crimes. All the specialists were women, as the fields of education and social assistance are feminized. Interviews were held with:

- Three managers and one psychologist, all private providers of specialized services for vulnerable children, including children affected by digital harm
- Two specialists from the PAS (one manager and one psychologist)
- Three representatives of educational institutions (one school principal, one teacher, and one school psychologist)
- One officer investigating crimes against children in the online environment
- One prosecutor dealing with online crimes against children (Appendix 5, Table 2)

Two FGDs were held with 22 parents/caregivers (17 women and 5 men). The selection was also purposive, aiming to include the perspectives of parents/caregivers and understand the challenges they face, ultimately developing relevant recommendations. This selection ensured diversity, encompassing parents and caregivers that are both men and women, individuals from rural and urban areas, and those with children in different school grades and varying educational backgrounds. The FGDs with parents/caregivers facilitated a dynamic exchange of ideas among participants, as one FGD was with parents/caregivers from urban areas (eight women and two men) and another FGD with parents/caregivers from rural areas (nine women and three men) (Appendix 5, Table 1).

Data Collection

The questionnaire for children had six sections: 1. General information; 2. Knowledge about the vulnerability characteristics of children participating in the research; 3. Use of internet; 4. Social media; 5. Behaviors in the digital environment; and 6. Online safety. The questionnaire was reviewed by

psychologists for age appropriateness and was finalized based on a pretest conducted with children. The collection of quantitative data was carried out during the period of April 22–May 15, 2024.

The questionnaires for children were applied in the educational institutions. A self-administered questionnaire was utilized through phone or tablet via an online platform, providing anonymity for respondents. The questionnaire was available on the platform in Romanian and Russian languages, and students could choose the language they wanted to answer in. The research team supervised the administration of the questionnaires to explain the purpose of the study and how to fill in the questionnaire and, at the same time, avoid (i) the intrusion of educational staff or other people when answering the questionnaire, (ii) discussing and commenting on questions among children, (iii) answering the questions by voice, (iv) situations where a student sees another child's answers or the educational staff want to see what the child has responded, and (v) potential conflicts between children.

The FGDs were carried out between May 18–25, 2024, and the IDIs were carried out from May 27–June 10, 2024.

Data Analysis

Quantitative data were analyzed using SPSS software. Data were checked to avoid questionnaire double data entry, missing data, and other issues. The analysis at the first stage involved frequency analysis for all questionnaire variables. All results were disaggregated by pupils' gender, age, school grade, geographical area, and non-vulnerable and vulnerable categories. Analyzing the results separately for each gender enabled capturing nuances and variabilities that may not be evident in general analysis. After that, the team analyzed the vulnerability status of children and its relationship to access to digital services and online behavior.

The qualitative analysis looked at the role of adults, including parents/caregivers and teachers, in addressing online challenges and issues faced by vulnerable children. The research team examined adults' perceptions and experiences regarding their ability to support children online, analyzed potential gaps in support, and identified areas for intervention and improvement. The analysis involved triangulating data on vulnerability characteristics with online behavior and risk experiences.

Data interpretation in the report depended on the school grade level rather than age, due to the fact that children's age in each grade is influenced by the date of September 1, which is when the school year begins. The recommended age for the 1st grade is seven years old, but parents decide whether to enroll children who turn seven in autumn. The data was collected from children between April and May, in the second period of the school year. This led to age variations among students within the same school grade (Table 4).

Table 4. Age distribution of children by school grade (%)

		Age							
		10 years old	11 years old	12 years old	13 years old	14 years old	15 years old	16 years old	17 years old
School grade	Grade 5	3	65	32					
	Grade 6		3	65	32				
	Grade 7			3	65	32			

		Age							
		10 years old	11 years old	12 years old	13 years old	14 years old	15 years old	16 years old	17 years old
	Grade 8				1	62	37		
	Grade 9					2	72	26	
	Grade 10						7	71	22
	Grade 11							10	90

1.4. Ethical Considerations

The research complied with ethical principles and norms promoted by the United Nations Evaluation Group, including ethical standards for research put forth by UNICEF. The resulting research protocol comprised aspects related to the protection of children's and adults' identities participating in the research, aspects related to ensuring the safety of children participating in the research, and protection of data collected. Participants were informed about the context and purpose of the research and about respecting the principles of anonymity (survey participants) and confidentiality (interviewees and participants in the FGDs). The research team paid particular attention to (i) respect for dignity and diversity, (ii) right to self-determination, (iii) fair representation, (iv) ethical protocols for children, (v) redress, (vi) children's privacy, (vii) harm avoidance, (viii) secure storing the data, and (ix) ethical use of data. Written consent for children's participation in the research was secured from one of their parents/caregivers, and after that, written assent was obtained from the child.

The research team informed children about the resources available for addressing online problems. The children were informed that if they or their friends encounter online issues, they can reach out to the school psychologist or teacher or call 116 111, the number for Telefonul Copilului (Child Helpline), or 0 800 10 808, the hotline run by the Alliance of Organizations for Persons with Disabilities. The helplines are free and also confidential.

1.5. Research Limitations

The following limitations influenced the implementation of the research:

1. **Exclusion of the Transnistrian region.** The research was not carried out in the Transnistrian region (which is not controlled by the authorities of the Republic of Moldova) due to security concerns and political issues. Thus, the results do not reflect these children's experiences.
2. **Some parents/caregivers were reticent about giving written consent for their children's participation in the research.** The research team, together with representatives of educational institutions, informed parents and children about the purpose of the research and data privacy, thus reducing the refusals as much as possible. We were also not able to collect response rates due to the time constraints during data collection.
3. **Exclusion of children ages 15–17 who do not continue their education after graduating from secondary school**. Some children do not pursue education after the 9th grade.[9]

[9] According to the National Bureau of Statistics, 18% of 9th grade graduates did not continue their studies in the 2023–2024 school year.

II. Children in the Digital Environment

2.1. Access to the Internet and Time Spent Online

The internet provides many opportunities for information, communication, and development for children. It is an immediate and fast way of communication, but also a place with unrestricted access to information, knowledge, and entertainment. The results reveal a high level of children's access to the internet in the Republic of Moldova, proving that the digital environment has become an integral part of their everyday lives. Ninety-seven percent of children in the 5th to 11th grades are online daily, and only 3% have restricted internet access during school days. On their days off or vacation, the number of children with restricted access is insignificant (1%). Consequently, nearly all children in the Republic of Moldova have access to the internet and mobile devices, irrespective of their family background and whether they come from affluent or disadvantaged households.

Specialists participating in the research emphasized that some children have access to the internet from a very young age, 3–5 years old. However, internet access varies and is influenced by the family's socioeconomic status. Parents reported that many socially vulnerable families do not limit children's access to the internet (*"They do not have enough financial sources but still buy smartphones for their children, they do not limit themselves"* (FGD_2_R); however, a few categories of children have more limited access. According to them, restricted or low access to the digital environment is typical for some children with disabilities and children neglected by parents. For example, some participants pointed out that alcohol-addicted parents are less able to focus on their children's needs. Although these children are directly deprived of access, they still use the internet, being helped by their peers or other adults who provide them with access opportunities in various public spaces (such as educational institutions, libraries, parks, etc.).

Data shows that 14% of 5th to 11th graders use the internet on school days for up to 1 hour, 51% between 1 and 3 hours, and 32% for more than 3 hours. Time spent online increases with school grade. Thirty-eight percent of children from low-income families, 37% of children with disabilities or with SEN, and 35% of children with limited parental communication and support spend more than 3 hours online daily, compared to 24% of children without social vulnerability (Table 5).

Table 5. Time spent online by children during school days (%)

Vulnerability Category	Up to 1 hour	Between 1 and 2 hours	Between 2 and 3 hours	Between 3 and 4 hours	More than 4 hours	Not at all
Total	**14**	**28**	**23**	**14**	**18**	**3**
Children without social vulnerability	15	35	25	14	10	1
Children from low-income families	14	25	20	15	23	3
Children with limited parental communication and support	13	28	21	13	22	3
Children with disabilities or with SEN	13	25	21	14	23	4
Children who speak a different language at home than at school	16	28	21	12	19	4

The amount of time children spend online on their days off and on vacation is larger than on school days. Thus, 41% of children spend more than 4 hours online these days. The proportion of children from vulnerability categories that spent more than 4 hours online during days off and on vacation is higher than those children that were not classified as vulnerable (Table 6). Moreover, children from the municipality of Chisinau spend more time online, both on school days and on days off.

Table 6. Time spent online by children during vacation (%)

Vulnerability Category	Up to 1 hour	Between 1 and 2 hours	Between 2 and 3 hours	Between 3 and 4 hours	More than 4 hours	Not at all
Total	**4**	**11**	**21**	**22**	**41**	**1**
Children without social vulnerability	2	16	23	25	34	0
Children from low-income families	4	8	20	20	47	1
Children with limited parental communication and support	3	10	18	21	47	1
Children with disabilities or with SEN	4	9	19	20	48	0
Children who speak a different language at home than at school	5	12	21	19	42	1

When asked about the largest number of hours spent online daily during the last month, the time varied from 1 hour to 24 hours; the largest differences were observed by grade and vulnerability criteria. On average, the largest amount of time spent online by children was 6 hours per day. The number of hours spent online increases with grade. In the 5th–6th grade, 5 hours; in the 7th grade, 6 hours; and in other grades, 7 hours. Children from the socially vulnerable categories spent, during the last month, 2 hours more per day than non-vulnerable children in the online environment (Table 7).

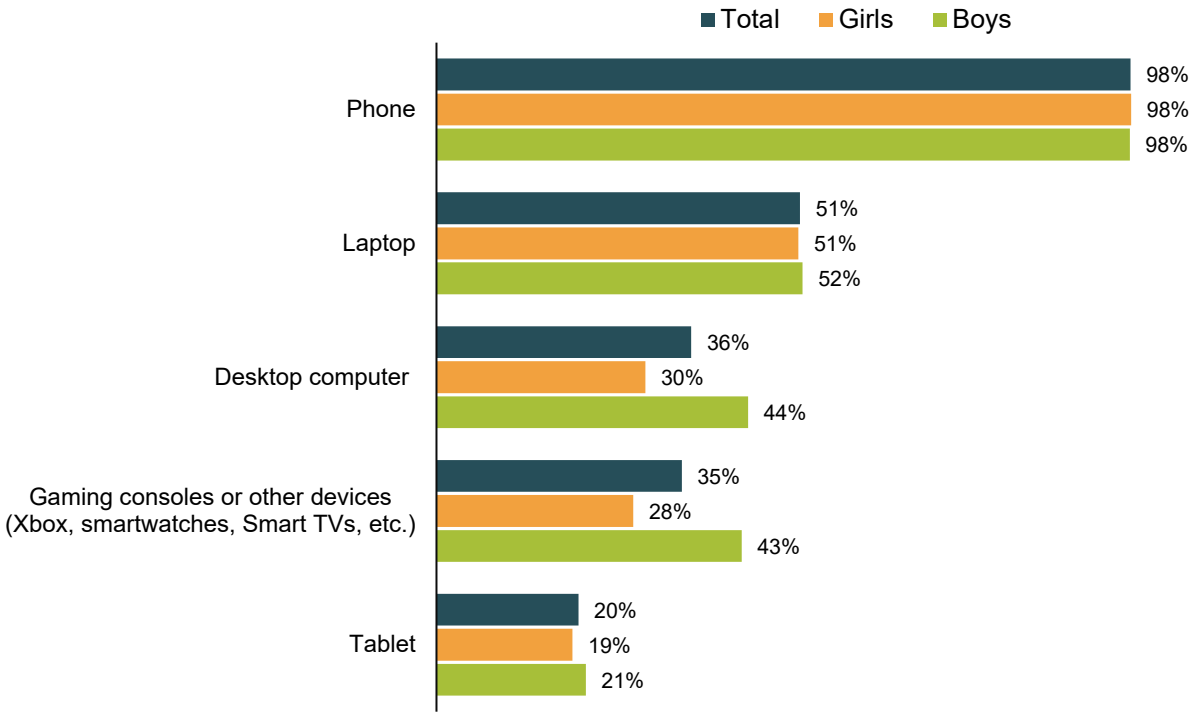
Table 7. The largest number of hours spent online by children during a day, within the last month

Vulnerability Category	Mean	Median	Mode	Minimum	Maximum
Total	**6**	**5**	**5**	**1**	**24**
Children without social vulnerability	5	4	3	1	20
Children from low-income families	7	6	5	1	24
Children with limited parental communication and support	7	5	5	1	24
Children with disabilities or with SEN	7	5	4	1	24
Children who speak a different language at home than at school	6	5	5	1	24

2.2. Devices Used to Access the Internet

Students stay abreast of new technologies, including how to use them. The internet is most often accessed via phone and less often from laptops, desktop computers, gaming consoles, or other smart devices, such as tablets, by all children. There is a slight difference in internet access on devices depending on a child's gender. A larger proportion of boys use desktop computers, gaming consoles, or smart devices, potentially due to greater interest in online games compared to girls (Figure 3).

Figure 3. Children accessing the internet, by type of device and gender (%)



2.3. Internet Access Points

Children from the Republic of Moldova use various opportunities to access the internet. The number of internet access points increases with the increase in children's school grade and age. Children without social vulnerability access the internet more at home (92%) and school (35%) compared to children from vulnerability categories (87–89% and 28–33%, respectively). Children from vulnerability categories access the internet more via Wi-Fi in public spaces and mobile internet. Data revealed that children from vulnerability categories have less internet access at home and school than in other public spaces, which confirms the working hypothesis that vulnerable children have less access to digital devices and the internet (Table 8).

Table 8. Children accessing the internet, by access point and vulnerability category (%)

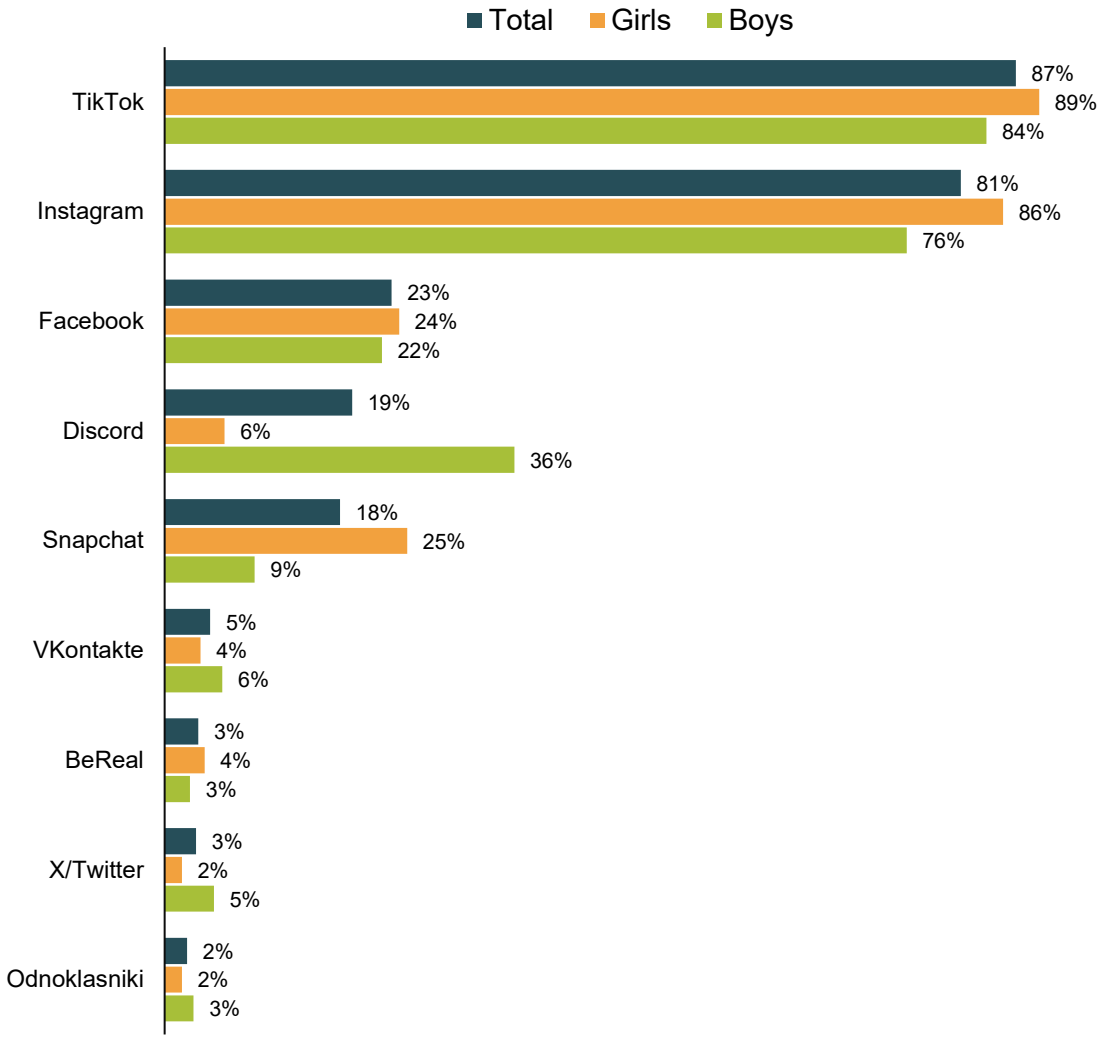
Vulnerability Category	At home			At school			Via WiFi in public places**			Anywhere, via mobile internet		
	Y*	S*	N*	Y*	S*	N*	Y*	S*	N*	Y*	S*	N*
Total	**90**	**8**	**2**	**31**	**33**	**36**	**36**	**37**	**27**	**63**	**28**	**9**
Children without social vulnerability	92	7	1	35	30	35	37	38	25	61	28	11
Children from low-income families	87	10	3	31	33	36	39	35	26	63	28	9
Children with limited parental communication and support	88	9	3	33	33	34	38	35	27	65	27	8
Children with disabilities or with SEN	89	8	3	28	31	41	35	38	27	65	25	10
Children who speak a different language at home than at school	87	10	3	32	34	34	37	36	27	63	28	9

* Y – Yes, S – Sometimes, N - No.
** parks, libraries, cafes

2.4. Social Media Account/Profile

Ninety-three percent of children have at least one social media account. Only 83% of 5th graders have a social media account, compared to students in the 11th grade (98%). Children prefer various social networks, and there are differences between boys and girls and a few differences linked to age/grade and social vulnerability (Figure 4). For example, children in 5th to 9th grades prefer TikTok, and those in 10th to 11th grade opt more for Instagram. Children from vulnerability categories choose TikTok (87% to 89%), Discord (19% to 23%), and Snapchat (17% to 19%).

Figure 4. Favorite social networks used by children, overall and by gender (%)



2.5. Purpose of Internet Use

The impact of informational technologies on society, particularly children, is tremendous. Children explore the opportunities provided by the digital environment as recipients of content, participants in various activities, initiators of activities, and users of various marketing materials. The digital environment has become part of the daily activities of children ages 10–17, being used for different purposes (Figure 5). This study shows that children use the digital environment mainly for communication (64% talked or sent/received video, audio, or text messages daily), socializing (59% accessed profiles on social networks daily), and spending free time (46% watch video clips, vlogs, and online movies daily). The digital environment was used less for personal development or homework (27% look for information needed to complete homework daily). There are differences in how children use the internet depending on their school grade, age, gender, and vulnerability category.

Specialists participating in the research emphasized more factors that influence the use of the digital environment: parents' education level, parents' control and supervision, and socioeconomic status of the family. Most of the interviewed specialists believe that children from families with higher socioeconomic status and a high level of parental education benefit more often from parental control, and the content they access is filtered. In these families, parents more often explain to their children about online safety, and children understand the online risks, while in the families that do not discuss the digital environment, *"Children do not understand what is normal and what is abnormal to do online, and subsequently, the abnormality becomes a norm"* (III_1).

Sixty-four percent of children spent time online daily within the last 3 months to communicate or send/receive video, audio, or text messages in real-time, and 59% accessed their personal social media accounts daily. Girls use the digital environment for these purposes more frequently than boys, and children from higher grades use it more frequently than those from lower grades.

Forty-six percent of children watch online videos, vlogs, and movies daily. Boys, students from higher grades, and children from vulnerable categories do this more frequently.

Forty percent of children use the internet daily to listen to music online, downloading and streaming it. Girls and students from 9th to 11th grade do this more frequently.

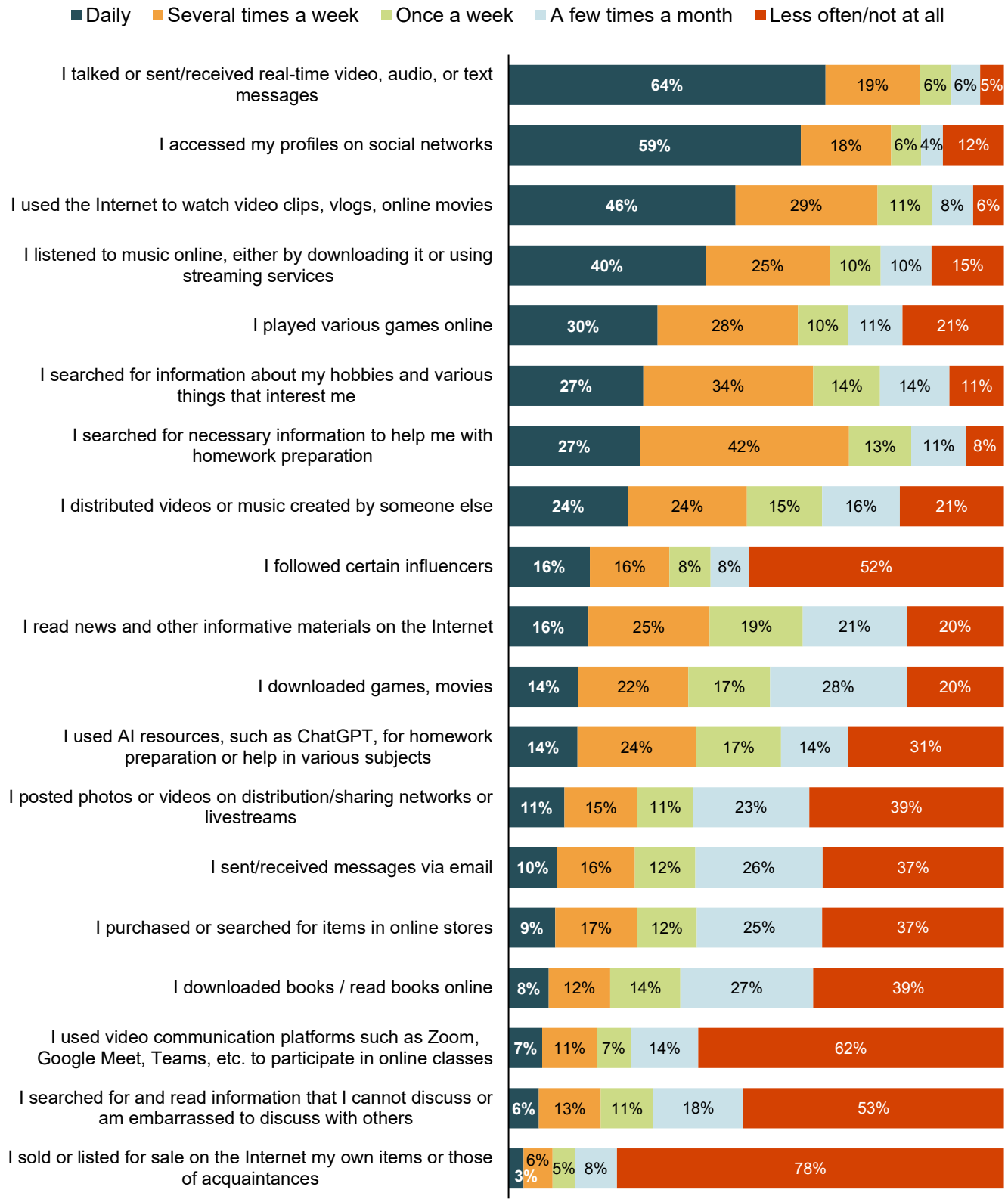
Thirty percent of children are engaged in online gaming daily. Boys play video games more often (46%) than girls (18%), as do younger students (40% of 5th graders) than older ones (25% of 11th graders).

Twenty-seven percent of children search daily for information about hobbies and interests, information necessary for their homework, and share videos or music made by others. Students in higher grades frequently use the internet for these purposes compared to those in lower grades. Only 15% of 5th graders search for information about hobbies or things they are interested in, compared to 40% of the 11th graders, which is also typical for homework.

Sixteen percent of children follow influencers daily, and 16% read daily news and other information resources. The share of children engaged in such activities in the digital environment increases with school grade and age.

AI resources, such as ChatGPT, are used for homework or other subjects daily by 14% of children and a few times a week by 24% of children. Boys and older students use the internet more often for this purpose.

Figure 5. Children's internet use in the last 3 months, by frequency and purpose (%)



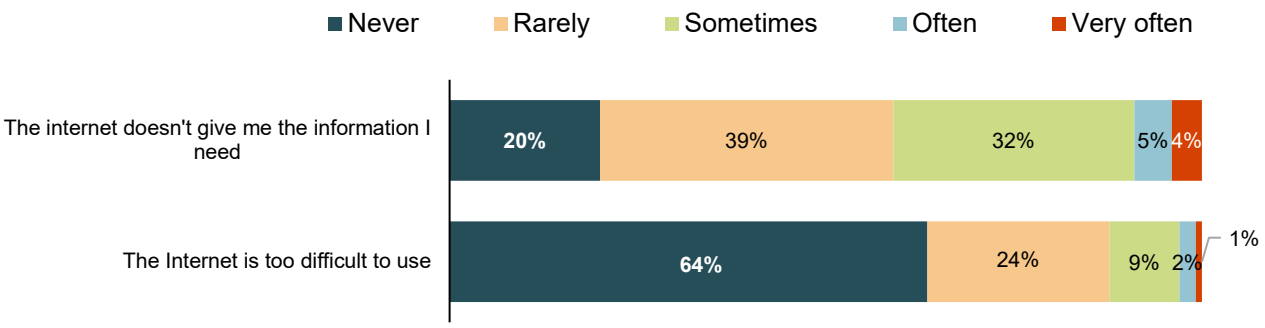
Eleven percent of children post photos and videos on social networks of livestreams daily, and 15% post a few times a week. These activities are carried out more frequently by girls and children from socially vulnerable categories, who do it twice as often daily compared to children without vulnerability.

Rarely do children use the internet to sell or advertise certain personal items/belongings. The number of those doing this daily, once or a few times a week, or monthly is 22%.

Significantly, 47% of children seek information they cannot discuss or are ashamed to discuss with someone else (daily, a few times a week, or a few times a month). This situation is typical mostly to children in 8th to 11th grades and those without social vulnerability.

Children have no difficulty accessing the internet. Only 9% of children believe that sometimes the internet is too difficult to use. At the same time, 41% of children agree that the internet meets their needs (sometimes, often, very often), providing them with needed information (Figure 6).

Figure 6. Children's opinions about the internet (%)



III. Children's Online Behaviors, Practices, and Experiences

3.1. Children's Online Behavior

Twenty-one percent of children claim that the internet never consumes too much time, while 29% believe it rarely happens, compared to 32% who claim that the internet takes too much time sometimes, 13% who claim it does often, and 5% who claim it does very often. Girls agreed to a greater extent that the internet consumes too much time, as well as the 11th grade students. Moreover, children from low-income families and children with disabilities or SEN pointed out this situation more often (Table 9).

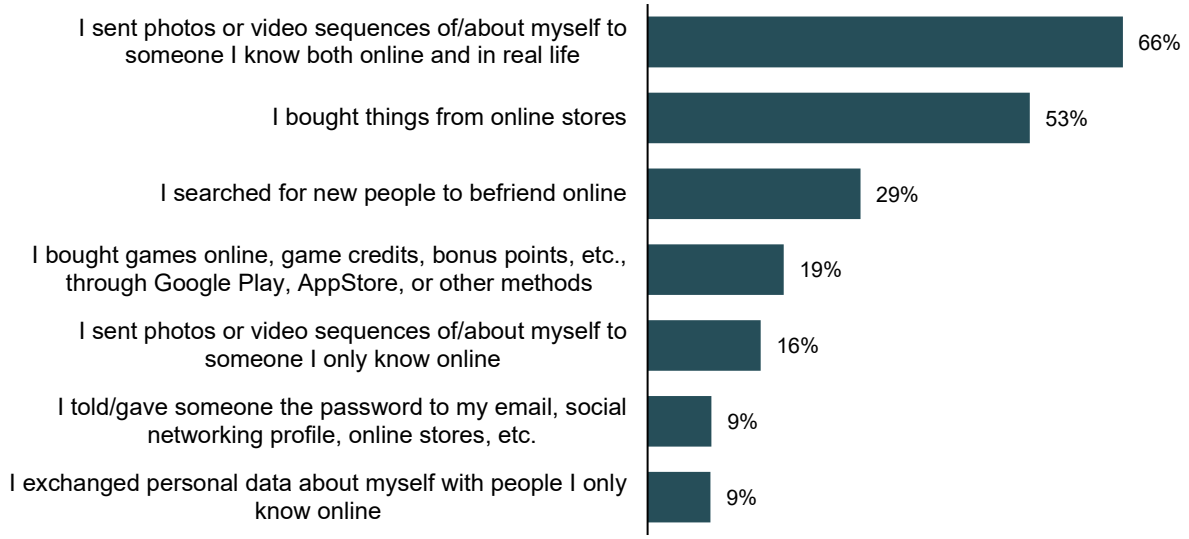
Table 9. Situation when children consider that internet consumes too much time (%)

Vulnerability Category	Never	Rarely	Sometimes	Often	Very often
Total	**21**	**29**	**32**	**13**	**5**
Children without social vulnerability	26	28	31	12	3
Children from low-income families	18	27	33	16	6
Children with limited parental communication and support	20	30	33	10	7
Children with disabilities or with SEN	19	26	31	17	7
Children who speak a different language at home than at school	23	28	34	11	4

For children, the internet has become a means of communication as well as a way to shop for various items, including games. Most often, children use the internet to share photos and videos via Messenger, Viber, WhatsApp, Discord, forums, chat rooms, etc., with a person they know in real life (66%) and for online shopping (53%). For 29% of children, within the last three months, the internet was the place to seek new friends (Figure 7).

Actions taken by children on the internet in the last three months differ according to sociodemographic characteristics. For example, 72% of girls prefer to share photos and videos via Messenger, Viber, WhatsApp, Discord, forum, chat room, etc., with a person they know in real life, compared to 58% of boys. Thirty-one percent of boys prefer instead to buy online games, game credit, bonuses, etc., via Google Play, the App Store, or other means, compared to only 9% of girls.

Figure 7. Actions taken by children on the internet in the last 3 months (%)



There is a greater proportion of children from 9th to 11th grade that reported looking for new friends online, sharing personal photos and videos, or sharing information (such as phone number, home address, name of the school, information about their parents, etc.) with people they only know online than the other grades. Significant differences were revealed that were linked to a child's social vulnerability category. Vulnerable children, to a large extent, look for new friends in the digital environment (32% to 38% in comparison to 21% of the non-vulnerable); buy games or game credits through Google Play, the App Store, or other methods (21 to 22% in comparison to 14% of the non-vulnerable); send personal photos or video sequences to strangers (17% to 19% in comparison with 9% of the non-vulnerable); or exchange personal data (such as phone number, home address, name of the educational institution they attend, information about parents, etc.) with people they only know online (8% to 12% in comparison with 5% of the non-vulnerable) (Table 10). The data confirms the second working hypothesis that vulnerable children are more prone to risk in the digital environment.

Table 10. Potentially risky actions taken by children on social networks (%)

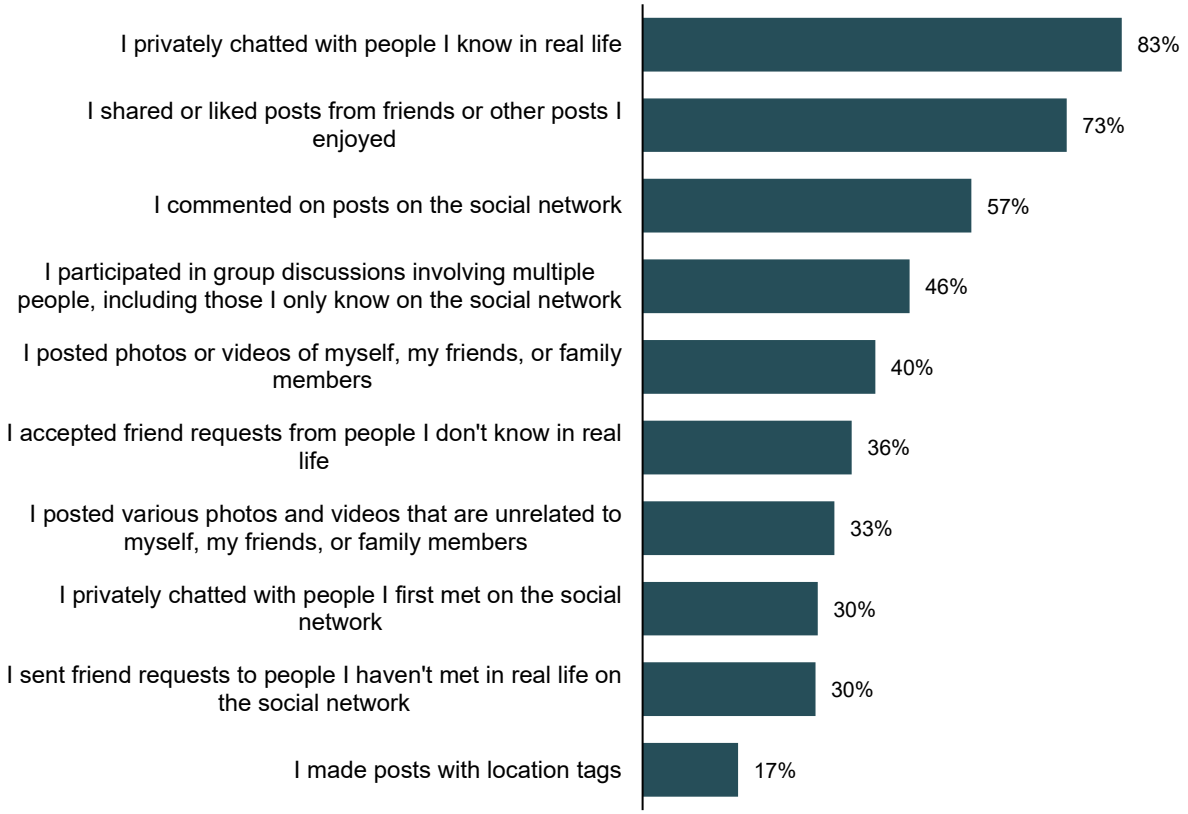
Vulnerability Category	I searched for new people to befriend online	I bought games online, game credits, etc., through Google Play, AppStore, or other methods	I sent photos or video sequences of/about myself to someone I only know online	I exchanged personal data about myself with people I only know online
Total	**29**	**19**	**16**	**9**
Children without social vulnerability	21	14	9	5
Children from low-income families	38	22	19	12
Children with limited parental communication and support	32	21	19	11

Vulnerability Category	I searched for new people to befriend online	I bought games online, game credits, etc., through Google Play, AppStore, or other methods	I sent photos or video sequences of/about myself to someone I only know online	I exchanged personal data about myself with people I only know online
Children with disabilities or with SEN	35	22	19	11
Children who speak a different language at home than at school	32	21	17	8

3.2. Children's Practices on Social Media

The research outcomes highlight that 83% of children use social networks to communicate privately with people they know in person, to share and follow friends' posts or other posts they enjoy, and to comment on posts on social networks (Figure 8).

Figure 8. Actions taken by children on social networks in the last 3 months (%)



Forty-six percent of children accessing social networks chat in large groups, including with people they are acquainted with only online. A larger proportion of boys and children with social vulnerability reported doing this than girls and children without social vulnerability, respectively. For example, 54% of children from low-income families chat on social networks in large groups, including with people they don't know offline, compared to 34% of children without vulnerability (Table 11).

Table 11. Chatting on social networks in large groups, including people unknown in real life, by gender and social vulnerability (%)

	Yes	No	I do not want to answer
Total	**46**	**47**	**7**
Boys	52	41	7
Girls	42	52	6
Children without social vulnerability	34	58	8
Children from low-income families	54	38	8
Children with limited parental communication and support	49	44	7
Children with disabilities or with SEN	49	45	6
Children who speak a different language at home than at school	51	41	8

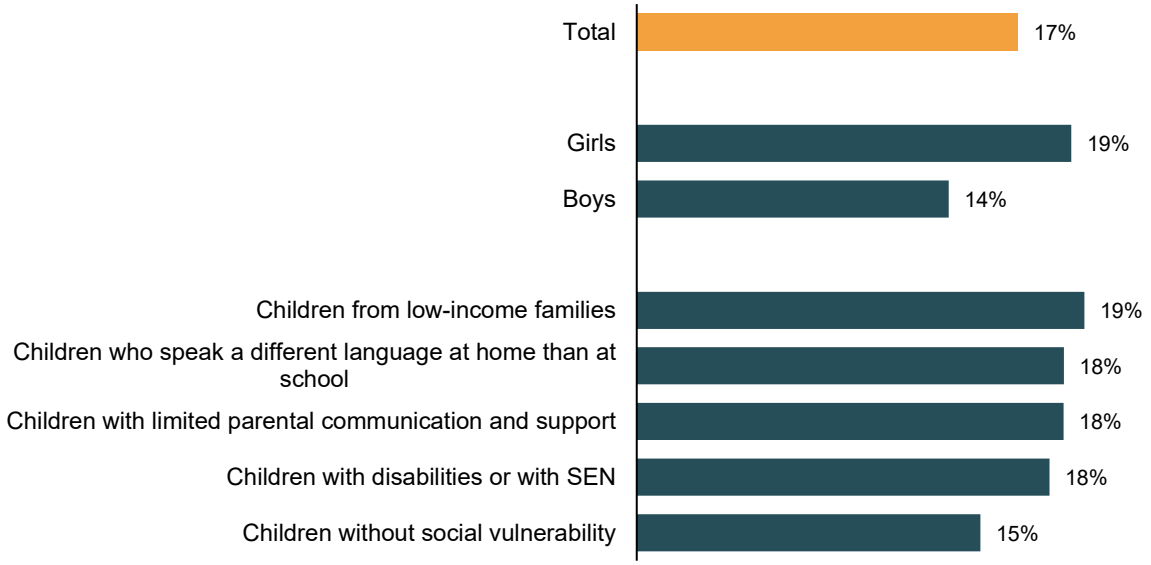
Some children use social networks to be accepted or to find new friends. Within the last three months, 36% of children accepted friendship or connection requests from people they did not know in real life, 30% communicated with people they met for the first time on social networks, and 29% sent friendship or connection requests to people they did not meet in real life. Differences are linked to gender, school grade, age, and the degree of social vulnerability. The data show that children from vulnerability categories undertake such actions in the digital environment to a greater extent than children not from the vulnerability categories. For example, 38% to 43% accepted friend or connection requests from people they don't know offline compared to 27% of children who are not vulnerable. Forty-three percent of children from low-income families use social networks to communicate and make friends (Table 12).

Table 12. Searching friendship on social networks, according to the degree of social vulnerability (%)

	I have accepted connection requests from people I don't know in person	I have chatted privately with people I don't know in person	I have sent connection requests to people I have not met in person
Total	**36**	**30**	**30**
Children without social vulnerability	27	20	21
Children from low-income families	43	38	36
Children with limited parental communication and support	39	34	35
Children with disabilities or with SEN	39	35	34
Children who speak a different language at home than at school	38	29	33

Seventeen percent of children ages 10–17 posted their location on social networks within the last three months. Girls and children from vulnerability categories did this to a greater extent than boys and children not from vulnerability categories (Figure 9).

Figure 9. Children posting their location on social networks, by gender and social vulnerability (%)



3.3. Children's Negative Experience Online

Fifty-seven percent of children revealed they had faced negative online experiences within the last three months, such as being blocked on social networks**,** having their social media accounts hacked, receiving inappropriate images or messages with sexual content, and being asked to send personal images or videos containing intimate parts of their body. Various adverse incidents were experienced to a greater extent by boys (62%), children from low-income families (67%), children with disabilities or with SEN (65%), and children with limited parental communication and support (62%) (Table 13).

Table 13. Children that faced online negative experience, by gender and social vulnerability (%)

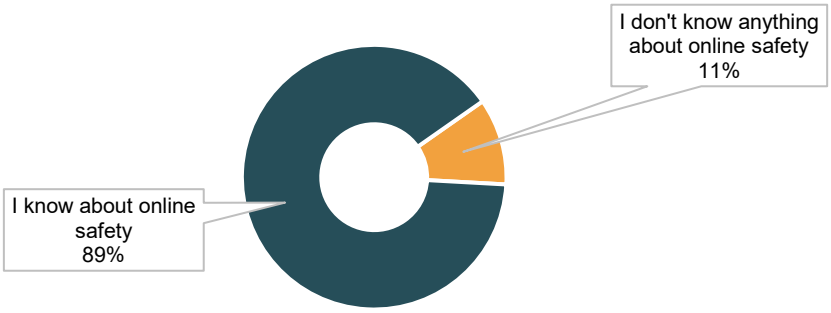
Category of children	Yes	No
Total	**57**	**43**
Boys	62	38
Girls	52	48
Children without social vulnerability	43	57
Children from low-income families	67	33
Children with limited parental communication and support	62	38
Children with disabilities or with SEN	65	35
Children who speak a different language at home than at school	60	40

IV. Children's Knowledge and Awareness of Online Risks

4.1. Online Safety Resources

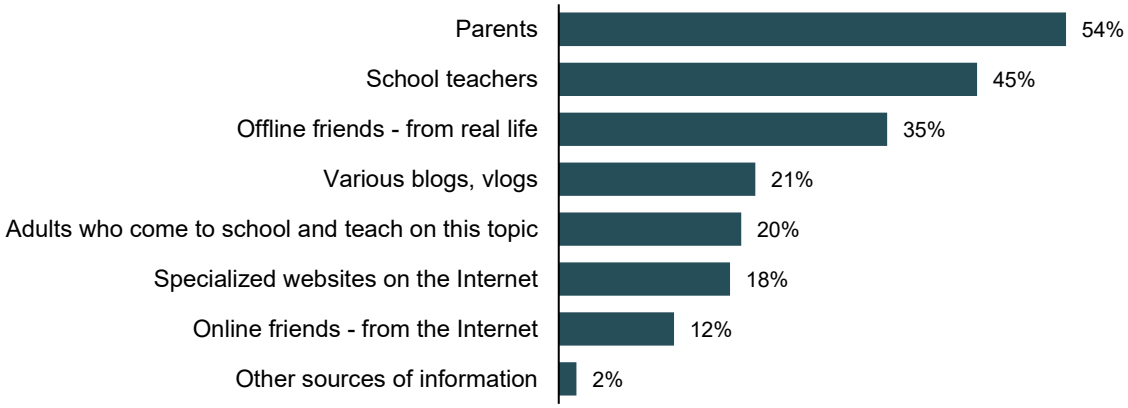
Quantitative data shows that 11% of children know nothing about online safety and have no source of information (Figure 10). Fifteen percent of boys, 16% of children whose mother tongue is different from the language of instruction, and 16% of 5th grade students reported knowing nothing about online safety.

Figure 10. Children's awareness about online safety (%)



Children who reported that they know about online safety cited various sources of information. Along with parents, educational staff play an important role in the information process, followed by friends from the offline environment (Figure 11). Parents and teachers are the main sources of information, to a greater extent, for girls (62%), younger students (64% of 5th grade students), and those from families without social vulnerability (65%).

Figure 11. Sources of information regarding online safety for those who know about online safety (%)



Parents represent a source of information for 46% of children from low-income families and for 47% of children with limited parental communication and support. School staff, to a lesser extent, are a source of information about online safety for these children (Table 14). Data confirm the fourth working hypothesis that adults (such as parents/caregivers, teachers) are not always reliable sources of information and

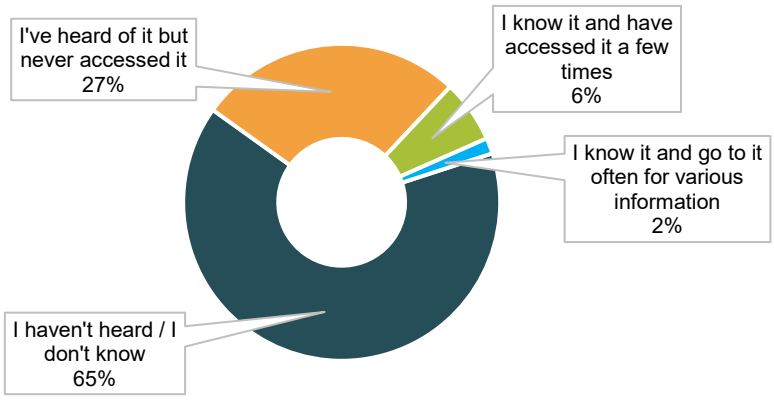
support for vulnerable children due to their lack of information, knowledge, and skills to cope with online challenges and difficulties.

Table 14. Online safety resources for children, depending on the category of social vulnerability (%)

Vulnerability Category	Parents	School teachers	Offline friends - from real life	Various blogs, vlogs	Adults who come to school and teach on this topic	Specialized websites on the internet	Online friends
Total	**54**	**45**	**35**	**21**	**20**	**18**	**12**
Children without social vulnerability	65	55	34	22	23	22	11
Children from low-income families	46	38	34	21	15	17	13
Children with limited parental communication and support	47	40	34	21	17	19	13
Children with disabilities or with SEN	52	46	34	22	20	20	14
Children who speak a different language at home than at school	51	39	36	16	17	16	14

Specialized Moldovan websites for preventing and combating risks in the online environment are not well known by the children participating in the research. For instance, only 6% of children are familiar with the website www.siguronline.md[10] and have accessed it a few times, and only 2% have used it often for various information. Another 27% of children have heard of this website but have never accessed it. Data proves that children without social vulnerability have more knowledge of this website, although they do not use it (32%) (Figure 12).

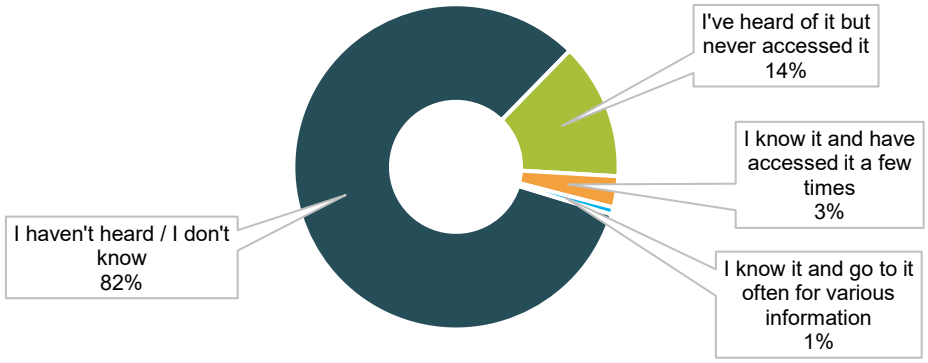
Figure 12. Children's awareness of the website www.siguronline.md



[10] See more about www.siguronline.md service in chapter 6.3.

As far as another specialized website is concerned, www.12plus.md[11], only 3% of children are familiar with it and have accessed it a few times, and only 1% used it often for various information. Fourteen percent of children have heard of this website but have never accessed it. Children without social vulnerability have more knowledge about this website, although they do not use it (16%) (Figure 13).

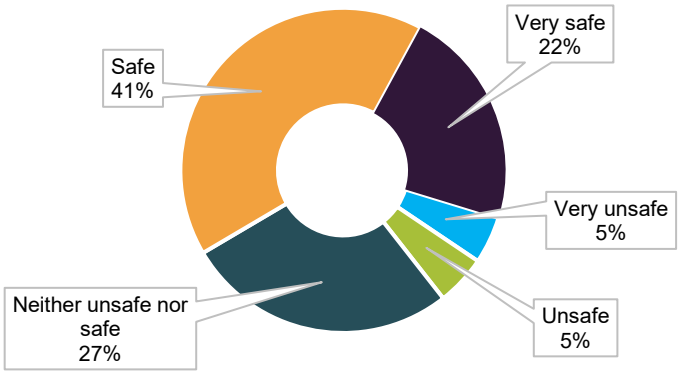
Figure 13. Children's awareness of the website www.12plus.md



4.2. Self-Perception of Safety and Awareness of Risks in the Digital Environment

Although there are challenges and risks in the digital environment, 63% of children said they feel safe and very safe online (Figure 14). Children from low-income families, children with limited parental communication and support, as well as children with disabilities or SEN, reported a higher level of safety in the digital environment.

Figure 14. Children's self-perception of their online safety (%)



[11] See more about www.12plus.md service in chapter 6.3.

Children self-evaluated their online practices, which show their awareness and prevention of particular risks related to their online safety (Figure 15). Eighty-one percent of children are always careful about what they say or post online. Such behavior is more typical for girls (86%), children from families without social vulnerability (89%), and 11th grade students (89%).

Seventy-three percent of children mentioned that they always use applications and sites they trust. Such behavior is more typical for girls (76%), children from families without social vulnerability (82%), and 11th grade students (77%).

Seventy-two percent of children are always careful about the links and videos they access. Girls are more careful about this aspect (73%), as are children from families without social vulnerability (77%).

Seventy-two percent of children are always careful about the friendship or connection requests they accept. Such behavior is more typical of girls (75%), children from families without social vulnerability (76%), and 11th grade students (77%). The number of children who are always careful about this aspect increases with school grade and age.

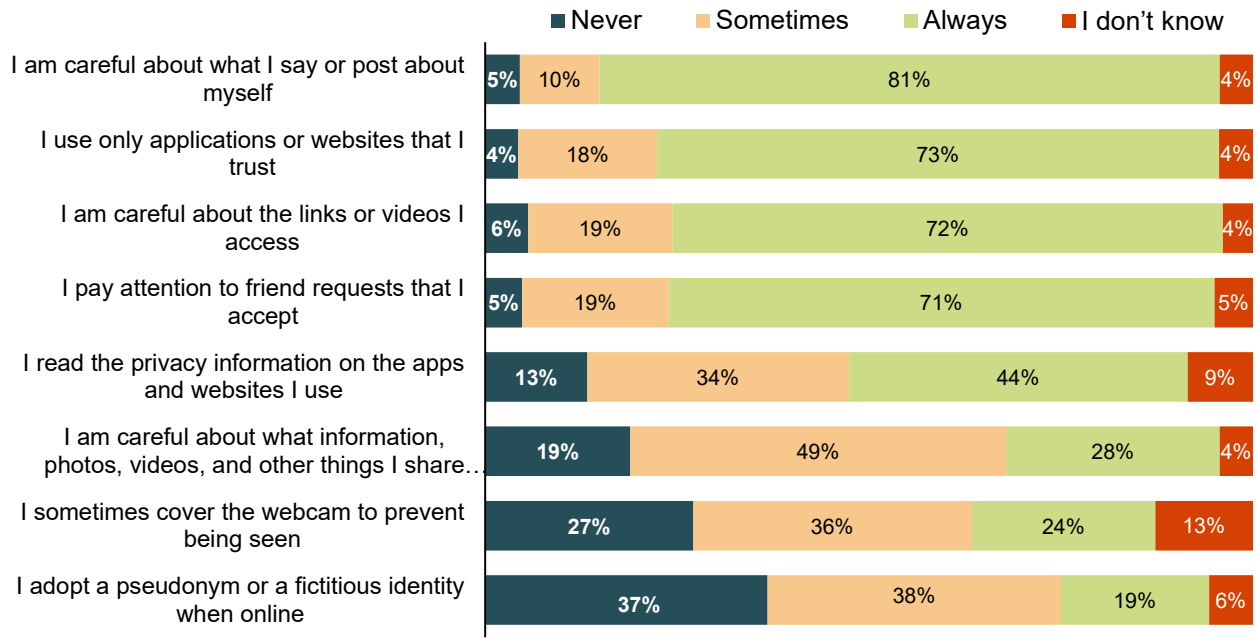
Only 44% of children are aware of certain contract risks and always read the information related to data privacy on the websites they access. There are significant differences linked to gender, with girls being more responsible (47%), as are children from families without social vulnerability (56%).

Children pay less attention to the information, photos, and videos they share with their close friends. Only 28% are always careful, and 49% are sometimes careful about their content.

Twenty-four percent of children always cover their web camera to prevent being seen. Girls (26%) take this action way more frequently than boys (21%). At the same time, as their school grade increases, the number of those who always do this increases, from 19% in the 5th grade to 30% in the 11th grade.

Using a fake name or identity online is practiced by 19% of children always and 38% sometimes. Twenty-four percent of boys and 15% of girls always use a fake name or identity in the digital environment. Children from vulnerable families (16%) and older students (14% of the 11th graders) rarely use fake names in the digital environment.

Figure 15. Aspects that children pay attention to when surfing the internet (%)



4.3. Cross-Cutting Risks

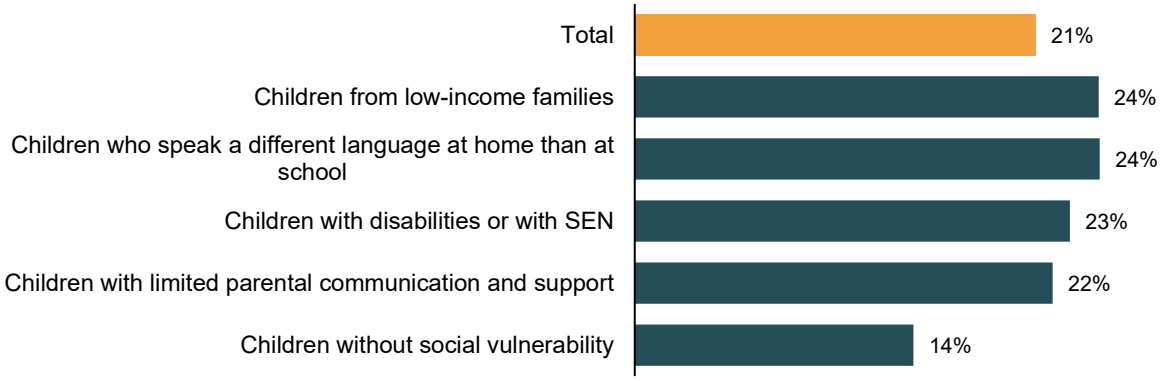
Cross-cutting risks are risks related to content, contact, conduct, and contract and have multiple manifestations across different dimensions of a child's development. These include online risks that are linked to privacy, physical or mental health, inequalities, or discrimination. For example, internet abuse leads to addiction that could affect health and well-being.

Research reveals diverse cross-cutting risks reported by children, parents, and specialists. In particular, the risks relating to data privacy and its impact on health and social well-being were emphasized.

Data Privacy

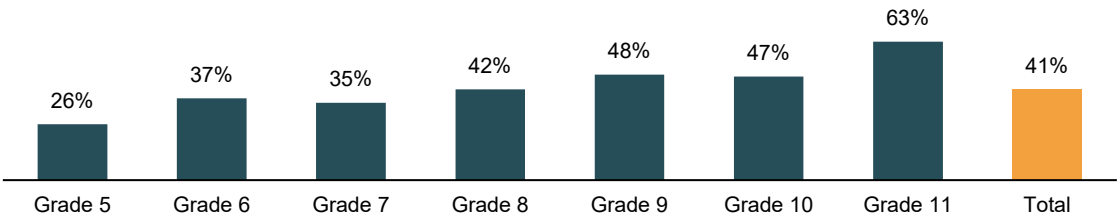
Research data shows that 21% of 1,312 children (93% of the sample) with a social media account have publicly displayed their date and year of birth**.** The share of children making this information available to the public increases with school grade, from 16% of 5th grade students to 33% of 11th grade students. At the same time, there are differences depending on the vulnerability category of children (Figure 16). Additionally, children from the municipality of Chisinau are more informed about the use of personal data in the digital environment, and 16% display their date and year of birth on the social network, compared to those from the Southern region (23%), Northern region (24%), and Center region (26%).

Figure 16. Children whose birth date and year are publicly displayed on social networks, by vulnerability category (%)



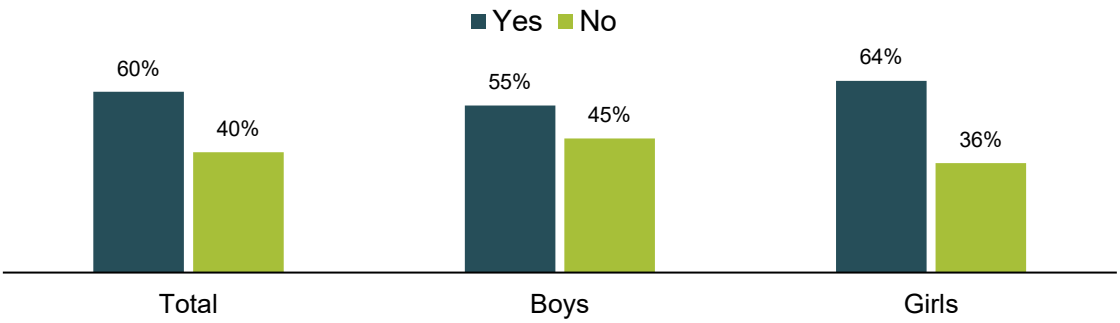
Forty-one percent of children revealed that the date and year of birth posted on social media are real**.** The number of children posting true information increases from 26% in 5th grade students to 63% in 11th grade students (Figure 17). No significant differences depend on the social vulnerability category but rather on geographical region. Only 33% of children from the municipality of Chisinau have posted on social media true information about the date and year of birth, compared to those from the Southern region (49%), Northern region (46%), and Center region (47%).

Figure 17. Public display by children of their birth date and year on social networks, by school grade level (%)



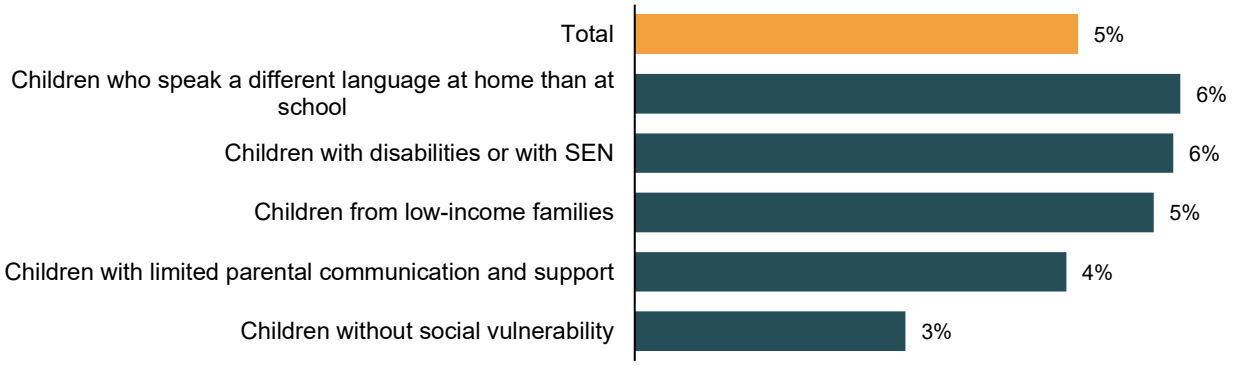
In 60% of cases, a child's social account shows their real name and surname**.** Fifty-five percent of boys post their real names and surnames, compared to 64% of girls (Figure 18). Children from lower grades (55% of 5th graders) post their real names to a lesser extent compared with older students (75% of 11th graders). Only 45% of children from the municipality of Chisinau have posted their real name and surname, compared to those from the Southern region (63%), Northern region (71%), and Center region (73%).

Figure 18. Children's real names on social networks, by gender (%)



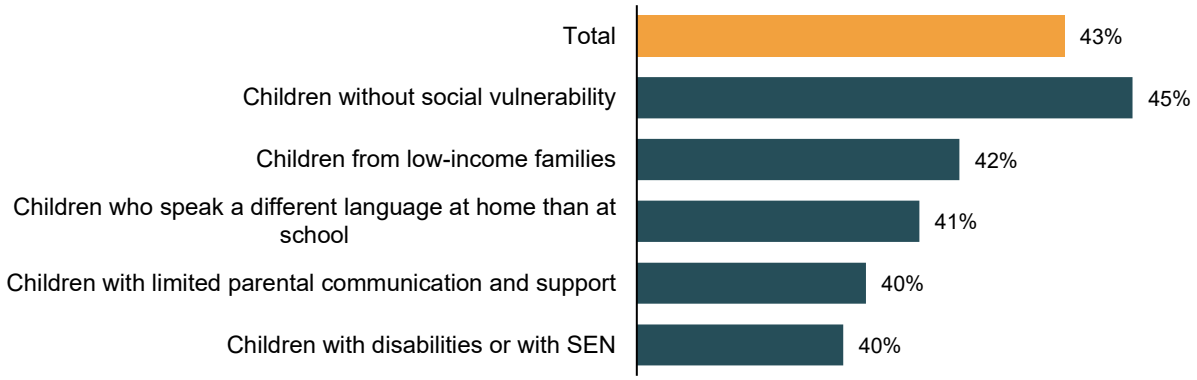
Five percent of children posted their contact information on social media (such as home address or phone number). Another 9% of children do not know if this information is available. Significant differences relate to gender, social vulnerability, school grade, age, and geographical region. The share of boys (6%) for whom this is true is higher than that of girls (3%). A greater proportion of children from social vulnerability categories publicly displayed their contact information (5% to 6%) than those from non-vulnerable families (3%) (Figure 19). Younger children (8%) displayed their home addresses and real phone numbers more than older students (3%). At the same time, fewer children from Chisinau municipality (3%) posted their real information, compared to those from other regions (5% to 7%).

Figure 19. Sharing of real contact information online, depending on the vulnerability category (%)



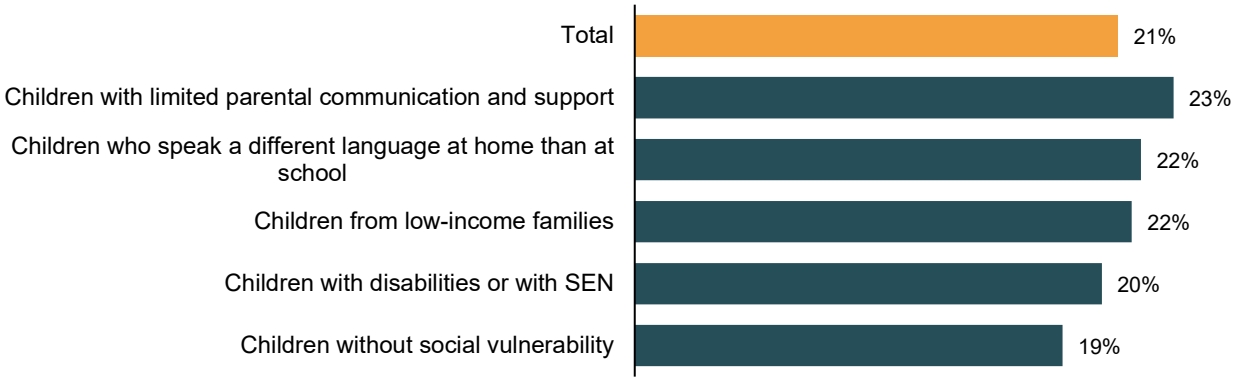
In 43% of cases, a child's social media account has a photo that clearly shows the face of the owner. Significant differences in this regard relate to gender, school grade, age, geographical region, and social vulnerability. This is more typical for girls (53%) than boys (31%). Children without social vulnerability post photos showing their faces in a greater proportion than those from vulnerable categories (Figure 20). Fewer younger students (40% of 5th graders) have a picture showing their face on social media, compared to older students (59% of 11th graders). Fewer children from Chisinau municipality (33%) have such a photo compared with those from other regions (48% from the Southern region, 54% from the Northern region, and 47% from the Center region).

Figure 20. Presence of a real photo on social media account showing the face, depending on the vulnerability category (%)



Information about the school that they attend is made public on social networks by 21% of the respondents. A smaller proportion of girls (18%) post such information than boys (25%). Once students get older, the share of children posting information about their educational institution decreases from 27% in 5th grade students to 15% in 11th grade students. Twenty-three percent of children with limited parental communication and support have publicly displayed information about the institution they attend (Figure 21). Only 15% of children from the municipality of Chisinau have publicly displayed information about the educational institution, compared to those from the Southern region (17%), Northern region (21%), and Center region (33%).

Figure 21. Public display on social networks of information about the educational institution of children, depending on the social vulnerability category (%)



Health and Well-Being

Nineteen percent of children reported that the internet negatively affects their school performance either very often, often, or sometimes. Children from the four socially vulnerable categories more frequently face such challenges compared to those without vulnerability (Table 15).

Table 15. Situation when grades in school went down due to the time spent online (%)

Vulnerability Category	Never	Rarely	Sometimes	Often	Very often
Total	**56**	**25**	**12**	**5**	**2**
Children without social vulnerability	65	22	8	5	0
Children from low-income families	47	29	16	5	3
Children with limited parental communication and support	53	26	13	6	2
Children with disabilities or with SEN	50	25	15	7	3
Children who speak a different language at home than at school	52	26	15	4	3

The internet affects the nutrition and sleep hours of 13% of children either very often, often, or sometimes. Between 14% and 19% of children from vulnerable categories reported that the internet affected their nutrition and sleep compared with 8% of non-vulnerable children (Table 16). Moreover, once the school grade increases, the percentage of children whose nutrition and sleep are affected due to excessive internet use also increases from 10% in the 5th grade to 23% in the 11th grade.

Table 16. Situation when children didn't eat or sleep because of the time spent online (%)

Vulnerability Category	Never	Rarely	Sometimes	Often	Very often
Total	**63**	**24**	**9**	**3**	**1**
Children without social vulnerability	72	20	6	2	0
Children from low-income families	49	30	15	4	2
Children with limited parental communication and support	58	27	11	3	1
Children with disabilities or with SEN	57	25	12	3	2
Children who speak a different language at home than at school	59	25	13	3	1

Thirteen percent of children reported that the internet leads to conflicts with family or friends either very often, often, or sometimes. This situation is also more characteristic of children from vulnerable categories, in particular children with disabilities or SEN and children from low-income families (Table 17).

Table 17. Situation when children had conflicts with the family or friends due to the time spent online (%)

Vulnerability Category	Never	Rarely	Sometimes	Often	Very often
Total	**64**	**23**	**10**	**2**	**1**
Children without social vulnerability	72	19	7	1	1
Children from low-income families	56	28	12	3	1
Children with limited parental communication and support	60	26	10	3	1
Children with disabilities or with SEN	59	24	13	3	1

Vulnerability Category	Never	Rarely	Sometimes	Often	Very often
Children who speak a different language at home than at school	62	23	11	3	1

About 1 in 10 children felt left out of their friend group because they do not use social media as much as their friends. These risks depend on a child's school grade and vulnerability category. For example, 15% of 5th grade students felt left out compared to 6% of 11th grade students. Differences linked to the vulnerability category are apparent as well (Table 18).

Table 18. Situation when children felt left out of their friend group because they don't use internet/social media as much as the group does (%)

Vulnerability Category	Never	Rarely	Sometimes	Often	Very often
Total	**79**	**12**	**6**	**2**	**1**
Children without social vulnerability	87	10	3	0	0
Children from low-income families	71	16	8	3	2
Children with limited parental communication and support	78	12	6	3	1
Children with disabilities or with SEN	74	14	7	4	1
Children who speak a different language at home than at school	76	12	7	4	1

It is essential to highlight that parents more frequently perceive cross-cutting risks of the digital environment compared to other types of risk. Within the FGDs, parents revealed the risks affecting children's physical and mental health. One parent said, "*She is hypnotized by the phone. Her life is in the phone; she does not notice when is time to eat, to do her homework, to clean her room, to arrange clothes. She cannot communicate with others"* (FGD_1_U). Parents emphasized children's addiction to the phone from a young age, with one saying: "*I am a nursery teacher in the kindergarten. The child is not even three years old and is already addicted. Mother brought him to the kindergarten, took his phone, and the child had a tantrum as he wanted his phone back"* (FGD_1_U).

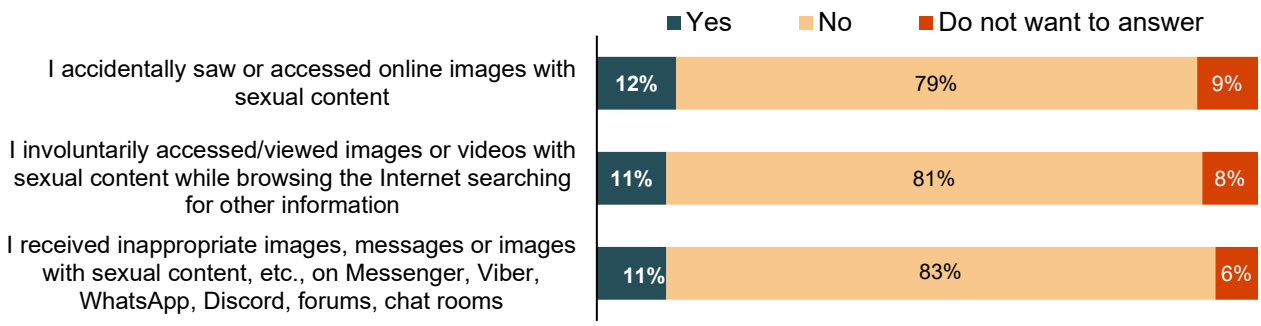
4.4. Content Risks

Content risk means that a child engages with or is exposed to unwanted and inappropriate content that is potentially harmful and age inappropriate. This may include sexually explicit images, pornographic and violent content, particular forms of advertising, racist and discriminatory content, violent and hate speech, and websites encouraging unhealthy behaviors, such as self-harm, suicide, and anorexia.

Exposure to Sexually Explicit Content

Children face various content risks; in particular, they are exposed to sexualized content. Twelve percent of children participating in the research accidentally saw or accessed online images with sexual content, 11% involuntarily accessed or viewed videos with sexual content while browsing the internet for other information, and 11% received inappropriate images or messages with sexual content via Messenger, Viber, WhatsApp, Discord, forums, or chatrooms (Figure 22).

Figure 22. Presence of content risks in the last 3 months (%)



There are significant differences in online content risks by gender and social vulnerability. The risks related to content on the internet affect more vulnerable categories: 10% to 17% accidentally viewed or accessed sexual content online (compared to 8% of the non-vulnerable), 12% to 14% involuntary watched videos or saw photos (compared to 6% of the non-vulnerable), and 11% to 14% received inappropriate photos, sexually explicit messages, or images (compared to 7% of the non-vulnerable) (Table 19). Moreover, the risk of viewing sexualized content increases with a child's school grade. For example, in the 5th grade, 8% of children saw or accessed such images, while in the 11th grade, 17% did.

Table 19. Content risks according to children's gender and social vulnerability (%)

Category	I accidentally saw or accessed online images with sexual content	I involuntarily accessed/viewed images or videos with sexual content while browsing the internet searching for other information	I received inappropriate images, messages or images with sexual content, etc., on Messenger, Viber, WhatsApp, Discord, forums, chat rooms
Total	**12**	**11**	**11**
Boys	15	11	13
Girls	9	10	9
Grade 5	8	11	9
Grade 6	7	8	11
Grade 7	18	11	17
Grade 8	17	15	14
Grade 9	15	20	16
Grade 10	18	18	18
Grade 11	17	17	15
Children without social vulnerability	8	6	7
Children from low-income families	17	14	14
Children with limited parental	15	14	13

Category	I accidentally saw or accessed online images with sexual content	I involuntarily accessed/viewed images or videos with sexual content while browsing the internet searching for other information	I received inappropriate images, messages or images with sexual content, etc., on Messenger, Viber, WhatsApp, Discord, forums, chat rooms
communication and support			
Children with disabilities or with SEN	17	13	13
Children who speak a different language at home than at school	10	12	11

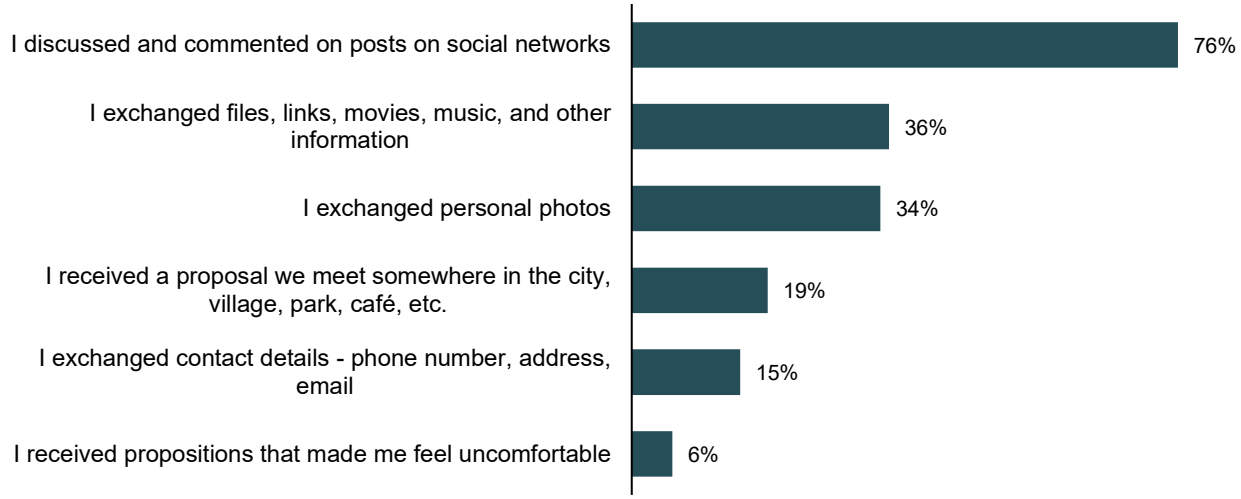
4.5. Contact Risks

Contact risks refer to situations where a child experiences or engages in risky contacts, such as communication with an adult seeking contact or requesting sexually explicit images of the child, communication with people who try to radicalize the child, or communication with people who persuade them to engage in unhealthy and dangerous behaviors. This can be related to harassment (including sexual harassment), stalking, sexual grooming, sextortion, or the generation and sharing of child sexual abuse material.

Activities with a Person Known Only Online

Children engage in various activities with people known only online. This leads to risks and potential consequences that could appear in the future because 34% shared personal photos; about 19% received proposals to meet somewhere in the city/village, park, or other locations; and 15% exchanged contact details (Figure 23). Six percent of children received propositions that made them feel uncomfortable.

Figure 23. Activities of children with a person known only online (%)

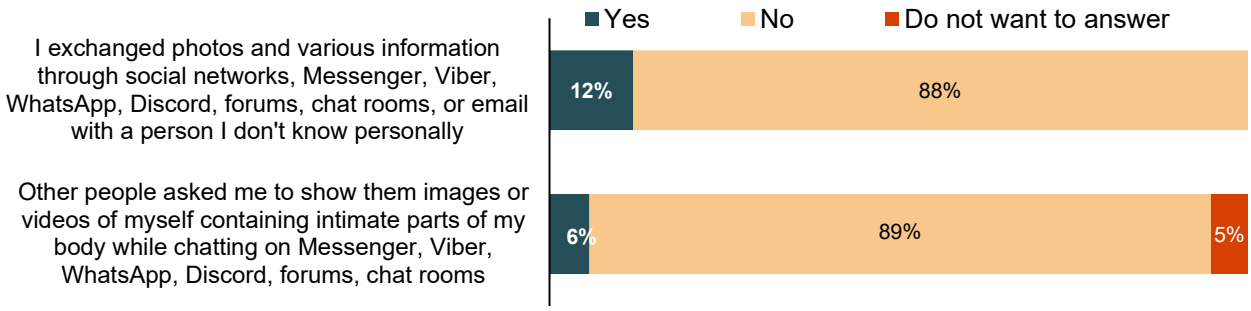


Note: 162 children (12% of the total number of child respondents) revealed that during the last 3 months they discussed and shared photos and information on social networks, Messenger, Viber, WhatsApp, Discord, forums, or chatrooms.

Asking for Intimate Personal Images

Children face various online risks related to being contacted by unknown adults. Twelve percent of children exchanged photos and information on social media, Messenger, Viber, WhatsApp, Discord, forums, chat rooms, or email with someone they do not know in person. One in six children were asked to send personal images or videos containing intimate parts of their body to other people online when communicating via Messenger, Viber, WhatsApp, Discord, forums, or chat within the last three months (Figure 24).

Figure 24. Presence of contact risks for children in the last 3 months (%)



The collected data shows significant differences regarding contact risks in the online environment depending on categories of social vulnerability. There is a more probable risk of harmful contact by exchanging photos and various information through social networks with a person known offline in the case of children from vulnerable categories, who do this in the proportion of 12% to 16%, compared with only 6% of non-vulnerable children. Also, 6% to 10% of children from vulnerability categories were asked to show images or videos containing intimate parts of their body, compared with 2% of non-vulnerable children. (Table 20).

Table 20. Contact risks according to categories of social vulnerability (%)

Vulnerability Category	I exchanged photos and various information through social networks, Messenger, Viber, WhatsApp, Discord, forums, chat rooms, or email with a person I don't know personally	Other people asked me to show them images or videos of myself containing intimate parts of my body while chatting on Messenger, Viber, WhatsApp, Discord, forums, chat rooms
Total	**12**	**6**
Children without social vulnerability	6	2
Children from low-income families	16	9
Children with limited parental communication and support	13	8
Children with disabilities or with SEN	16	10
Children who speak a different language at home than at school	12	6

Parents highlighted some circumstances related to contact risks with unknown people online during the FGDs. One parent said, *"Child gave the home address and phone number to a stranger. He asked her when the parents are home, when they are not. Her luck was that in the last moment, when she gave her home address, she felt a spark and told her mother."* (FGD_2_R). Still, a few parents revealed from their own experience about grave consequences of contact risks,

> *We recently learnt about a very tragic family situation due to social networks. The eight-year-old nephew shot himself. He had access to social media. The father and mother did not even know whom the child was communicating with. He died because of the group, as he was making videos and posting them. He was influenced as the child's mind at eight years old is not so stable (FGD_2_R).*

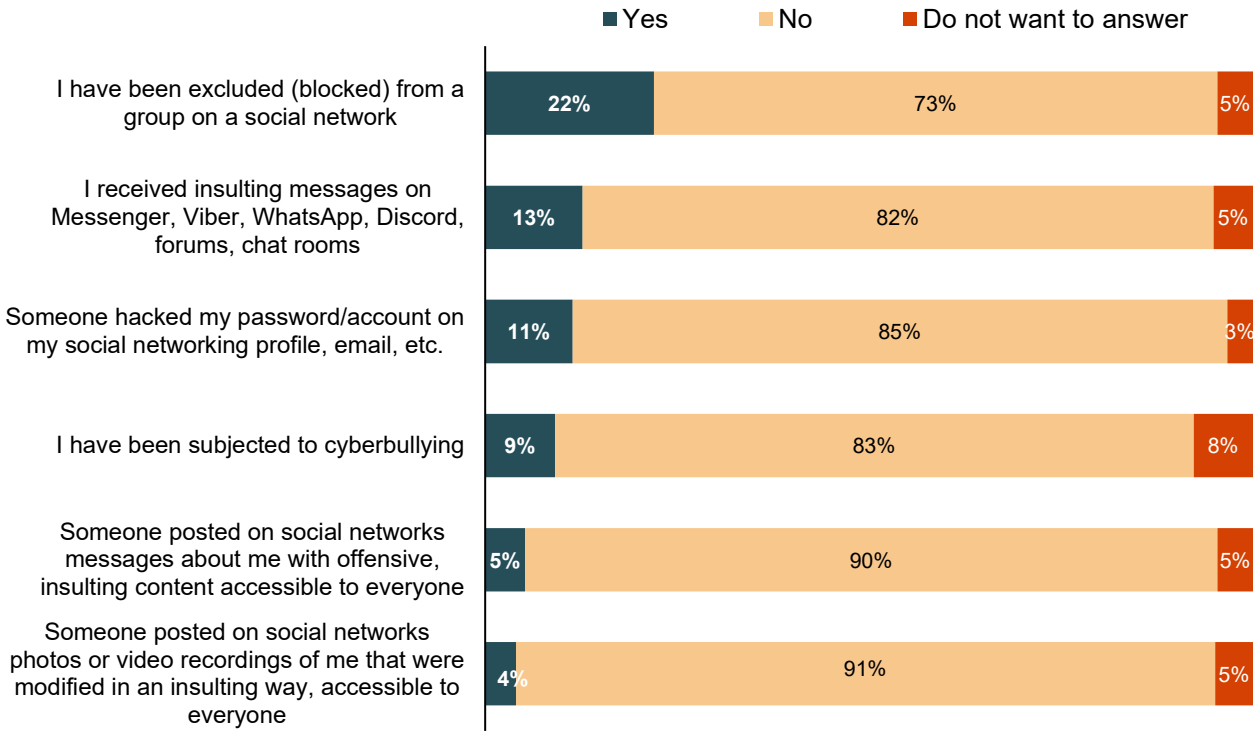
4.6. Conduct Risks

Conduct risks refer to a child's behavior that contributes to risky content or conduct. These risks include writing or generating racist hate speech about other children or posting and sharing sexual images, including self-produced material. In this case, other children witness, participate in, or become victims of potentially harmful conduct, such as harassment, hateful peer activity, trolling, sexual messages, pressures, and harassment, or are exposed to potentially harmful user communities (for example, self-harm or eating disorders). Typically, the conduct risks arise from interactions between peers, although not necessarily of equal status.

Online Risks from Peers

Children experience various conduct risks from peers. Twenty-two percent of children participating in the research were blocked by others on social networks. Thirteen percent of children received insulting messages. Nine percent of children were subject to cyberbullying, and 11% had their social media accounts hacked. Five percent of children experienced situations when someone posted offensive, insulting messages accessible to everyone or had photos or video recordings modified in an insulting way on social networks (Figure 25).

Figure 25. Presence of conduct risks in the last 3 months (%)



Research outcomes show significant differences regarding conduct risks from peers in the online environment depending on categories of social vulnerability (Table 21). Twenty-nine percent of children with disabilities or SEN were excluded from social media, and 19% received offensive messages. Additionally, 15% of children from low-income families face social media hacking, 13% were subject to cyberbullying, 9% experienced hate speech from peers on social media, and 7% experienced situations when peers posted photos and videos modified in an insulting way.

Table 21. Conduct risks for children according to categories of social vulnerability (%)

Vulnerability Category	I have been excluded (blocked) from a group on a social network	I received insulting messages on Messenger, Viber, WhatsApp, Discord, forums, chat rooms	Someone hacked my password/account on my social networking profile, email, etc.	I have been subjected to cyberbullying	Someone posted on social networks messages about me with offensive, insulting content accessible to everyone	Someone posted on social networks photos or video recordings of me that were modified in an insulting way, accessible to everyone
Total	**22**	**13**	**11**	**9**	**5**	**4**
Children without social vulnerability	14	7	7	5	2	2
Children from low-income families	28	18	15	13	9	7
Children with limited parental communication and support	24	13	12	11	7	6
Children with disabilities or with SEN	29	19	13	11	8	5
Children who speak a different language at home than at school	22	14	12	10	6	4

Parents pointed out various online risk circumstances from peers. They reported on:

- Threatening messages on the phone from friends: "*I was checking with whom he was talking, and I saw some threatening messages from friends. I am afraid as a parent to speak"* (FGD_1_U)
- Posting compromising videos on social networks: "*Children are given school group projects, and several girls met at one person's home, and after finishing the project, they decided to take clothes off and make a video. An envious person from the group posted the videos on social networks when going home."* (FGD_2_R)
- Posting sexual videos on social networks: ”…*a 17-year-old boy who has a girlfriend secretly filming her. They broke up, and he posted those erotic videos."* (FGD_2_R)

4.7. Contract Risks

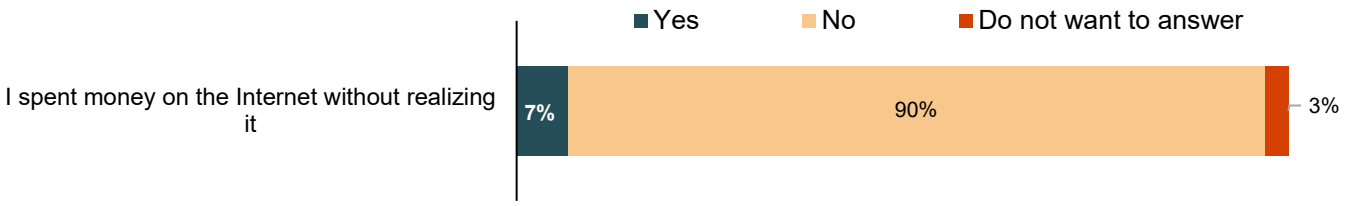
Contract risks are when the child “accepts” (including unintentionally, involuntarily, or unknowingly) the terms and conditions of a commercial provider of digital products and services. The child is party to and exploited by potentially harmful contracts or commercial interests (such as gambling, exploitative interests, or age-inappropriate marketing). This can be mediated by the automated (algorithmic)

processing of data. This includes risks related to ill-designed or insecure digital services that enable identity theft, fraud, or scams. It also includes contracts made between other parties involving a child (such as child trafficking, sexual streaming, and abuse). Such contact may be unfair or exploitative to the child and pose security or privacy risks that they have little control over or means to escape. Related risks arise because of the data processed by the public sector and various organizations and through private partnerships. Children cannot understand what they are signing up for when they install apps or log on to the site. Services and obligations that are designed for adults must be age-limited so that children cannot sign up for them without parents'/caregivers' permission. While online, children also risk spending money without parents'/caregivers' permission and having their data collected.

Children Spending Money Online

Contract risks are more specific and less acknowledged by children and parents. It was revealed that 7% of children within the last three months spent money online unknowingly (Figure 26).

Figure 26. Children's spending of money online unknowingly in the last 3 months (%)



These risks were experienced by a greater proportion of boys (8%) compared to girls (5%). Such situations are faced by a large proportion of children from low-income families (9%) and children with disabilities or SEN (9%) (Table 22).

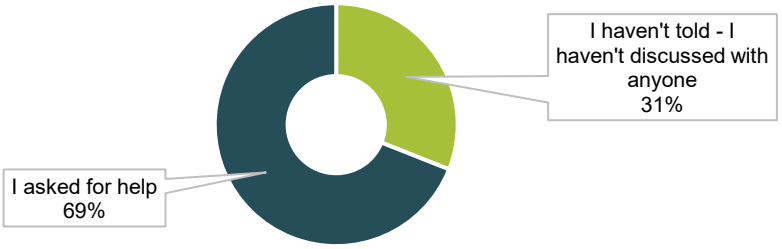
Table 22. Situation when children spent money online unknowingly (%)

Category	Yes	No	Do not want to answer
Total	**7**	**90**	**3**
Boys	8	88	4
Girls	5	93	2
Children without social vulnerability	3	92	5
Children from low-income families	9	88	3
Children with limited parental communication and support	6	91	3
Children with disabilities or with SEN	9	88	3
Children who speak a different language at home than at school	8	88	4

4.8. Asking for Help When Facing Digital Risks

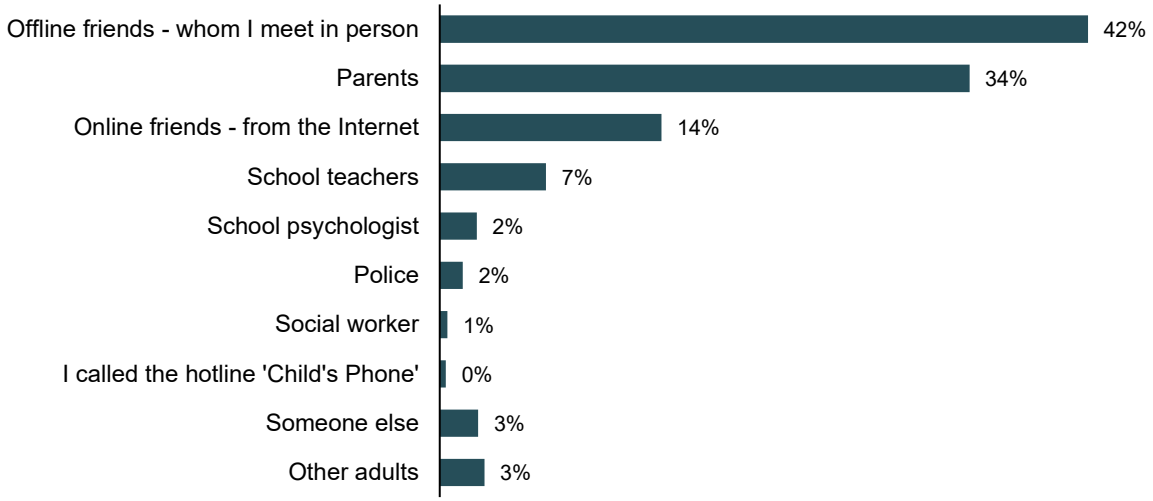
Only 69% of children seek help when they face challenges and negative online experiences, and 31% prefer not to discuss such experiences with anyone (Figure 27). Most of those who do not seek help are boys (36%) and children who speak a different language at home than at school (39%).

Figure 27. Discussing the problems children encounter online (%)



Children discuss problems they face online to a greater extent with real-life friends and parents (Figure 28). A large proportion of girls discuss online issues with real-life friends (45%). The same happens in the case of 10th grade students (50%) and 11th grade students (54%). Also, a larger proportion of girls discuss online issues with their parents (39%), as do the children without social vulnerability (40%) and younger students (45% of 5th grade students). Children from social vulnerability categories, such as children with disabilities or SEN (18%), children from low-income families (17%), and children with limited parental communication and support (16%), reported discussing their negative experiences with online friends. Such experiences are discussed with teachers by children without social vulnerability (11%) and younger students (11% of 5th grade students). The research data about cross-cutting, content, contact, conduct, and contract risks presented in this chapter confirm the third working hypothesis that the online behaviors of vulnerable children and their response to online risk situations are influenced by the specific characteristics of their vulnerability (low income, lack of parental care, disabilities or SEN, etc.).

Figure 28. People with whom children discussed problems encountered online (%)



V. Protective Factors and Risk Factors in the Digital Environment

Protective factors are individual, inherited characteristics or family, school, or community conditions that help children successfully deal with online challenges and neutralize risk factors. Risk factors are individual characteristics, family, school, or community conditions that increase the likelihood that a child will not seek help and will be further exposed to online risk.

IDIs held with the representatives of educational institutions, PAS, child protection services, specialized services for children affected by online abuse, and prosecutors and investigation officers in charge of preventing and combating online risks in children targeted the identification of protective factors and risk factors in children's safe browsing in the digital environment. In this regard, the research team relied on the Ecological Model of Human Development suggested by Urie Bronfenbrenner (1979).

5.1. Individual Level

Specialists participating in the research underlined that the main protective factors for children's safety in the digital environment involve informing children about the benefits and risks of digital engagement, their awareness of the consequences of their online behaviors, and the development of critical thinking and self-confidence, including seeking help (Table 23).

Table 23. Protective factors and risk factors at the individual level

Protective factors	Risk factors
Self-confidence and seeking help	Disability or SEN
Being informed and aware of risks and consequences of online behavior	Low self-esteem
Critical thinking	Lack of self-confidence
Seeking help	Isolated, introverted
	Extroverts, who have no limits and communicate with too many people
	Immaturity and difficulty in distinguishing between reality and the game

5.2. Family Level

Parents play a crucial role in their children's education, including informing them about the risks in the digital environment. Face-to-face ongoing communication between parents and children and monitoring their online conduct represents significant protective factors against online risks. A dysfunctional family environment, as well as emotional issues between parents and a lack of positive parenting practices, constitute risk factors in the opinion of the interviewed professionals and experts (Table 24).

Table 24. Protective factors and risk factors at the family level

Protective factors	Risk factors
Open communication, trustful relationships, good communication between parents and children, encouraging children	Dysfunctional family (excessive alcohol consumption, drug addiction, conflicts, violence etc.)
Effective and continuous communication	Lack of parental care, including the lack of monitoring and setting of reasonable time spent online
Parents' education and training, including their digital skills	Lack of parents' communication skills with children, ineffective communication
Monitoring child's behavior in the digital environment and setting reasonable limits for children regarding their online activities	Uninformed parents that are unaware of risks and trauma of the online abuse
	Lack of affection, attachment between parents and children
	Emotional issues in the family (single parent families, divorced families, families with one parent or both parents working abroad, etc.)
	Internet-addicted parents
	Lack of individual extracurricular activities or being together with the parents

5.3. Friend Group Level

High-value friends, knowledge, and awareness of online risks by a friend group and open, face-to-face communication are essential factors in ensuring children's safety in the digital environment. Among the risk factors at this level are a lack of genuine friends and online searches. Consequently, peer-to-peer interaction about challenges faced in the online environment should be addressed by nonprofit organizations as well as by educational institutions.

Table 25. Protective factors and risk factors at the level of friend group

Protective factors	Risk factors
Knowledge and risk awareness within the friend group (friends-resource)	Lack of reliable friends
Peer-to-peer information	Friends that are not informed and aware of online risks
The positive values (*"human values", "high values"*) within the friend group	Attitudes encouraging risky behavior, including poor perception of the risk, danger
	Member of groups, online chats that encourage aggressive conduct or accept it as normal

5.4. Educational Institutions Level

Children spend about 6–8 hours at school every day, suggesting the importance of this setting in ensuring children's safety in the digital environment. School has an even more crucial role in the case of vulnerable children who lack parental support (Table 26). Interviewees from the education sector, including PAS

representatives, highlighted that implementing the *Online children' students safety standards*[12] is essential in protecting children against online risks. Specialists from social protection also underlined the need to integrate a school subject on sexual education.

Table 26. Protective factors and risk factors at the level of the educational institution

Protective factors	Risk factors
Educational staff's knowledge and training on online safety and protection	Limited teacher training and lack of knowledge about risks
Knowledge of relevant cases, typical to children in the digital environment	Teacher's reticence to engage in activities related to the improvement of knowledge about online risks and the protection of children
Curricular and extracurricular activities on online safety	Ineffective measures to prevent and combat cyberbullying causing the escalation of these issues online
School internet safety	Teachers who encourage punitive discipline making children afraid to report and discuss online safety
Parents' engagement in school activities, including their training of online safety	Internet security problems in schools
Projects with other educational institutions from the country or abroad (for example "Internet heroes")	Emphasis on school performance rather than children's education
Existence of reliable teachers at school for children	Lack of school psychologists in some educational institutions
Monitoring of changes in children's behavior	Lack of sexual education in schools to make children understand how and when they have to seek help from parents and specialists
Providing some techniques or methods of selecting information from the digital environment	

5.5. Community Level

At the community level, there are also resources that can become important protective factors (Table 27). The respondents emphasized the need to organize more social activities at the community level and the engagement, in particular, of children from vulnerable categories in these activities. At the same time, specialists operating in the community required training about online risks for children and the identification, intervention, and immediate assistance in such cases. The need for more information campaigns to sensitize actors was emphasized.

Table 27. Protective factors and risk factors at the community level

Protective factors	Risk factors
Ongoing training of children, parents, specialists regarding the benefits and risks of the digital environment	Lack of information and education about online safety of children, parents, professionals
Knowledge of concrete situations that children face in the digital environment	Lack of awareness of the risks and trauma associated with online abuse/crimes
Organizations providing information to children,	Tolerance of online abuse/crimes and failure to report

12 Order no. 985 of 07.10.2022 on the approval and implementation of Online children/students' safety standards.

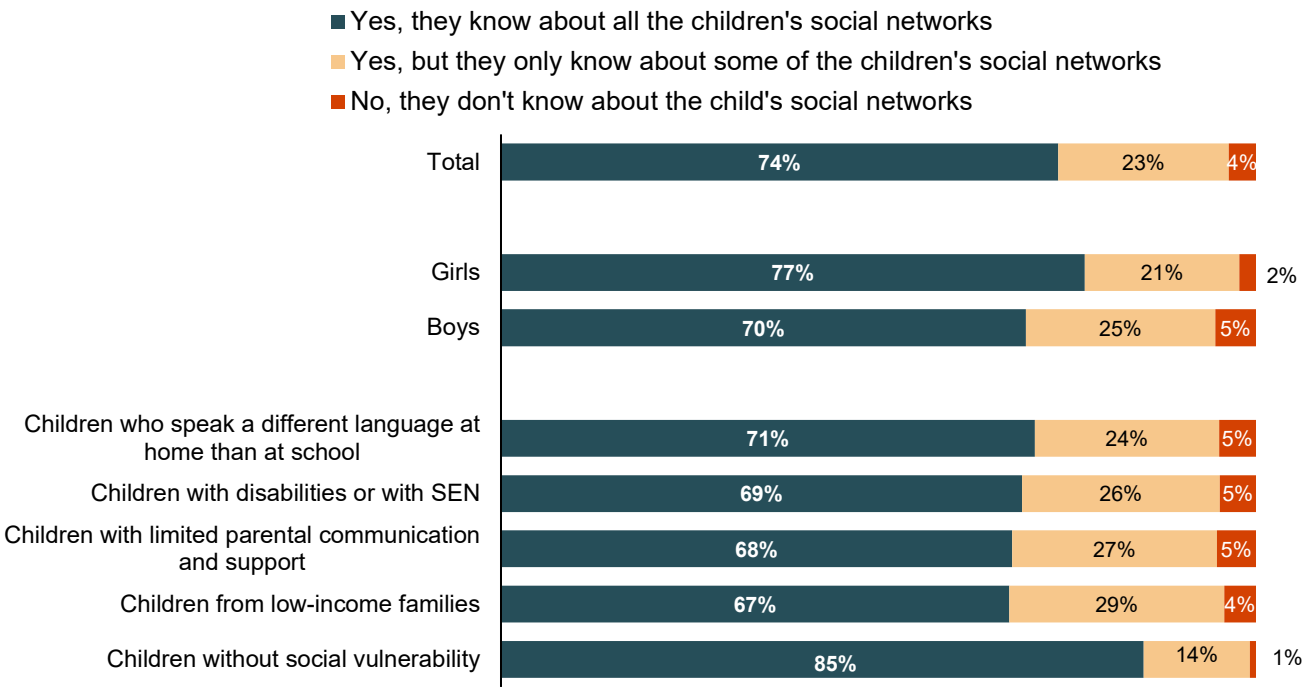
Protective factors	Risk factors
educational staff, parents about the online safety	such cases
Extracurricular activities about online safety	Small number of organizations addressing this field
Various extracurricular activities and opportunities for children from vulnerable families	Shortage of efficient awareness raising campaigns, focused on the capacity building of children, parents, educational staff
	Risky behaviors encouraged by bloggers, vloggers or influencers, on social media
	Lack of awareness about the digital risks of parents, police officers, educational staff, social workers and of institutions providing support

VI. Measures Taken to Ensure Children's Safety in the Digital Environment

6.1. Actions Taken by Parents

Seventy-four percent of children participating in the research revealed that their parents/caregivers know about their social media accounts, 23% are partially acquainted, and 4% do not know anything. More informed are the parents/caregivers of girls and children without social vulnerability (Figure 29). A few parents participating in FGDs pointed out that they try to supervise and control their children's accounts on social media: "*One day, I got angry and deleted her Facebook, Instagram, and TikTok accounts, and I did not even know she has so many*" (FGD_1_U). Still, they admit that children are "*more skillful*", *and* "*more up to date.*" (FGD_1_U) Consequently, they try to identify and prevent particular risks, but not always successfully: "*I removed all children's social media accounts, but they made new ones and disguised them so I cannot find"* (FGD_2_R).

Figure 29. Parents'/caregivers' awareness of children's activities on social networks, by child's gender and vulnerability categories (%)



Parents have not restricted 55% of children from internet surfing within the last few months. Restricted internet access from parents is more typical for students in 5th to 9th grades, where 16% to 22% of parents have limited access sometimes, often, *or* very often. Only 8–9% of parents, in the case of children in 10th to 11th grades, set restrictions (Table 28).

Table 28. Situations when parents do not allow children to use the internet, by school grade level (%)

Grade	Never	Rarely	Sometimes	Often	Very often
Total	**55**	**27**	**13**	**3**	**2**
Grade 5	44	31	16	5	4

Grade	Never	Rarely	Sometimes	Often	Very often
Grade 6	55	26	13	4	2
Grade 7	46	32	15	6	1
Grade 8	59	25	14	1	1
Grade 9	58	24	14	2	2
Grade 10	62	29	7	1	1
Grade 11	75	17	5	2	1

The FGDs with parents also looked at their understanding of children's online safety, including the challenges and risks of children in the online environment. Parents emphasized that they require training in this regard, although they have been informed during particular school meetings or given information via the Viber parent group. Most parents have limited knowledge: *"We hear what is happening to other children on the news"* (FGD_2_R), and very few look for information on specialized sites. Parents perceive online safety in terms of actions they allow or prohibit their children to do online (Table 29).

Table 29. Children's online safety according to parents

Actions allowed for children	Actions prohibited for children
"To have friends online only from class or school" *"To watch only age-appropriate movies"*	*"To provide personal data – name, phone number etc."* *"To communicate with strangers, to accept their friendship requests"* *"To view videos and ads encouraging bad things – junk affecting behavior or health"* *"To access unsafe sites"* *"To post personal photos"* *"To play online games with unknown people"* *"To film each other and post other people's photos"*

Parents shared a few successful practices in monitoring and controlling children online. They reported on:

- Creating a relationship of trust between the parent/parents and the child: "*The best solution is talking to your child and building trustful relationships."* (FGD_2_R)
- Discussing online safety issues as a family: "*We are just discussing what is good and wrong to do online. I bring her bad examples.*" (FGD_1_U)
- Installing parental controls and limiting the time spent online: "*I set up parental control. He has the right to stay 3 hours online daily, and I see what he downloads.*" (FGD_2_R)
- Limiting access to the phone during the night: "*The phone is turned off at 10 pm and turned on at 7:00 am.*" (FGD_1_U)

However, among these successful practices, those limiting children's privacy were also recommended. One parent said, "*I check all messages..."* (FGD_2_R), and another said, *"I ask him to speak loudly when he communicates with his friends online. This way, I am familiar with whom he is talking to and what they are talking about*" (FGD_1_U). These practices point to the need for better information for parents regarding the monitoring and control of children's activities in the digital environment.

Some parents, however, resort to shutting down the internet and taking away their mobile phones, but they admit that this does not help. Parents underlined that *"children are hackers"* (FGD_1_U)*;* consequently, some children were amused when their parents set up parental controls.

A potential risk detected in parents refers to their belief that although the digital environment has particular risks, their children could learn from their mistakes in the digital environment: "*They will learn from a small mistake, then a bigger one, little by little"* (FGD_2_R).

Some specialists pointed out that limiting children's access to the digital environment by some parents does not mean reducing the risks. Children find access anyway, while the risks remain, making children "*fear"* seeking help. Moreover, a few specialists emphasized the need for parents to understand that limiting internet access represents limiting children's development and opportunities for social integration.

In the meantime, specialists that were interviewed believe that children and parents minimize or ignore the risks they are exposed to in the digital environment, thinking that everything is ok if there is no physical evidence. One specialist said, *"Naive adults think that physical or sexual abuse did not occur and the child is safe. The child is emotionally devastated, although physically is ok and they hope it will pass"* (III_2); another said, "*Adults are not even interested in understanding what the child is going through, what made him end up in this ugly situation in the online environment, what are the consequences* (III_1). Thus, severe cases are brought to the authorities' attention. They underlined the importance of being aware of the emotional consequences of online abuse and collaboration with child protection authorities.

6.2. Actions Taken by Educational Staff

IDIs with educational staff revealed that beginning with the 2022–2023 school year, the MoER's *Online children/students' safety standards*[13] were implemented in schools. They are focused on critical areas, such as school management, educational staff training, availability of particular policies and procedures, parent engagement, online safety education, and safe technologies and infrastructure. The standards aim to support the education system in the development and implementation of measures to secure students' safety online by committing to online safety at the local level, empowering the academic environment to communicate positively online with no risk to the security and well-being of children. They also aim to ensure minimum actions that education institutions should take to strengthen efforts in promoting online safety, creating a safe and secure environment for children/students, and ongoing training for the educational staff, parents, and children/students.

Interviews showed that educational institutions are conducting various activities such as providing information to students according to the curriculum (e.g., discussing the subject during class hours, personal development classes, informatics, media education, as well as during other classes, etc.), organizing extracurricular activities, and engaging students in the dissemination of the subject. Educational institutions also foster online safety by conducting annual activities in the school community in the context of Safer Internet Day and Cybersecurity Awareness Month. Projects are implemented, and contests are carried out on this subject within these activities. Students make videos and interactive

13 Order no. 985 of 07.10.2022 on the approval and implementation of Online children/students' safety standards.

learning materials, and discussion and research workshops are held to identify the risks and raise students' awareness: "*Primary school children made a phone of recyclable materials, and we also put down the rules of online communication," "Older students made videos and presentations for their classmates" (III_8).* A few educational institutions carried out specific activities to mitigate mental health risks "*This year, we organized a digital detox day, and it was quite complicated to refrain from digital devices"* (III_8).

Certain educational institutions have established collaboration agreements with the IC La Strada for training students and teachers. They have developed guidelines to support primary and secondary education teachers. Some representatives of the law enforcement agencies dealing with such crimes, as well as representatives of mobile phone companies, also carry out information activities for students, with one interviewee saying, "*Specialists of the IC La Strada informed us, but also employees of Orange Moldova, Moldcell Moldova provided training to teachers, children, parents"* (III_8).

According to some specialists, educational institutions' efforts to ensure children's safety online are uneven and need to be streamlined. Accountability and engagement, including from specialists from other fields, are rather weak. A few specialists pointed out that teachers' understanding of the risks children can be exposed to online is limited, especially about the severe consequences of this problem: *"It is regarded as something superficial that does not affect the child,"* and *"if the child was not physically touched, then this is not abuse"* (III_1), being primarily aware of identity theft and card fraud.

The IDIs revealed several good practices. For example, teachers who benefited from the training from the IC La Strada became certified trainers in this field. They have organized the training of all teachers from the administrative-territorial unit on the implementation of *Online children/students' safety standards* and regularly carry out thematic inspections, applying various research methods, including questionnaires with children, parents, and teachers.

The interviews with specialists in the education system were instrumental in understanding how the identification and intervention in cases where children face particular risk situations online occur. Children report cases to their homeroom teachers and more rarely to the school psychologists. These cases are recorded by the Abuse, Neglect, Exploitation, and Trafficking coordinator, according to the Order of the MoER. The educational institutions that have employed school psychologists engage them together with other specialists in counseling children affected by different forms of abuse. In the absence of a school psychologist, the school administration requires support from PAS to provide counseling for the child victim and their family (except in the municipality of Chisinau, where the referral is made to other specialized services, such as www.siguronline.md, due to the shortage of specialists). Sometimes, PAS receives notifications from parents and children or petitions from hierarchical authorities such as the MoER, local education authorities (LEA), the prosecutor's office, and the police, in addition to requiring the engagement of Youth-Friendly Health Centers (YFHC) to provide long-term counseling to abused children.

PAS representatives have access to all educational institutions and collaborate with multidisciplinary teams at the educational institutions. Besides providing assistance to children affected by online abuse and their families, PAS conducts a wide range of prevention activities, such as explanation and information about risks for children and parents, information and training services for the educational staff, and methodological support for school psychologists in preventing online risk situations in children.

The interviewed specialists indicated the following challenges at educational institutions in ensuring the online safety of children: (i) insufficient training and awareness of teachers on the matter, (ii) shortage of information and resources for preventing and responding to online abuse, (iii) difficulties in securing Wi-Fi networks, and (iv) lack of school psychologists in a few institutions. Teachers, as well as PAS representatives, also emphasize the neglect and lack of monitoring of children's online activity by parents/caregivers; the weak parental education and poor communication between parents and children in general, and on online safety in particular; and the lack of parents' consent to investigate and punish perpetrators.

6.3. Actions Taken by Specialists Employed in Specialized Child Protection Services

There are few specialized services in the Republic of Moldova that provide services for children affected by online abuse and exploitation. The best known by children, parents, educational staff, and other specialists are siguronline.md (IC La Strada) and service 12plus of the National Center for the Prevention of Child Abuse (CNPAC). Children, parents, and specialists also call the Child Helpline, which receives notifications on online abuse and refers these cases to specialized service providers. The representatives of specialized services use the provisions of Law No. 140/2013, Government Decision No. 270/2014 and Guidelines on the functioning of the free phone assistance for children and the Minimum quality standards.

Siguronline.md is the specialized service of the IC La Strada, dealing with children's safety in the digital environment from Moldova. The platform provides information, advice, and support to protect children against online risks. It comprises information services for children, parents, and teachers about online safety, such as articles, tutorials, and video spots, leaflets, and podcasts for children; articles, tutorials, video spots, and leaflets for parents and articles; and tutorials, video spots, leaflets, podcasts, and learning resources for educational staff. It also comprises services related to counseling and reporting of online abuse cases via online chat and opportunities to report content/materials representing sexual abuse (since 2023). Moreover, this platform provides free psychological and legal advice to children who have experienced online abuse.

12 plus is a platform created by the CNPAC for children ages 12 and older who speak Romanian, Russian, and English languages. This platform provides children with free, confidential access to online chats with experienced psychologists. The objectives of this platform lie in preventing sexual abuse and exploitation of children and young people.

Child Helpline is a free and confidential service designed to provide counseling and psycho-emotional support to children, parents, and caregivers. The service is available 24/7 at the short number 116 111, managed by the Ministry of Labor and Social Protection and implemented by the National Center for Training, Assistance, Counseling and Education from Moldova. It aims to protect children against any form of abuse, neglect, or violation of their rights by providing immediate assistance and referral to relevant authorities. Moreover, the Child Helpline facilitates the reporting of cases of abuse and provides psycho-emotional support in crisis situations.

The representatives of these services mentioned that most cases of risks, including digital abuse, are reported by children and less often by parents/caregivers and specialists. The number of such calls is small:

In 2023 – 50 of 3,000 calls received by the Child Helpline about online abuse. (III_2)

In 2023 we had 1,048 cases of online abuse reported to the IC La Strada, fewer than in 2022 and about 5,000 allegations on abusive content/materials (95% safeguarding notifications from other countries and 5% from the Republic of Moldova). (III_3)

Currently we have five allegations of online risks and consequences and two alleged cases of online abuse at 12 plus. (III_1)

At the same time, specialists of these services reported that there are many cases of attempted suicide, blackmail, and self-harm, which can be caused by online abuse. One specialist said, *"It has to [be] investigate[d] although it is online"* (III_1). However, the specialists emphasized that the decrease in allegations does not represent the improvement of children's knowledge of online risks. This is explained by the fact that many digital platforms and social networks have become more responsive to allegations and react more promptly. For example, YouTube adapted its policies by introducing regulations related to content, while some sites established more age verification requirements for children. Moreover, the specialists emphasized that the phenomenon of online abuse is a continuously changing process, with one specialist saying, "P*erpetrators are more subtle and online abuse is more difficult to recognize"* (III_3).

The specialized services mentioned above include a database containing information on all reported cases. Siguronline.md records who reports the abuse, on what platform it occurs, age, residence environment, language spoken, form of abuse, and information to prove the case of abuse or risk. 12plus records whether the allegation is single or repeated; time, date, and location; gender; age; language spoken; relationship with the perpetrator; category of suspects; and actions taken in the case. Allegations of content abuse reported to the IC La Strada include age, gender, and information about images.

The intervention in cases of online abuse depends on the specifics of each case, but broadly it follows these steps:

1. Psychological counseling to stabilize the child's situation and obtain more details about the case in a manner that avoids re-traumatizing the child.
2. Informing the local guardianship authorities (i.e., mayor) or a social worker (depending on who is the case manager) and explaining the situation. The LEA and the territorial guardianship authorities are notified depending on the case.
3. Cases of online abuse between peers are dealt with by LEA, PAS, or local guardianship authorities. Cases of abuse from adults are referred to the Center for Combating Cybercrime, based on the Allegation Form, with data collected for investigation.

Challenges faced by specialists providing specialized social services include the fact that children can leave the chat without ending the conversation and allowing for the collection of complete information about the abuse situation. One specialist said, *"It takes much more time and effort to make a child speak out about the abuse. Children's greatest fear is that their parents will find out"* (III_3). Additionally, children do not always give their consent to specialists to intervene in cases of online abuse, and there is a lack of methods for parents/caregivers' to do more activities with their children and be able to understand them.

6.4. Actions Taken by Law Enforcement Agencies in Cases of Online Child Abuse

There are several ways the cases of online child abuse are brought to the attention of law enforcement agencies. They can be reported by institutions and people from the Republic of Moldova and notified by international institutions and organizations. Allegations of abuse in the country's territory are made by private individuals, IC La Strada, the Child Helpline, and police inspectorates, including cases identified by the representatives prosecuting cybercrimes. Although the number of such crimes reported to authorities is low, in many cases, "*Sexual abuse and exploitation faced by children took a long time"* (III_9).

Law enforcement agencies collaborate with guardianship authorities, educational institutions, and other specialized services, such as psychological counseling and legal advice, including hearings conducted under special conditions.

Challenges reported by law enforcement specialists include (i) difficulties in identifying the cases, such as when the child seeks help from parents and they advise to delete information and do not report to relevant authorities; (ii) not all police inspectorates report cases of online abuse against children to the Center for Combating Cybercrimes; (iii) there are multiple alleged cases, but sometimes the evidence cannot be collected to send the case to trial; (iv) lack of advanced tools to identify online crimes; (v) insufficient ongoing training of representatives of law enforcement agencies; and (vi) insufficient counseling to avoid job burnout in specialists investigating cases of online child abuse.

6.5. Specialists' Perceptions Regarding Measures Taken to Ensure Children's Safety in the Digital Environment

The study enabled the identification of strengths and weaknesses in measures taken by authorities to prevent and combat the risks faced by children in the digital environment (Table 30). A few specialists highlighted that there are particular gaps in the perception of online risks and crimes by some representatives of education, social protection, and police. One specialist said, *"A young man was taking photos of children naked. Parents reported to the police, but the police officer suggested them to delete the information and go home"* (III_9). A few respondents believe that authorities do not make enough efforts to ensure children's safety online, mentioning the shortage of properly-trained specialists and insufficient financial resources allotted to this field. In this context, the need for national training programs was underlined, but also the need for more community awareness-raising campaigns on this issue.

Table 30. Specialists' perceptions regarding measures taken by authorities to ensure children's safety in the digital environment

Strengths	Weaknesses
Approval by the MoER and implementation by educational institutions of *Online children/students' safety standards*	Few awareness raising and information campaigns about children's online risks
Information provided to children about online safety, including activities promoting children rights implemented by non-profit organizations	Few training classes for children, parents and specialists
Training provided to the educational staff by IC La Strada on the implementation of *Online children/students' standards*	Some parents are unaware of online risks for their children and consequences of online abuse against children
Delivery of support tools for educational staff (guidelines for primary and secondary education	Some educational institutions are not familiar with and do not implement the *Online children/students' safety*

Strengths	Weaknesses
teachers) by the IC La Strada	*standards*
Information provided to parents by teachers	Lack of awareness of risks of some teachers, including inappropriate attitude and practice related to intervention and assistance of children
Availability of guidelines regarding the use of phone and other digital resources in the educational institutions	Few non-profit organizations operating in this field
Availability of services for children, parents, teachers (www.siguronline.md, 12plus, etc.), as well as for PAS, YFHC, etc.	Services available to ”more elite” children and less known by children experiencing social vulnerability
Engagement of various actors in identifying the perpetrators and providing assistance to the child and family in cases of online abuse (educational institutions, LEA, PAS, police, specialized services)	Lack of ongoing training of the educational staff, PAS representatives, representatives of the child protection system, police officers, prosecutor’s office and law enforcement agencies
Initiation of criminal prosecution (including attempt to identify all victims) to convict perpetrators	Lack of multidisciplinary approach and intervention in preventing online risks
Collaboration with various institutions, including overseas – international organizations, to investigate and punish perpetrators	Lack of advanced technologies for case identification and fast proof management
	Unsecured internet in particular educational institutions
	Lack of information resources in Russian language for children, parents, teachers, and other specialists

Conclusion

The study findings revealed high levels of access to the internet for children from the Republic of Moldova. However, there are differences in access points and in the online behaviors, practices, and experiences of children from vulnerability categories compared to those from families without social vulnerability. Meanwhile, the data shows that children from the vulnerability categories are more likely to access mobile or public Wi-Fi, spend more time online during school days and vacations, and report more problems with eating and sleeping due to excessive online time.

Children from the vulnerability categories demonstrate a greater reliance on social networks for communication and friendship, often with people they have not met in real life. They report poor school results due to time spent online and issues related to social inclusion. Moreover, these children go to parents and school teachers as sources of information regarding online safety to a lesser extent than those children not in the vulnerability categories.

This study found that children are often exposed to potential harm linked to content, contact, conduct, and contract risks in the digital environment. The risks are higher among children in the vulnerability categories because a larger proportion of this group make their personal data, information about their educational institution, or even contact information public on social media compared to children not in the vulnerability categories. These findings suggest poor digital literacy in children experiencing one or more vulnerabilities compared to children without vulnerability.

This study confirms the general hypothesis that children who experience vulnerabilities offline are at greater risk when interacting online. This is due to a wide range of factors, according to specialists participating in IIAs: lack of reliable people in the child's circle of trust, poor knowledge about online risks, the limited capacity of specialists to identify online abuse, and a lack of multidisciplinary approaches and interventions for preventing risks in the digital environment.

IDIs with specialists and experts engaged in education, social protection, and law enforcement systems, as well as FGDs with parents, enabled the identification of strengths and weaknesses in measures taken by authorities to prevent and combat the risks facing children in the digital environment, the protective factors, and the risk factors in children's safe browsing in the digital environment. In their opinion, authorities must make more efforts to ensure children's safety online, including mitigating the shortage of appropriately-trained specialists and insufficient financial resources allotted to this field.

The authors hope that the study findings can offer the foundation for a better understanding of online risks to vulnerable children. If vulnerable children encounter problems, the level of intervention and support should be well-informed, relevant, proactive, and responsive to the possible risks that might be present. These findings could also provide crucial information that can help the authorities of the Republic of Moldova and other key actors ensure a safe and inclusive digital environment.

Not least, the study also underlines the need for further investigation of children under 10 from vulnerable groups and the integration into future surveys of children ages 15–17 who do not continue their studies after graduating from secondary education to understand their vulnerabilities better.

Recommendations

The study findings enable the submission of the **following recommendations** for central and local authorities, governmental agencies, the private sector, and educational and child protection professionals on key areas**:**

I. Ensuring the Digital Inclusion of Vulnerable Children

- Develop specific strategies for the digital inclusion of vulnerable children with limited access to digital devices and online connections to ensure equal access to development and learning opportunities in the digital environment.
- Develop capacity-building programs and information resources for specialists employed in the PAS and child protection to be able to prevent online risks and intervene in cases of online abuse, taking into account the needs of children with disabilities or SEN or those from other vulnerable categories.
- Explore the potential of digital tools available to educational institutions (such as tablets, interactive boards, online courses, AI technologies, etc.) to inform and sensitize the school community, including students, about the opportunities of digital education and how risks can be turned into opportunities.
- Identify, expand, and disseminate successful experiences in preventing online risks in various linguistic and ethnic communities via specific multilingual learning practices and adjust the available information resources to their cultural and linguistic needs.
- Develop and implement comprehensive school policies reflecting the strategic vision of the school for the integration of technologies in the classroom, in teaching, and in the learning process, in parallel with building the motivation of educational staff, students, and parents to use digital tools and develop skills to use them safely.

II. Promoting at the National Level a Multidisciplinary Approach to Prevent and Combat Online Risks Based on Integrated Evidence

- Approve the *Online children's safety action plan*, which will set forth the commitment of all relevant stakeholders to ensure a child-safe online environment through an interdisciplinary approach.
- Embed a comprehensive and constructive approach by the MoER in all initiatives to assess, amend, and review curricular programs through embedding online safety as a cross-cutting subject.
- Develop guidelines on the practical implementation of the intersectoral cooperation mechanism stipulated by Government Decision No. 270/2014 in online abuse and exploitation cases for specialists engaged in social protection, education, healthcare, and the police.

III. Implementing Online Children/Students' Safety Standards by Educational Institutions

- Develop monitoring mechanisms on the implementation of *Online children/students' safety standards* by the MoER to collect regular data about progress in their implementation by educational institutions and use them for the development of evidence-based policies to ensure children's safety in the digital environment.
- Engage LEA in promoting the implementation of the *Online children/students safety standards* by educational institutions through control and monitoring activities.
- Organize exchanges of good practices between educational institutions in the implementation of

Online children/students safety standards and protection of children in the online environment by encouraging a comprehensive response at the institutional level.

- Ensure an inclusive approach at the local level by providing information to marginalized groups about online risks, disseminating the information in different languages, and making it accessible to all linguistic and ethnic communities.
- Integrate activities for the development of transversal competencies into digital education programs, such as skills related to social interaction, communication, collaboration, online content creation, problem-solving, and critical thinking.
- Regularly update educational staff about technological innovations and trends linked to young people's use of digital resources, organize activities to develop teachers' digital literacy, and integrate the sub-competency on online safety.

IV. Changing Attitudes and Practices of Community Members Toward Better Prevention of Risks in the Digital Environment

- Carry out thematic awareness-raising campaigns for parents, caregivers, child protection specialists, and community members about online child abuse to change attitudes and combat stereotypes.
- Develop parenting programs adjusted to various child age categories, aimed at improving communication with children about online safety and shifting the approach from a restrictive to an informative and educational one, based on trust and respect.
- Empower child protection specialists operating at the local level to supervise and provide support to vulnerable families and to prevent risk situations in children, including online risks.

V. Ensuring Children’s Access to Information Resources, Reporting Tools, and Support Services

- Carry out national evidence-based information and awareness-raising campaigns about how specific risks might affect the children, including the lesser-known ones, such as exposure to abusive or sexual content, online risks from peers, and online shopping safety risks.
- Empower youth in the field of online safety to be able to engage them in peer-to-peer communication, raise other students' awareness of online risks, and provide successful examples of coping with these.
- Develop children’s digital skills and mechanisms to assess their competency, including the sub-competency related to online safety, tailored to all levels of compulsory education.
- Develop children's critical thinking and ability to recognize online risks through practical activities and case studies within the compulsory school curriculum as well as through informal education activities.
- Ensure opportunities for improving the digital literacy of all children, particularly vulnerable children, by developing and implementing educational programs outside school (such as in libraries, youth centers, etc.).

VI. Awareness Raising of the Information and Communication Technology Private Sector to Prevent and Combat All Forms of Digital Violence Against Children

- Approve the recommendations for online intermediary service providers on preventing and combating illegal content and harmful/illegal behavior online.
- Develop and disseminate mechanisms for reporting illegal content on service providers' platforms that are available to users.
- Promote child protection principles in the digital environment, including in consuming digital products and services, as well as the development of services that apply safety measures in the design and corporate policies of digital service providers.

References

Bronfenbrenner, U. (1979). *The Ecology of Human Development*. Cambridge, MA: Harvard University Press.

Child sexual exploitation and abuse online: Survivors' perspective in Moldova. (2021). Retrieved from http://www.lastrada.md

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, October 25, 2007.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 *on combating the sexual abuse and sexual exploitation of children and child pornography,* and replacing Council Framework Decision 2004/68/JHA

Global Kids Online Research Toolkit. (2020). Survey guide.

Government of the Republic of Moldova, Government Decision no. 270 of 08-04-2014 on the approval of *Guidelines on the intersectoral cooperation mechanism on the identification, assessment, referral, assistance and monitoring of child victims and potential victims of violence, neglect, exploitation and trafficking*. Issued: 18-04-2014 in the Official Monitor. 92-98 art. 297.

Government of the Republic of Moldova, Government Decision. 519 of 22-07-2022 *on the approval of the organization and functioning regulations of free child phone assistance and the Minimum quality standards*. Issued: 26-08-2022 in the Official Monitor no. 267-273 art. 664.

Impact of piloting the Online children/students safety standards. (2022). Retrieved from http://www.lastrada.md

International Centre "La Strada." (2017). *Online children's safety*. Retrieved from http://www.lastrada.md

International Centre "La Strada." (2021). *Online children's safety*. Retrieved from http://www.lastrada.md

Internet Matters/Youthworks (2019). Vulnerable children in a digital world. Retrieved from: https://www.internetmatters.org/about-us/vulnerable-children-in-a-digital-world-report/

Livingstone, S., Lievens, E., & Carr, J. (2020). *Handbook for policy makers on the rights of the child in the digital environment*. Council of Europe.

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe*. EU Kids Online.

Livingstone, S., Mascheroni, G., & Stoilova, M. (2021). *The outcomes of gaining digital skills for young people's lives and wellbeing: a systematic evidence review*. New Media & Society. ISSN 1461-4448.

Livingstone, S., Stoilova, M. (2021). *The 4Cs: classifying online risk to children*.

Mascheroni, G. (2020). *Datafied childhoods: Contextualising datafication in everyday life*. Current Sociology, 68(6), 798–813. http://doi.org/10.1177/0011392118807534

O'Neill, B. (2014). *First report on the implementation of the ICT principles*. Dublin Institute of Technology & ICT Coalition.

Organization for Economic Co-operation and Development (OECD). (2020). *Children in the digital environment: Revised typology of risks*. OECD Digital Economy Papers, No. 302.

Parliament of the Republic of Moldova, Law no. 140 of 14-06-2013 *regarding the special protection of children at risk and children separated from their parents*, issued: 02-08-2013 in the Official Monitor no. 167-172 art. 534.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries.* EU Kids Online. Retrieved from: http://doi.org/10.21953/lse.47fdeqj01ofo

Online children/students' safety standards. (2022). Ministry of Education and Research, Chisinau.

United Nations Children's Fund (UNICEF) and International Telecommunication Union. (2020). *How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic*. New York, NY: UNICEF.

United Nations Children's Fund (UNICEF). (2017). *State of the world's children: Children in a digital world.*

United Nations Children's Fund (UNICEF). (2021). *Procedure on Ethical Standards in Research, Evaluation, Data Collection and Analysis*.

United Nations Development Programme (UNDP). (2021). *Digital Readiness Analysis Moldova*.

United Nations Evaluation Group (UNEG). *Code of Conduct for Evaluation in the UN system*.

Appendices

Appendix 1. International and National Surveys on Children Online Safety Reviewed

Table 1. International surveys that collected data on safety of children in the digital environment

Survey	Countries	Age group	Methodology and sampling	Managing institution
EU Kids Online, 2020[14]	19 countries	9-17 years	Quantitative Sample – 25 101 children 2 methods of sampling: via households (9) and via schools (10) 2 forms for questionnaire: short for 9-10 years and longer for 11-17 years 3 base methods of data collection: CASI/CAWI CAPI PAPI[15]	Teams of the EU Kids Online network
Young people experiencing internet-related mental health difficulties: The benefits and risks of digital skills. An empirical study, 2020[16]	UK Norway	12-22-years	Qualitative Sampling 62 young people	London School of Economics and Political Science
Vulnerable children in the digital world[17], 2019		10-16 years	Quantitative Sampling 2988 children	Adrienne Katz & Dr Aiman El Asam, in partnership with with Internet Matters

14 https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

15 EU Kids Online, 2020. Survey results from 19 countries, p.13-15. https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

16 Livingstone, S., Stoilova, M., Stänicke, L. I., Jessen, R. S., Graham, R., Staksrud, E., & Jensen, T. K. (2022). Young people experiencing internet-related mental health difficulties: The benefits and risks of digital skills. An empirical study. KU Leuven, ySKILLS. https://www.hf.uio.no/imk/english/research/center/children-media/publications/reports/yskills/d6.1---young-people-experiencing-internet-related-mental-health-difficulties.pdf

17 Vulnerable Children in a Digital World. https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf

Table 2. National surveys that collected data on safety of children in the digital environment

Survey	Age group	Methodology and sampling	Managing institution
School-based surveys			
Children's safety on the Internet, 2017	12-15 years	Quantitative and qualitative methods PAPI survey with self-competition Sampling 1450 children	International Center La Strada and Sociopolis
Children's safety on the Internet, 2021	9-17 years	Quantitative and qualitative methods Online survey with self-completion Sampling 3829 children	International Center La Strada and Magenta
Child sexual exploitation and abuse online. Survivors' perspective in Moldova[18], 2021	18-21 years	Qualitative. Sample of 10 survivors (10 Individual face-to face In-depth Interviews) Quantitative. Online survey. Sample of 54 support workers who works with child survivors of sexual exploitation and abuse	International Center La Strada and ECPAT International
The impact of the Standards for the protection and safety of children/students in the online environment, 2022	9-16 years	Quantitative and qualitative methods Pre- and post- Standards for the protection and safety of children/students in the online environment implementation Sample pre – 600 children Sample post – 591 children	International Center La Strada and Sociopolis

18 Child sexual exploitation and abuse online. Survivors' perspective in Moldova. https://lastrada.md/pic/uploaded/Publicatii_2021/04-11-2021Moldova_National%20Report_EN_FINAL.PDF)

Appendix 2. Vulnerable Children According to the Republic of Moldova Law

Law 140/2013 regarding the special protection of children at risk and children separated from their parents	Law 547/2003 regarding social assistance
The Law no. 140/2013 *regarding the social protection of children at risk and children separated from their parents* does not stipulate the term of „vulnerability", but that of „children at risk". Consequently, according to the article 8 children are at risk when:	Law no. 547/2003 on *social assistance* does not stipulate the term „vulnerability", but that of "vulnerable person", "social assistance recipient" and "risk situation". Article 1 sets forth the term „vulnerability" when describing the notion "needy persons and families" as "socially vulnerable persons and families which are in the conditions interfering their normal economic, educational, social and other activity, etc.;". Thus, the definition of "socially vulnerable person and family" brings no clarity about the "vulnerability". Article 7 stipulates the recipients of social assistance: *persons and families which owing to economic, physical, psychological or social factors have no opportunity due to their capabilities and knowledge to warn and overcome difficult situation,* and namely:
- *children face violence;* - *children are neglected;* - *children are engaged in begging, prostitution, vagrancy;* - *children are deprived of parental care and supervision due to their absence for unknown reasons;* - *children's parents passed away;* - *children live on the street, ran away or were kicked out;* - *children's parents refuse to observe their parental rights in taking care of children;* - *children were abandoned by parents;* - *children's parents were deprived of parental rights by the court.*	- *children and youngsters whose health, development and physical, mental and moral integrity are endangered by the living environment;* - *families who fail to fulfill properly their obligations in educating, caring and raising children;* - *families with no income or low income;* - *families affected by domestic violence;* - *people without family, who cannot manage alone, who require care and supervision or are unable to cope with socio-medical needs;* - *families with three or more children;* - *single parent families with children;* - *elder people;* - *people with disabilities;* - *other people and families struggling with difficulties.*

Appendix 3. Vulnerability Categories Used in the Research

Based on the questions included in the *Characteristics* section of the survey, four *Categories* of child vulnerability were identified. A child could be included in one or more vulnerability category. For example, one child may have only one characteristic from the vulnerability category of children from low-income families - *During the last year of studies, I had difficulties completing school assignments because I didn't have access to the necessary educational materials or books, such as textbooks, exercise books, or other things I needed for school.* Another child; however, could have three characteristics that fall into that vulnerability category – *1. During the last week, at least once, I went to school hungry, I didn't eat in the morning, 2. During the last year of studies, some days I did not go to school because it was necessary to help my parents/caregivers with household work, 3. During my last year of studies, sometimes I didn't go to school because I didn't have clothes or shoes*. In this example we have two children that had four vulnerability characteristics. Therefore, the *Total per category* indicates the number of children in each vulnerability category, while the *Total per each characteristic* shows how many times a child had a characteristic within a category.

From the total sample of 1,412 children, the results are as follows:

- 264 children (19%) do not fall into any vulnerability category
- 464 children (33%) are only in one vulnerability category.
- 387 children (27%) fall into two vulnerability categories.
- 239 children (17%) fall into three vulnerability categories.
- 58 children (4%) are simultaneously in all four vulnerability categories.

Category	Characteristics	Number	%
Children from low-income families	Total per category	642	45
	Total per each characteristic	1088	77
	During the last week, at least once, I went to school hungry, I didn't eat in the morning	422	30
	During the last year of studies, some days I did not go to school because it was necessary to help my parents/caregivers with household work	144	10
	During my last year of studies, sometimes I didn't go to school because I didn't have clothes or shoes	20	1
	During the last year of studies, I often did not have school supplies (like backpacks, notebooks, books, pencils, rulers, etc.)	97	7
	During the last year of studies, when there were online lessons, I couldn't participate in online school activities because I didn't have access to an electronic device or an Internet connection	100	7
	During the last year of studies, I had difficulties completing school assignments because I didn't have access to the necessary educational materials or books, such as textbooks, exercise books, or other things I needed for school	61	4
	During the last year of studies, I did not participate in extracurricular activities or school trips because my family could not afford the costs of them	96	7
	At home, I do not have a specific place to do my school assignments	148	10

Category	Characteristics	Number	%
Children with limited parental communication and support	Total per category	604	43
	Total per each characteristic	690	49
	I live with both parents, but one of them is not in the country	172	12
	I live only with mom	201	14
	I live only with dad	32	2
	I live with the grandparents / one of the grandparents	50	4
	I live with a relative	13	1
	I live someone else	11	1
	At home, usually, my parents do not talk to me about school, issues I have at school, how I feel at school	211	15
Children with disabilities or with SEN	Total per category	507	36
	Total per each characteristic	686	49
	I wear glasses - I see very poorly without glasses	209	15
	I use hearing aids - I often can't hear what the teacher or my classmates are saying	25	2
	Speech is difficult for me - I pronounce words unclearly	125	9
	I have locomotor problems - I have movement-related issues or need assistance to walk	12	1
	I have difficulties understanding school material and learning - I need help to understand the assignments	242	17
	It is very difficult for me to interact with schoolmates	73	5
Children who speak a different language at home than at school	Total per category	434	31
	Total per each characteristic	434	31
	I study at school in a language other than the one spoken at home	434	31

Appendix 4. Sampling Strategy

Region/Territorial Unit	Proposed school	Reason for selection
South		
Cahul	Gymnasium ”I.L.Caragiale”, Doina village	Small rural community where the level of poverty is higher
	Gymnasium ”Ion Creanga”, Zirnesti village	Locality with ethnic minorities, especially with a larger proportion of the Roma population
Basarabeasca	High School ”N. Gogol”, Basarabeasca town	Locality where Refugee Accommodation Centers for Ukrainian refugees are present
	High School ”Constantin Stere”, Abaclia village	
GATU		
GATU	High School "Todur Zanet" Congaz village	Locality where Refugee Accommodation Centers for Ukrainian refugees are present. Locality with ethnic minorities.
	High School ”S.I.Baranovski”, Copceac village	Locality with ethnic minorities.
North		
Balti	High School "Vasile Alecsandri”, Balti town	Locality with children placement centers
	Gymnasium no.3, Balti town	Locality with children’s placement centers. School with high number of children from vulnerable families
Soroca	High School ”Ion Creanga”, Soroca town	Locality with a larger proportion of the Roma population
	Gymnasium Racovat village	Small rural community where the level of poverty is higher
Riscani	High School ”Silvian Lucaci”, Costesti town	
	Gymnasium "Victor Dumbraveanu", Corlateni village	
Ocnita	High School "Mihai Eminescu" Otaci town	Locality with a larger proportion of the Roma population
	High School "Constantin Stamati" Ocnita village	
Centre		
Criuleni	High School "Boris Dinga”, Criuleni town	
	High School Malaiesti, Malaiestii Noi village	
Hincesti	High School "Stefan Holban", Carpineni village	Locality where Refugee Accommodation Centers for Ukrainian refugees are present.
	Gymnasium Bozieni village	Locality where there are more children placed in alternative family care (foster care)
Anenii Noi	High School “Mihai Eminescu”, Anenii Noi town	
	Gymnasium “A. Guzun”, Bulboaca	Small rural community where the level of poverty is higher
Rezina	High School “Alexandru cel Bun” Rezina town	
	Gymnasium Ciniseuti village	Small rural community where the level of poverty is higher

Chisinau		
Chisinau	High School ”Alexei Mateevici”, Cricova town	Locality where Refugee Accommodation Centers for Ukrainian refugees are present. Locality with children placement centers
	Gymnasium no.68, Dobrogea village	
	Gymnasium Durlesti, Durlesti town	
	High School ”Dimitrie Cantemir”, Chisinau city	
	Gymnasium no.51, Vatra village	
	High School ”Anton Cehov”, Chisinau city	
	High School ”George Calinescu”, Chisinau city	
	High School ”Titu Maiorescu”, Chisinau city	
	High School ”Tudor Vladimirescu”, Chisinau city	
	Gymnasium nr.31, Chisinau city	
	The Municipal Boarding High School with a Sports Profile, Chisinau city	
	High School ”Ion si Doina Aldea-Teodorovici”, Chisinau city	
	High School ”Vasil Levski”, Chisinau city	

Appendix 5. Participants in the Qualitative Research

Table 1. Data about parents/caregivers participating in focus group discussions

PARENTS			
No. of focus group discussions	**Category of participants**	**Residence environment**	**Number of participants**
FGD_1_U	Parents/caregivers from various regions	Urban	10 (8 women and 2 men)
FGD_2_R	Parents/caregivers from various regions	Rural	12 (9 women and 3 men)
Total 2 FGD	Parents/caregivers	Urban/Rural	22 (17 women and 5 men)

Table 2. Data about specialists participating in in-depth individual interviews

Code	Category	Sex	Field of activity	Work experience, years
III_1	Manager, specialized services for children	F	Child protection	10
III_2	Manager, specialized services for children	F	Child protection	7
III_3	Manager, specialized services for children	F	Child protection	5
III_4	Teacher	F	Education	20
III_5	Manager, PAS	F	Education	33
III_6	Psychologist, PAS	F	Education	5
III_7	School psychologist	F	Education	9
III_8	School principal	F	Education	20
III_9	Prosecutor dealing with online crimes against children	F	Law	6
III_10	Officer investigating crimes against children in the online environment	F	Law	2
III_11	Psychologist, highly specialized services	F	Child protection	10

Appendix 6. Information Note Approving the Research Protocol

Attachments:
- Informed Consent Form FGD participants 15.04.24.pdf
- Informed Consent Form KII participants 15.04.24.pdf
- Informed Consent Form Parents for their children 12.04.24.pdf
- Assent Form Children 15.04.24.pdf
- Expedited Review Approved: IRB #2553.pdf

HML IRB
RESEARCH & ETHICS

Expedited Review Approved: IRB #2553

To: Camelia Gheorghe
Institution: Palladium Group
From: HML IRB
Subject: Study #2553
Date: 04/16/2024

Dear Camelia Gheorghe,

The protocol **Children's Safety in the Digital Environment, 2553** was assessed through an expedited research ethics review by HML Institutional Review Board. This study's human subjects' protection protocols, as stated in the materials submitted, received research ethics review approval on 04/16/2024 in accordance with the requirements of the US Code of Federal Regulations for the Protection of Human Subjects (45CFR46 & 45CFR46.110) and were expedited by (7) Research on individual or group characteristics or behavior.

You may rely on this IRB for review and continuing ethical oversight of this study. You and your project staff remain responsible for ensuring compliance with HML IRB's determinations. Those responsibilities include, but are not limited to: 1) ensuring prompt reporting to HML IRB of proposed changes in this study's design, subject risks, informed consent, or other human protection protocols; 2) investigators will conduct the research activity in accordance with the terms of the IRB approval until any proposed changes have been reviewed and approved by the IRB, except when necessary to mitigate hazards to subjects; 3) and to promptly report any unanticipated problems involving risks to subjects or others in the course of this study.

The approval of your study is valid through 04/15/2025, by which time you must submit an annual check-in report either closing the study or requesting permission to continue for another year. Please submit your report by **04/08/2025** so that the IRB has time to review and approve your report prior to the expiration date. For instructions on how to manage an approved study refer to: How to Manage an Approved Study.

Please note that we have changed our fee schedule for 2024. For details, please see 2024 HML IRB Fees.

HML IRB is authorized by the U.S. Department of Health and Human Services, Office of Human Research Protections (IRB #00001211, IORG #0000850), and has DHHS Federal-Wide Assurance approval (FWA #00001102).

If you have any questions, please contact us at admin@hmlirb.com.

Sincerely,

D. Michael Anderson PhD, MPH
IRB Chair & Human Research Protections Director
dma@hmlirb.com

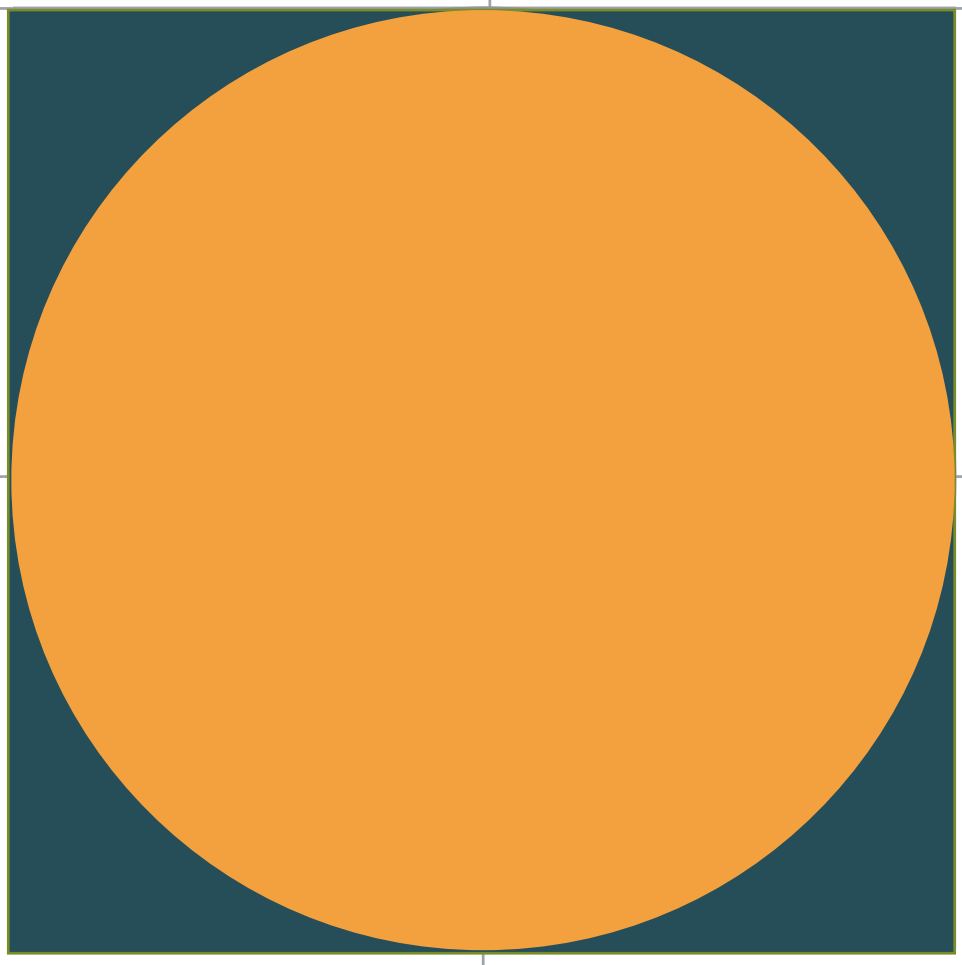
Health Media Lab, Inc.
1101 Connecticut Avenue, NW Suite 450 Washington, DC 20036 USA
+1 202.246.8504 info@hmlirb.com www.HMLIRB.com

Data for Impact

University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC 27516 USA

Phone: 919-445-6949

D4I@unc.edu
http://www.data4impactproject.org



This publication was produced with the support of the United States Agency for International Development (USAID) under the terms of the Data for Impact (D4I) associate award 7200AA18LA00008, which is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill, in partnership with Palladium International, LLC; ICF Macro, Inc.; John Snow, Inc.; and Tulane University. The views expressed in this publication do not necessarily reflect the views of USAID or the United States government.TR-24-588

USAID FROM THE AMERICAN PEOPLE

DATA FOR impact