Fundația Soros Moldova

Norwegian Ministry of Foreign Affairs

LA STRADA Moldova

CHILD SAFETY ONLINE

Public Policies Research

How can the state response be improved in order to prevent and combat the online sexual abuse of children?

Chisinau 2020

Child online safety. Public Policies Research.

How can the state response be improved in order to prevent and combat the online sexual abuse of children?

The present public policies research has been elaborated by the author in 2020 within the project "Public Policy Fellowship" implemented by the Good Governance Department of the Soros-Moldova Foundation. The opinions expressed in this study are those of the author and do not necessarily reflect the views of the Soros-Moldova Foundation or its partners. The copyright on this study belongs in equal measure to the author and the Soros-Moldova Foundation. The author gives Soros-Moldova the right to freely edit and distribute the Public Policy Research.

The research was translated into English with the financial support of the Norwegian Ministry of Foreign Affairs in the framework of the Project „Supporting national authorities to advance policy response to trafficking in human beings with full respect to human rights and rights of trafficked persons".

Author:

Elena BOTEZATU, lawyer, director of Issues Affecting Children Program, International Center „La Strada"

Coordinators:

Ana REVENCO
Victor GOTIȘAN

For additional information regarding the present publication, you can contact us at:

Soros Foundation Moldova, 2019

Bulgara street, no. 32, Chișinău,
Republic of Moldova, MD-2001

Tel.: +373 22 274 480,
+373 22 270 031 Fax: +373 22 270 507,
E-mail: foundation@soros.md

PA International Center „La Strada Moldova"

MD-2012, CP 259, Chișinău,
Republic of Moldova

Tel.: (+373) 22 23 49 06
Fax.: (+373) 22 23 49 07
E-mail: office@lastrada.md www.lastrada.md

Table of Contents

Introduction

In 2017, the Government of the Republic of Moldova, along with various public authorities and institutions, adopted the first Action Plan that intended to promote the safety of children online. The document was approved in the context of a highly mediatized online game[1] – dangerous for children, that shocked the public, shaking the child protection system, but also law and educational systems, signalling about the need of urgent consolidated measures for prevention of similar situations.

The process of implementation of this document was challenging, particularly because the system was caught off-guard - online safety suddenly became a subject of interest, but the level of knowledge around the subject was rather low. Online safety measures have been approached from a technological point of view – ensuring secure access and secure online browsing on digital devices, with no regard to developing safe behaviours and critical thinking in children. Despite the actions undertaken, statistics indicate that children are exposed to a high risk of online sexual abuse. One of the factors that contributes to this risk is the attitude of teenagers towards sending photos of intimate character to people they communicate with online and their attitude towards initiating online relationships with people they don't know.

Three years after the implementation of the Action Plan, it is necessary to evaluate the efforts undertaken and to establish a new course of action for the promotion of safety online. Simultaneously, a thorough analysis of the concept of online safety is required: what it entails and what aspects it refers to, what practices other countries use in the field, what international recommendations and policies can be used to set a directory framework for developing policies of our own.

The purposes of this study are to analyse the framework of national and international policies in the field of child safety online; present the experience of European states in the elaboration and coordination of policies in the field; and come up with recommendations of public policies for the Republic of Moldova, based on the identified needs.

[1] Online game known as "Blue Whale".

Executive Summary

In the context of the expiry of policy documents that regulate the promotion of child online safety (the Action Plan regarding promotion of child online safety; the National Cyber security Program of the Republic of Moldova for the years 2016-2020; the Action Plan for the implementation of the program etc.), it has become obvious that the following priorities need to be established.

In the past few years, there was some significant progress registered in the field of child online safety in the Republic of Moldova in terms of reducing online risks. The policy documents that regulated the actions intended to promote child online safety follow a complex approach that includes planned actions targeting different competence areas, from the promotion of child online safety and reduction of illegal content on the internet to actions that update the legal framework in the field of sexual abuse and sexual exploitation facilitated by the use of ICT devices.

Every policy document that planned actions in the field of child online safety had its own coordination of efforts mechanism – there is no unique discussion and monitoring platform for all the actions in the field. These coordination mechanisms are not inter-connected. For this reason, the processes of monitoring and evaluation are inefficient, being limited to reporting statistical data, which is often duplicated in different reports.

The main achievements in the area of child online safety concern the progress in the field of education, justice and auto-regulation recommendations for Internet service providers. At the same time, the backlogs registered concern some key-aspects, without which a complex and systematic approach to online safety on a policy level cannot be ensured:

- Some mechanisms for reporting illegal content online are missing, which is why it is impossible to report the existence of such content and request its removal, a practice performed by Hotline[2] services around the world;

[2] https://www.inhope.org/EN

- The only online platform that offers counselling and information about online safety www.siguronline.md is managed by a non-governmental organization, there were no official partnerships established between the Ministry of Internal Affairs, the Ministry of Education, Culture and Research, Ministry of Health, Labour and Social Protection and La Strada Moldova – who created and manages www.siguronline.md;
- The process of assessing the illegal and harmful content has not been developed and consolidated, meaning the Agency for Protection of Morality continues to assess illegal content based solely on the provisions of law no. 30 from 07.03.2013;
- The legal framework has not been adjusted to the provisions of the Lanzarote and Budapest Convention, commitments taken on by the Republic of Moldova with the ratification of these Conventions;
- There is a lack of qualitative statistics available online on cybercrime involving children and adolescents, which creates impediments in estimating the complexity and scale of child abuse in the online environment.

Although online safety has been discussed more in the past three years, national studies show that children use the Internet more, they communicate and socialize more, getting exposed to contact and conduct risks in the online environment (online harassment, sexting, sexual abuse etc.). The most problematic situations that children have to deal with online concern online relationships and communication, especially with unknown people, data shows that:

- 16.3% of children have involuntarily accessed images or videos of a sexual character;
- 8.1% of children have been encouraged to send photos or videos of their intimate body parts;
- 14.8% of children have received messages of a sexual character online;
- 10% of children who have sent pictures of themselves to unknown people have received indecent proposals from people they met on the Internet.

Many of the risks that children expose themselves to in the online environment are closely linked to the low level of involvement of the parents in educating about online safety; the infrequent and superficial approach to online safety in the school curriculum; and the insufficient level of knowledge of the general public about online risks and support services to contact in the case of online abuse. This shows the need for consolidated efforts in promoting safety online, which would establish measures to inform teachers, parents and pupils about online safety on a regular basis.

Internationally, states of the European Union (EU) elaborate policies on online safety based on the framework set by

the European Strategy for a safer internet for children, the National response model for preventing and combating online sexual abuse and exploitation "We-Protect" and other recommendations from international institutions such as the International Telecommunications Union (ITU), the Council of Europe and others. All these establish a complex framework of measures intended to ensure raising awareness and informing the wider public about the risks of the online environment; educating children in school about online safety by including the subject into the school curriculum; training teachers; elaborating institutional policies on online safety and adjusting the national legal framework to international standards.

The international approaches and recommendations can serve as guidelines for the Republic of Moldova in establishing the dimensions of the policies in the field of child online safety. This study aims to formulate some recommendations for the next cycle of policies, to ensure a comprehensive approach to online safety that would respond to the national needs based on the issued identified in the field.

Methodology

This study intends to support the efforts of the state in protecting children online, especially from the risks of online sexual abuse and exploitation, by considering existing international and regional recommendations and successful practices in the field.

The objectives of this research are:

- To identify the risks that children are exposing themselves to online and describe the problem that needs to be solved through policy documents;
- To identify the national framework of public policies that regulates the measures in the field of child online safety;
- To study recommendations and international policies in the field of protecting children online;
- To develop recommendations consistent with international recommendations for improving the state response towards protection of children online.

Research tasks:

- To analyse the trends in the use of the internet by children, associated risks and factors that contribute to developing risky behaviours;
- To study the achievements and backlogs in the implementation of public policies in the field of child online safety;
- To identify gaps and challenges in the implementation of public policies in the field of child online safety, and the monitoring and coordination of measures in the field and to identify the relevance of the proposed objectives in the current context;
- To analyse the national approaches in public policy documents, the type of actions planned and to identify the authorities responsible for the implementation of these actions;
- To analyse models for coordinating measures targeting child online safety on an international level and to identify examples of good practices;

- To analyse international priorities set in the field of child online safety, as well as the main objectives and areas of intervention;
- To develop proposals, both strategic and operational, for improving the state response to the risks that children are exposed to online, to ensure a comprehensive approach and a consolidated strategic vision in the field.

In order to achieve the objectives and the research tasks, the following research methodologies were used:

- In depth study/analysis of the national public policy framework compared to international recommendations and public policies;
- Online questionnaires to be completed by experts from public authorities responsible for the implementation of actions in the field of child online safety;
- Conducting individual semi-structured interviews with representatives from national institutions responsible for the implementation of policies concerning the protection of children online in the Republic of Moldova.

1.

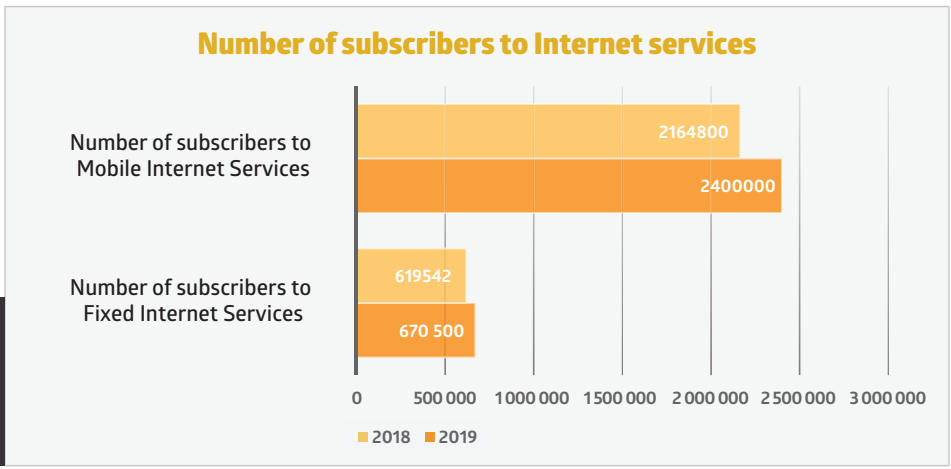
Children online: trends and associated risks

In the Republic of Moldova, **the number of internet users increases** from year to year. Data on the development of electronic communications in the Republic of Moldova in 2018-2019 confirms the existence of a growing number of subscribers for fixed internet and mobile internet services.[3] Internet has become more accessible for everyone in the country, including for children.

The active use of internet by children offers them various opportunities, but it also exposes them to numerous risks that could affect their physical, emotional or sexual integrity. Children access the internet to socialise and communicate with friends, to find information that would help with their homework, to watch movies or to play online games. Usually, on social networks children socialize with people they know, or they make new friends, they post different photos or videos[4]. In the last 5 years, we observed the following trends in the way children use the Internet:

- The use of the internet has increased among children aged 12-13;
- Children communicate and socialize more and more online;
- More and more children under the age of 10 have accounts on social networks, despite the fact that most networks have a minimum age requirement of 13;
- More children make friends online with people they do not know in real life.

Figure 1

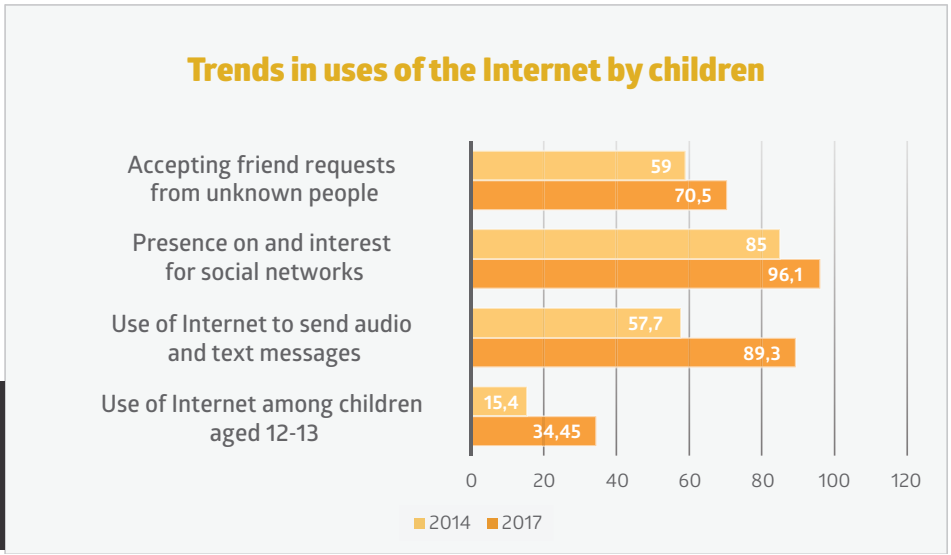


"Number of subscribers to Internet Services (Fixed and Mobile)". Source: National Regulatory Agency for Electronic Communications and Information Technology of the Republic of Moldova (hereafter NRAECIT)

[3] https://www.anrceti.md/files/filefield/Anuar%20statistic%202019_22aprilie_2020.pdf (Text available in Romanian)

[4] http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf (Full text available in Romanian; http://lastrada.md/pic/uploaded/Child_Safety_online_ENG.pdf summary of the report available in English)

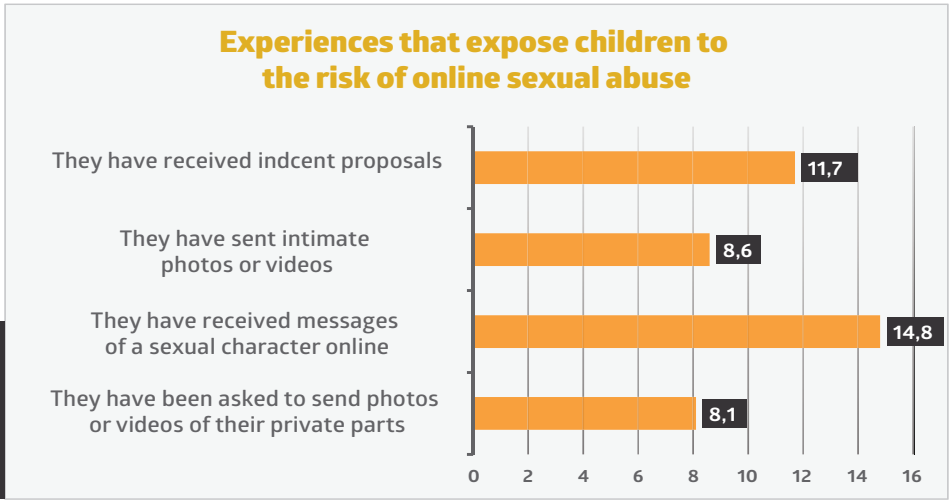
Figure 2



"Trends in uses of the Internet by Children". Source: La Strada Moldova (Study on children's safety online in the Republic of Moldova, 2nd edition, year 2014 and the Study on Child Online Safety, year 2017)

The actions of children online expose them to numerous **contact risks** – risks that involve the direct interaction between a child and an adult, initiated and dominated by the adult. The risk of online sexual abuse is an example of contact risk, which is explained by the following children experiences[5]:

Figure 3



"Experiences that expose children to the risk of online sexual abuse:. Source: La Strada Moldova (Study on Child Online Safety, year 2017)

[5] http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf (Text available in Romanian)

- Children sending photos or videos of their private parts;
- Children receiving messages of a sexual character online;
- Sending intimate photos to unknown persons;
- Receiving indecent proposals online.

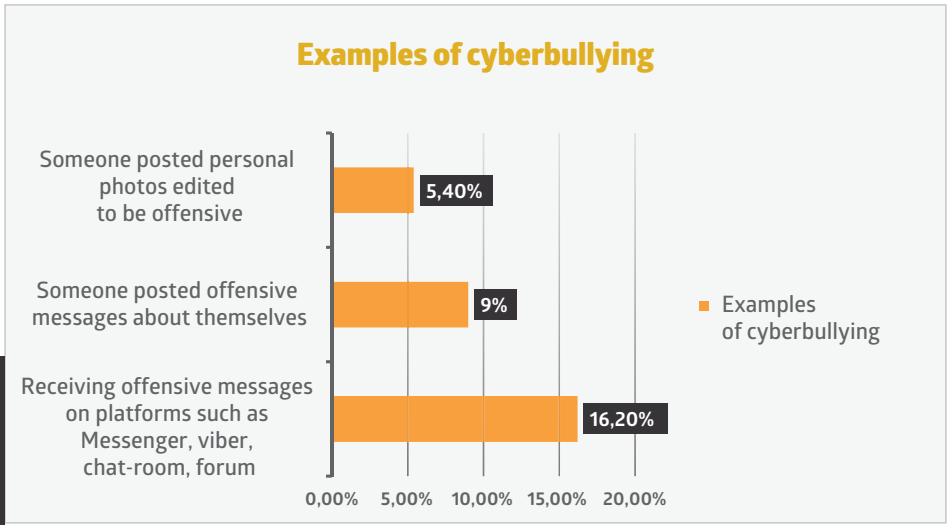
One of the factors that **increase the vulnerability of children to the risk of online sexual abuse** is the teenagers' erroneous perception of amorous relationships online. Over 50% of Moldovan teenagers aged 14-15 consider it normal to send intimate photos to the person you're in a relationship with[6]. Even if the child knows the person in real life, by sending these intimate pictures, he/she loses control over the picture, which could lead to potential harassment or sexual blackmail. The risk is even higher when the child is in a relationship with a person met online, because it could be anyone on the other side of the screen. After sending intimate photos and videos, the probability of further requests for sexual materials becomes considerably higher, as well as requests for other actions of a sexual character, online or offline.

Because children are receptors of mass distributed information, children of the Republic of Moldova are exposed to **content risks**. Children can access content that promotes violence or pornography, content not appropriate for their age, which has a negative impact on their psycho-emotional development. National statistics show that 16.3% of children aged 12-15 have unwillingly accessed videos or images of a sexual character while browsing on the internet. Teenagers aged 15 have been in this situation more often (29.7% out of the total number of children), the risk being lower in children of younger ages (7.4% out of the total number of children)[7].

Conduct risks refer to peer-to-peer interactions, when a child initiates or causes a certain situation, being the online ‚aggressor'/offender. Online harassment is one of the most encountered risk of conduct. A national study on bullying in the Republic of Moldova shows that 70.8% of pupils in the country have faced bullying, while 28.9% of them have faced bullying online too[8]. Online interactions between peers, when children are offended, manifest themselves differently:

[6] http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf
[7] Ibidem
[8] https://www.unicef.org/moldova/media/3146/file (Text available in Romanian)

Figure 4



"Examples of cyberbullying". Source: La Strada Moldova (Study on Child Online Safety, year 2017)

Risky behaviours online don't always develop into abuse, but they certainly influence the level of vulnerability of children. The magnitude of online sexual abuse cannot be estimated because children rarely report the abuse. **21.3% of teenagers don't talk to anyone about any problems they face online, preferring to find solutions on their own**[9]. Because sexuality is a taboo subject in families and the society in general, the probability of children reporting online sexual abuse is even lower.

Statistical data confirms this, the number of cases of online sexual abuse investigated by the police is much lower compared to data on children's vulnerability online. In 2019, the General Police Inspectorate (hereafter GPI) has registered and investigated 49 criminal cases of online sexual abuse or exploitation of children (4 cases of enticing minors for sexual purposes – art. 175/1 CP RM; 5 cases of trafficking of children with the intent of online sexual exploitation – art. 206 CP RM; 39 cases of child pornography – art. 208/1 CP RM; 1 case of child prostitution – art. 208/2 CP RM)[10].

At the same time, the platform www.siguronline.md, which offers online counselling to children victims of online sexual abuse and exploitation, registered 29 cases of online sexual abuse[11]. Only 50% of these cases have been referred to law enforcement agencies, because in the rest of the cases, the

[9] http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf
[10] From data supplied by the General Prosecutor's Office
[11] http://lastrada.md/pic/uploaded/Siguronline%20Factsheet%202nd%20half%20of%202019.docx.pdf

children have refused to work with the police, being afraid of how their parents would react[12]. In the first half of 2020, 36 cases of online sexual abuse have been reported on www.siguronline.md. This is three times the number of cases during the same time last year, suggesting a growing trend in the number of cases registered[13].

Identifying cases of online child sexual abuse is a global challenge, not only applicable for the Republic of Moldova. Materials that contain child abuse become more and more accessible, and the online resources that host these materials are launched and accessed easier than they are identified and blocked. The magnitude, severity and complexity of online sexual abuse and exploitation increases faster than the measures to combat them. Between 2014 and 2018, the number of websites with child sexual abuse content that have been blocked in a year has tripled - from 31225 websites in 2014 to 105047 in 2018[14].

Simultaneously, in 2019, the American National Center for Missing & Exploited Children (hereafter NCMEC) has registered **10516 materials of child sexual abuse uploaded online from the Republic of Moldova.** For comparison, data on other countries include: Austria – 10216 materials were uploaded and shared; Switzerland – 8567 materials; Norway – 8031 materials; Slovakia – 6769 materials; Slovenia – 6890 materials. Although this data does not necessarily imply that 10516 materials represent children from the Republic of Moldova, it does certainly suggest that in the Republic of Moldova there is a high interest from sexual offenders for this type of content.

Although the number of criminal cases that represent online sexual abuse and exploitation of children is relatively low for 2019 (49 cases), data on risky online behaviours of children and their negative virtual experiences[15] signal about a much higher number of unidentified cases. The high number of child sexual abuse materials uploaded from the RM in 2019 (10516 materials[16]) also indicates that there is interest and demand in sexual content including children, **making children even more vulnerable to online interactions with unknown people**.

However, the level of knowledge and preparation of children on how to face these risks is minimal. Only 30% of children aged 12-15 have learnt about child safety online from teachers in school, the other 70% have learnt about it from

[12] http://lastrada.md/pic/uploaded/CST%20factsheet%202nd%20half%20of%202019.docx.pdf
[13] http://lastrada.md/pic/uploaded/Siguronline%2520factsheet_1%2520sem._2020.pdf (Text available in Romanian)
[14] https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc-4c5ef23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf
[15] Based on the study conducted by La Strada 'Child Online Safety', 2017
[16] Based on data from NCMEC

their parents, friends, or professionals[17]. Even in these cases, children are often only taught about the cybersecurity aspect – password security and data protection. The topic of online relationships and intimate conversations has not been approached, suggesting that the topic of safe behaviours and practices online are only approached superficially, both at home and in school. At present, as part of the digitalization process of the educational system, technology is integrated more and more in the teaching process, making the subject of online safety and all its aspects more relevant and necessary than ever.

Another factor that contributes to the vulnerability of children online is the **minimal involvement of parents in educating good online safety practices.** Parents lack knowledge about the potential risks and ways of mediating them, they don't know how to cultivate critical thinking abilities in the online environment in their children, and thus they resort to restrictive methods – limiting and even forbidding the use of technologies. The "generational conflict" also accentuates the lack of communication and understanding in the parent-child relationship. Parents don't perceive online safety as compulsory in a child's education. Or, parents may wrongly consider that their child knows enough about the Internet and he/she can handle it by him/herself. The mass migration of parents and the fact that many children are cared for by their grandparents, who have very little knowledge of digital technologies, equally contributes to the deficient knowledge of children on online safety.

The impact of online abuse has long-term consequences on children. A traumatising online experience can be associated with emotional problems, a low level of efficiency, sleep problems, unjustified risk taking, tobacco consumption, eating disorders or other health issues. Moreover, sharing images or videos of children online, the possibility of the material being watched thousands of times, repeatedly victimises the children, inevitably amplifying the negative consequences of the abuse.

Long-term, childhood abuse determines a low level of efficiency in adult life, low retention rate of the same job, low level of interest and involvement in social life etc. **From an economic point of view,** the phenomenon involves costs for rehabilitation and reintegration into the society of the child/adult who has suffered from abuse in his childhood, costs for developing programs of appropriate rehabilitation, costs to diminish the indirect negative consequences of the abuse (unemployment, health problems, high crime rate, etc.).

The impact of online abuse on the society is manifested through a high level of anxiety regarding sex offenders in the community. The way these cases

[17] http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf

are approached will influence the level of understanding and the emotional response to the phenomena. Even if the impact of these cases on each person in the society may be small, the collective impact on child online safety will be significant. Parents may feel that there is no other way to protect their child online but to forbid them to access the internet. Long-term, these restrictions can reduce the children's level of resilience to abuse. Forbidding the use of technologies makes children more curious, less prepared to identify potentially risky situations and thus more vulnerable to abuse. At the same time, the lack of knowledge and the low level of awareness about online sexual abuse contribute to the blaming of the child by the society. These reactions intensify the psycho-emotional consequences of the abuse, the feeling of guilt and shame, making the child feel responsible for being abused.

Main findings:

1. There is a high level of vulnerability of children online, prompted by the lack of an education oriented at developing critical thinking skills and by the low level of involvement from the parents and the school;
2. Children present a high level of risky, potentially harmful behaviours online;
3. The most problematic situations that children face online concern online relationships and communication, especially with strangers;
4. Parents show a low level of knowledge in the field and are poorly informed about positive parental mediation practices;
5. The "Generational conflict" and the fear of being blamed for what happened reduce the likelihood that a child will directly report a case of online abuse.

2.

The role of the state in reducing the risks that children are exposed to online

2.1. Mapping the national policies in the field

In the past years, the subject of child online protection reached the decision makers, prompting the approval of several policy documents in the field.

Information security strategy of the Republic of Moldova for 2019-2024 and the Action Plan for its implementation[18]

The strategy was developed based on the Concept of information security of the Republic of Moldova, approved through Law no. 299/2017[19]. This was driven by the need to protect the interests of the state, the society and the individual; the vital objectives and of strategic importance for national security; the need to ensure the protection of state secrecy information; and the need to prevent and combat cybercrime.

The concept aims to ensure the protection of fundamental rights and freedoms in the information space; democracy and rule of law; the main objectives when it comes to ensuring information security are largely related to developing response capacities, monitoring the level of information security or informational space, the creation of a communication and evaluation system for information security threats and other aspects that would improve the state response to the risks related to information security.

In chapter III of the Strategy, a series of barriers and normative gaps in the field of preventing and combating cybercrime is listed. They concern the failure to criminalize the offense of breaching secrecy of correspondence, the lack of a computer system and computer-data search procedure as set out by the Budapest Convention, the impossibility of carrying out the special investigative measures necessary to document cybercrimes, the lack of special investigative measures for intercepting computer data, but also other measures on cybersecurity. This chapter also mentions the issue of not criminalizing the conscious access to child pornography using information and communication technology (as provided by the Lanzarote Convention).

The 7th Objective of the strategy is to *protect children from any kind of online abuse,* which resulted in the provision of the following actions:

1. Combat child pornography online;
2. Combat grooming and sexual harassment of children through the use of the internet;
3. Promote a safer internet for children through online counselling; and encourage children to report abuse through specialized informational campaigns.

[18] Government Decision no. 257 of 22.11.2018 on the approval of the Information security strategy of the Republic of Moldova for 2019-2024 and the Action Plan for its implementation published on 18.01.2019 in the 'Monitorul Oficial' Journal no. 13-21, art. 80

[19] Law no. 299 on the approval of the Concept of Informational Security of the Republic of Moldova, approved on 21.12.2017

Including child pornography into the context of preventing and combating cybercrime is not legally justified. Art 208[1] of the criminal code is part of Chapter VII "Crimes against families and minors", whereas cybercrimes are regulated under Chapter XI "Cybercrimes and telecommunications crimes". Even in the Budapest Convention the measures referring to child pornography are included under Title no. 3 "Content-related offences" and are regulated separately from Offences against the confidentiality, integrity and availability of computer data and systems (Title 1) and Computer-related offences (Title 2).

Regulating measures that refer to combating child pornography using policies in the field of cybersecurity is somewhat based on the provisions of the Budapest Convention. Still, such an approach is obsolete, particularly in the context of the international evolutions in the field of child protection against online sexual abuse and exploitation. The Budapest Convention was approved in 2001 and it was the first international treaty that criminalized child pornography offences. At that stage, the technology was actively and substantially developing, which consequently facilitated the development of the criminal phenomenon in the online environment. Regulating child pornography in the Budapest Convention has created levers to combat online sexual exploitation of children[20].

Consequently, in 2007, sexual abuse and exploitation of children, including in the online environment, have been stated in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) as forms of sexual exploitation of children. Thus, since the endorsement of the Lanzarote Convention, offences of child pornography can be perceived from another perspective – an offence that violates the sexual integrity of children, and not an offence in the field of cybersecurity.

The National Cybersecurity Plan of the Republic of Moldova for the years 2016-2020 and the Action Plan for its implementation[21]

This programme aims to create a cybersecurity management system in the RM, by securing information society services, thus contributing to the development of an economy based on knowledge, which consequently will stimulate the increase of the degree of economic competitiveness and social cohesion and will ensure the creation of new jobs.

Also, according to Title 14 in this Programme, cybersecurity is a 'state of normality which has resulted from the application of set of complex proactive

[20] Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, adopted by the Cybercrime Convention Committee, Working group on other forms of online violence, especially against women and children.
[21] Government Decision no. 811 from 29.11.2015 regarding the National Cybersecurity Plan of the Republic of Moldova for the years 2016- 2020, published 13.11.2015 in the 'Monitorul Oficial' journal no. 306-310, art. 905.

and reactive measures that ensure confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, information systems and resources, public and private services". The proactive and reactive measures include policies, concepts, standards and security guidelines, risk management, training and awareness activities, implementation of technical solutions to protect cyber-infrastructures, identity management and consequence management.

This Programme also includes the crime of child pornography (art. 208[1] Criminal Code of the RM) into the cybercrime category, referring to the provisions of the Council of Europe Convention on cybercrime, approved in Budapest on the 23rd of November 2001.

The Action Plan of this Programme includes, under Object 4 "Preventing and Combating cybercrimes", title 4.5 establishes "Adjusting the national regulations to the provisions of the Council of Europe Convention on Protecting Children against sexual exploitation and abuse and of the additional Protocol to the Convention (Lanzarote, 25th October 2007)".

This policy document has created levers for adjusting the national legal framework to the provisions of the Lanzarote Convention. Although the subject has been included in the cybersecurity platform – a field that aims to protect values different to those of protecting the sexual integrity of children in the online environment, this has given rise to the first actions in the adjustment of the national judicial framework to international standards. This policy document has served as a basis for the efforts initiated by the Ministry of Internal Affairs (MIA) and La Strada Moldova regarding the creation of a national mechanism for monitoring the implementation of the Lanzarote Convention. However, none of the initiated actions has been implemented. The draft bill registered in the Parliament of the RM under no. 161 from 13.04.2017 for the modification and completion of some legislative documents, has not been examined during the first reading of the parliamentary session, it being declared void and afterwards withdrawn. The national mechanism for monitoring the implementation of the Lanzarote Convention has not been approved because the MIA and the State Chancellery could not find common ground on which main structure would monitor the Convention[22].

The Action Plan regarding promoting safety of children and adolescents on the Internet for the years 2017-2020[23]

This Action Plan has been elaborated in the context of the implementation of the provisions of the Strategy for Child Protection for the years 2014-2020 and the Activity Programme of the Govern-

[22] http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf (available in Romanian)

[23] Government Decision no. 212 from 05.04.2017 on approving the Action Plan regarding promoting safety of children and adolescents on the Internet for the years 2017-2020

ment of the Republic of Moldova for the years 2016-2018, but also in the context of coordinating and stimulating efforts from all the parties interested in increasing the level of safety of children and teenagers on the Internet.

This Action Plan has the following priorities:

1. Reduce illegal content on the Internet and address negative behaviour online;
2. Promote a safer digital environment for children and teenagers by collaborating with all the parties involved;
3. Raise awareness and inform all parties that are in direct contact with children about the risks of the online environment and formulate recommendations regarding the safe use of the Internet;
4. Generate statistics and promote research on safety of children and teenagers online.

This was the first thematic policy document which regulated actions of promoting child online safety. Thus, several public authorities and institutions, which until 2017 have never had responsibilities in the field of child online safety, have participated in actions promoting online safety. Through this Action Plan, the foundation of the first common efforts in protecting children against online dangers has been laid.

The Action Plan on the implementation of the Strategy regarding child protection for the years 2014-2020[24]

One of the objectives of this Action Plan is to "Prevent and combat violence, negligence and exploitation of children, promote non-violent practices when raising and educating children" (General Objective 2). In this context, the following actions regarding child online safety have been planned:

Action 2.1.16 "Develop and promote information and prevention services in the field of child online safety through the use of an online platform (option to report child pornography content, parental empowerment on securing the access of children to information)."

Action 2.1.18 "Elaborate a minimum set of compulsory rules for the internet service providers and a set of recommendations on auto-regulating mechanisms, such as parental controls, that limit the access of children to content that is potentially negative to the psychological wellbeing of the child."

Action 2.1.22 "Organize national awareness campaigns that target children, parents and the general public on prevention of violence against children and the safe and responsible use of the Internet."

Action 2.2.18 "Organize informative activities during the awareness raising campaigns on Cybersecurity and safety of children online."

[24] https://gov.md/sites/default/files/document/attachments/intr05_75.pdf (text available in Romanian)

Action 2.2.19 "Elaborate and institutionalize the curriculum on preventing and combating offences of a sexual character committed against children using informational technologies intended only for the use of law enforcement agencies and representatives of the judicial system."

These actions have served as a foundation for the elaboration of the Action Plan regarding promoting safety of children and teenagers on the Internet for the years 2017-2020 – all these actions have been transposed and detailed in thematic policy document.

The National Strategy for the Information Society Development "Digital Moldova 2020" and the Action Plan for the implementation of the strategy[25]

The national strategy "Digital Moldova 2020" for the development of the Information Society has the general objective to create favourable conditions for developing and using the ICT potential widely and in full by public institutions, businesses and citizens, to achieve economic, social and cultural goals that would benefit everyone. The strategy focuses on three main lines of political involvement:

1. Expanding access and connectivity by promoting competition for broadband access networks and services;
2. Stimulating the creation/development of digital content and electronic services;
3. Strengthening the use capacity of the benefits offered by ICT.

In this strategy, there is only one action that concerns our research field:

Pillar II, General Objective: Create favourable conditions for the elaboration and valorisation of national digital content and the digitalization of existing national content, as well as for the implementation and use of electronic services.

Action 4.14 Elaborate and disseminate recommendations for children and adults on accessing digital content on the Internet, mentioning potential dangers.

Thus, policy documents that regulate actions intended to promote child safety online have a rather complex approach. For more details, see Table 1.

[25] Government Decision no. 857 from 31.10.2013 regarding the approval of the National Strategy for the Development of the Information Society "Digital Moldova 2020".

Fields regulated by national policy documents

Policy document	Government Decision no. 857 from 31.10.2013	Government Decision no. 835 from 04.07.2016	Government Decision no. 212 from 05.04.2017	Government Decision no. 811 from 29.11.2015	Government Decision no. 257 from 22.11.2018
Field	Information Society Development "Digital Moldova"	Child protection	Promoting safety of children and teenagers online	Cybersecurity	Information security
Dimension	Accessing safe content	Information and Prevention	Reduce illegal content on the Internet	Adjust the legal framework in the field of sexual abuse and exploitation	Combat child pornography on the Internet
		Reporting child pornography	Promote a safer digital environment		Combat grooming and sexual harassment of children using the Internet
		Auto-regulation measures for Internet service providers	Raise awareness and provide information for parents and people in direct contact with children		Though the use of specialized informative projects, promote a safer Internet for children by offering online counselling and encouraging to report abuse
		Develop capacities in law enforcement agency and judicial system representatives	Elaborate statistics and promote research on the topic of safety of children and teenagers online		

Table 1.

Main findings:

Policy documents that regulate actions intended to promote child online safety have a rather complex approach, the actions planned concern various areas of competency, starting from promoting child online safety – actions such as reducing illegal content on the internet, to actions on updating the legal framework in the field of sexual abuse and exploitation facilitated by ICT.

2.2. Achievements and backlogs in policy implementation

Main achievements

One of the most important achievements from the past few years, which was a consequence of the implementation of policies that promote child online safety is the **raising of awareness and informing teachers, students, and parents on the use of technologies online in a safer and more responsible manner**, the risks of the Internet and the ways to face them. Every year, in the context of the Safer Internet Day and the Cybersecurity Month, educational institutions organize informative activities for parents, students and teachers on the risks of the online environment, risky behaviours and ways to stay safe on the Internet[26].

In the field of education, it can be seen that multiple subjects related to online safety have been integrated into the curriculum. Although such an update has not been planned in the policy documents, these evolutions have determined the need to develop educational programmes that contribute to the digital education of children, an example of such programmes are the optional class "Media Education" for gymnasium and lyceum students and the compulsory class "Digital Education" for primary students only.

Another important achievement concerning the prevention of content risks for children is the approval of the **Recommendation on auto-regulating filters for online content that is negative for children** – service provided by the network and IT communication providers. Therefore, according to statistical data for the year 2019, from the 97 Internet service providers, a large proportion of them have made tools available that allow filtering of content that has a negative impact on children. But it should be noted that a considerable number of service providers have reported a lack of requests from end users (parents, tutors, educators etc.) on how to make use of the content filters. Only 3 providers have reported an actual provision of this service[27].

In terms of combating online abuses of children, **methodical instructions for investigations of online sexual offences**

[26] http://mei.gov.md/sites/default/files/raport_hg_212_pe_2019.pdf (text available in Romanian)
[27] Ibidem

against children have been elaborated and **trainings for judges and prosecutors** have been organized **on methods and tactics for investigation and prosecution of offences committed against children through the use of informational technologies**. The carrying out of these trainings is mentioned in the Information on the implementation of the Action Plan on promoting child safety online but also in the Report on the execution of the National cybersecurity plan of the Republic of Moldova for the years 2016-2020[28] during semester II of 2019. The General Prosecutor's Office has reported actions undertaken to examine criminal procedure regulations, special investigation measures all in relation to provisions of international documents. The GPO also reports the realization of a statistical study of the state of affairs regarding the investigation of child pornography for the years 2013-2017 (as per actions 4.6[29] and 4.7[30] of the National Action Plan for the implementation of the national cybersecurity programme).

Main backlogs

- No mechanisms have been created to report illegal content on the Internet (actions 1.1, 1.2, 1.3 of the National Action Plan for the promotion of child online safety, institution responsible – the State Agency for the Protection of Morality and the Ministry of Internal Affairs);
- A web platform that would provide information and counselling on online safety, operational procedures and the procedure of referral to specialized assistance and protection services/law enforcement agencies has not been created (action 2.1, 2.2, 2.3, 2.4 of the National Action Plan for the promotion of child online safety, institutions responsible – Information Society Development Institute, Ministry of Internal Affairs, Ministry of Health, Labour and Social protection and the Ministry of Education, Culture and Research);
- The process of assessing the illegal and harmful content has not been developed and consolidated (action 4.6 of the National Action Plan on promoting child online safety, institution responsible – Agency for Protection of Morality);
- There was no systematization and analysis of statistical data on cybercrime involving children and adolescents, no systematized statistical data or analysis reports were published (action 12.1 of the NPA on promoting child safety online, responsible insti-

[28] http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf (available in Romanian)
[29] National Cybersecurity Plan of the RM, Action 4.6 "Carry out a study to perfect the normative framework in the field of preventing and combating cybercrimes".
[30] National Cybersecurity Plan of the RM, Action 4.7 "Within the General Prosecutor's Office, Security and Intelligence Service and the General Inspectorate of Police consolidate capabilities for the prevention and combating of cybercrime and, where appropriate, generate proposals to modify the normative framework and create a testing and evaluation lab".

tution – Ministry of Internal Affairs);

- No mechanism has been set up to monitor the implementation of the Lanzarote Convention (action 4.5 from the National cybersecurity plan of the RM for the years 2016-2020, institution responsible – the Ministry of Internal Affairs);
- The legal framework has not been adjusted to the provisions of the Budapest Convention regarding the procedures for the investigation of crimes committed with the use of ICT (action 4.1 of the National cybersecurity plan of the RM for the years 2016-2020, institutions responsible – Ministry of Internal Affairs, Security and Intelligence Service and the General Prosecutor's Office);
- The legal framework has not been adjusted to the provisions of the Additional Protocol to the Budapest Convention, concerning the criminalization of racist and xenophobic acts committed through computer systems (action 3.1 of the NPA on promoting child safety online, responsible institution – Ministry of Internal Affairs);

According to the information provided by the representative of the Ministry of Economy and Infrastructure, following the restructuring and the merging of the ministries, there were few human resources left who could be attracted to the field. This has contributed to difficulties in the implementation of the Action Plan on promoting safety of children and teenagers online.

Main findings:

The main findings in the field of child online safety concern the progress in the area of education, autoregulation in the private ICT sector and the field of justice. At the same time, the shortcomings registered concern key-factors, without which a complex and systematic approach to online safety on a policy level cannot be ensured:

- Some mechanisms for reporting illegal content online are missing, indicating the impossibility to report the existence of such content and request its removal, a practice performed by Hotline services around the world[1];
- The only online counselling and information platform on online safety that is available at the moment, www.siguronline.md, is managed by an NGO;
- The process of assessing the illegal and harmful content has not been developed and consolidated, which indicates that the Agency for the Protection of Morality continues to assess illegal content based solely on the provisions of Law no. 30 from 07.03.2013;

[1] https://www.inhope.org/EN

- The legal framework has not been adjusted to the provisions of the Lanzarote and Budapest Convention, commitments taken on by the Republic of Moldova with the ratification of these Conventions;
- There is a lack of qualitative statistics available online on cybercrime involving children and adolescents, which creates impediments in estimating the complexity and scale of child abuse in the online environment.

2.3 Policy coordination Mechanism

All of the policy documents that regulate actions in the field of protecting children online have their own coordination, monitoring and reporting mechanisms for the implementation of their actions. These are specified in Table 2.

Authorities responsible for the coordination, monitoring and evaluation of policies in the field

Table 2.

Policy document	Authority responsible for coordination	Monitoring and evaluation
The National Cybersecurity Strategy of the Republic of Moldova for the years 2019-2024 and the Action Plan for its implementation	**Security and Intelligence Service** as decided through Government Decision (GD) no. 257 from 22.11.2018	As per Government Decision (GD) no. 257 from 22.11.2018, the Security and Intelligence Service is responsible for monitoring. The authority responsible of the evaluation process is not specified.
National **Cyber Security** Program of the Republic of Moldova for the years 2016-2020 and the Action Plan for its implementation	The Ministry of Information Technology and Communication (**now Ministry of Economics and Infrastructure**) as decided through Government Decision no. 811 from 19.10.2015	As per GD no. 811 from 19.10.2015 the MITC (at present MEI) is responsible for monitoring. The authority responsible of the evaluation process is not specified.
The Action Plan on **Internet safety for children and teenagers** for the year 2017-2020	According to GD no. 212 from 05.04.2017, the MITC (presently **MEI**) is responsible for monitoring the execution, collection of information on actions taken by ministries and institutions responsible and presenting a report to the Government.	Not specified

The Action Plan for the years 2016-2020 on the implementation of the **Child protection** strategy for the years 2014-2020	As per GD no. 434 from 10.06.2014, the Ministry of Labour, Social Protection and Family (now Ministry of Health, Labour and Social Protection) has the role of coordinating the implementation of the Action Plan. Within the ministry, a work group will be created including representatives of relevant authorities, institutions and organizations involved in the process of strategy implementation. The intermediary evaluation report of the implementation of the strategy and the plan it is specified that the National Council for Child Rights Protection is responsible for coordination.	As per GD no. 434 from 10.06.2014, the Ministry of Labour, Social Protection and Family is responsible for the processes of monitoring and evaluation.
The National Strategy for the Information Society Development "**Digital Moldova 2020**" and the Action Plan for the implementation of the strategy	As per GD no. 857 from 31.10.2013 the MITC (presently MEI) is responsible for implementing the strategy.	As per GD no. 857 from 31.10.2013, the e-Transformation Council, with the support of MITV (at present MEI) is responsible for the process of monitoring and evaluation of the strategy implementation.

Table 2.

The existence of several policy documents that establish measures in the field of online safety and the existence of parallel coordination mechanisms often causes the same actions to be reported multiple times on different platforms.

Duplications in the data reported

Table 3.

Data reported	Planned action	Platform for the reporting of results
Involving teachers into informative and awareness activities dedicated to children within the "Cybersecurity month" and "Safer Internet day";	Action 8.1 Promote the subject of a safe online environment during extracurricular activities, formal and informal events for pupils and young people;	Information on the level of completion as of 2019 of the Action Plan about promoting Internet safety for children and teenagers for the years 2017-2020;
	Action 6.2 Add cybersecurity to the school curriculum;	Report on the execution of the National cybersecurity plan of the Republic of Moldova for the years 2016-2020 during semester II of 2019[2];
	Action 2.1.22 Organize national awareness campaigns targeting children, parents and the general public on preventing and combating violence against children and on the safe and responsible use of the Internet;	Report on the implementation of the Action Plan for the years 2016-2020 on the implementation of the child protection strategy for the years 2014-2020;
Methodical instructions for investigating online sexual offenses committed against children;	Action 1.2 Elaborate and implement **specialized training modules** in the field of identifying, investigating and prosecuting offences committed against children using information technologies;	Information on the level of completion as of 2019 of the Action Plan about promoting Internet safety for children and teenagers for the years 2017-2020;
	Action 4.4. Elaborate methodical instructions for investigating offences of a sexual character committed against children using information technology;	

[2] http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf (text available in Romanian)

Tabelul nr. 3

Carry out subjects with the topic "Methods and tactics for the identification, investigation and prosecution of **crimes committed against children using information technology**;	Action 4.2 Train law enforcement agencies' representatives and cybersecurity specialists on: a. detecting, investigating and prosecuting **cybercrimes**; b. the link between cybercrime, organized crime, economic crimes and offences of other categories.	Report on the execution of the National cybersecurity plan of the Republic of Moldova for the years 2016-2020 during semester II of 2019
	Action 4.3 Professional training of representatives of law enforcement agencies and the judicial system on identifying, investigating and prosecuting offences committed against children using information technology.	Information on the level of completion as of 2019 of the Action Plan about promoting Internet safety for children and teenagers for the years 2017-2020.

Main findings:

The existing coordination mechanisms are not inter-connected. There is no unique entity that would coordinate all efforts in the field of child online safety. This makes the processes of monitoring and evaluation inefficient, limiting them to reporting statistical data, which is often duplicated in different reports.

2.4. Identified gaps and challenges

Challenges in the implementation of policies

The Action Plan regarding promoting child safety online has not been put into practice for several reasons:

1. Lack of financial resources allocated for the implementation of activities. This problem was mentioned by all the public authorities that have completed the online questionnaire in the context of this research.
2. Confusing/vague wording of Government Decision no. 212 from 05.04.2017, which generated impediments in the implementation of the planned actions.
3. A low level of understanding of the subject by public authorities, confirmed by the constant confusion of the term 'online safety' and 'cybersecurity'.
4. A low level of knowledge/expertise in the field among representatives of the public authorities responsible for the implementation of the actions planned, which is confirmed by the poor reporting of the actions carried out, with no details given. Representatives of the Ministry of Internal Affairs, Ministry of Educa-

tion, Culture and Research and the Ministry of Economy and Infrastructure have also mentioned the issue of human resources and the deficiencies in training.

Due to the conflicting evaluations and inconsistent data provided by various representatives of the public authorities, it is becoming a real challenge to determine to what level the Action Plan has been implemented. Although most activities have been reported as put into practice, multiple representatives provide irrelevant, contradictory data or data that does not comply with the regulated progress indicators in their implementation reports.

The level of involvement and collaboration of the authorities responsible for the implementation of policies on child online safety is low. For example, the national Plan on child online safety states that actions that would be implemented, would be done so in partnership with the e-Government Agency, authorities of the local public administration, ICT/network service providers, the Republican Center of Psycho-pedagogic assistance and others. But the data provided in the implementation report of this plan indicates the lack of collaboration in the field, the actions being carried out only by the authorities responsible. This problem was mentioned by the representative of the Ministry of Internal Affairs, who specified that many actions have been carried out separately by authorities, without the input of other institutions or partners.

Issues concerning the coordination of policies in the field

After the optimization reform among central public authorities, the subject of child online safety has reached the agenda of the Ministry of Economy and Infrastructure. The fields managed by the MEI are complex and diverse and online safety, at the moment, is not a priority for the MEI.

Regardless, in the past 3 years, the MEI was responsible for coordinating the thematic Action Plan in the field of child online safety, and of other policies that established online safety measures. In this period, there have been no coordination meetings carried out with representatives of the ministries responsible for the monitoring of the implementation of policies. An update for the reporting period was regularly requested. In some cases, additional requests were made to identify the causes of failure to take action and to take the necessary measures to remove them. The reason for not carrying out the coordination meetings is the lack of dedicated personnel and/or the lack of financial resources. In this situation, summoning coordination meetings would have been fruitless, as there would have been no actions to report.

Another challenge has been the regulating of actions that concern online safety in several policy documents (Digital Moldova, Child Protection, Cybersecurity, Information Security, Promoting safety of children and teen-

agers online). This creates obstacles in ensuring an efficient coordination, monitoring of all initiatives in the field and in the carrying out of an appropriate evaluation. Every Action Plan or strategy mentioned takes a segmented approach to analysing the efforts made, based on the strategic objectives proposed. Consequently, although the Action Plan for the implementation of the strategy on child protection includes actions of child protection online, the intermediary implementation report focused only on the strategic objectives planned and did not specify details about the implementation on these activities or the results obtained in the field of online safety.

The lack of a coordination unit or a mechanism for monitoring/coordinating efforts in the field, which would take into account all policies that establish online security measures, leads to a poor governance mechanism of public policies.

This issue was also mentioned by representatives of the Ministry of Internal Affairs in the context of this study.

The lack of an adequate coordination mechanism in the area of child protection policies is an issue that has been recognized for many years. In the context of the elaboration of several thematic studies that concern the implementation of the Lanzarote Convention by the RM, it has been established that there is no one responsible for applying the Convention and no distinct institution that would monitor the efforts in the field.

Issues regarding the monitoring and reporting of implemented actions

The reports on the implementation of policies in the field of online safety indicate about a material problem with the collection and presentation of relevant data. Although there is a clear reporting mechanism to the Ministry of Economy and Infrastructure, the way in which authorities/institutions report of implemented actions does not take into account the provisions of the National Action Plan regarding promoting child safety online. An example of this is the data presented on the implementation of sub-action 3.1 – implement a legal framework that **incriminates xenophobic acts committed using IT**. On this matter, the MIA has presented data on the number of offences involving **online sexual abuse and exploitation** investigated by the police – offences that have nothing to do with xenophobic acts.

Similarly, although the National Action Plan clearly established progress indicators, most of the **information reported was about carrying out activities without taking into account the activities already planned**. For example, the sub-action 4.5 "Develop a national database for photo/video material that presents illegal content" has the following progress indicators:

- Adjusted and efficient database;
- Classification mechanism for photo/video material with illegal content;

- Number of complaints/reports registered that present photo/video material with illegal content.

However, data provided by the MIA is on the collaboration within the international project "I-CARE" initiated in 2016. It is not clear how the photo/video materials with illegal content are classified, what the number of complaints/reports is, if there is a national database or if the police only uses the international database provided by Interpol.

The information reported by the authorities is incoherent. The same activities are mentioned multiple times on different platforms. For example, activities carried out in the context of the "Safer Internet Day" and "Cybersecurity Month" are reported both in the context of the implementation of the Action Plan regarding promoting child safety and in the context of the National Cybersecurity Programme (see Figure 3).

Moreover, **data reported by the authorities is contradictory and irrelevant**. An example refers to the implementation of action 1 "create national contact points for reporting illegal content on the Internet". Although a normative framework for the operation of a platform for reporting illegal content on the internet (sub-action 1.1) has not been created, the Agency for the Protection of Morality reported that it is in the process of creating(sub-action 1.2) and promoting (sub-action 1.3) a platform for reporting illegal content on the internet. Taking into account that the creation and promotion of a platform are sub-actions, which logically should be preceded by the creation of a legal framework for the regulation/operation of the platform, from the data published, it looks like the promoting the platform goes ahead even if the platform has not yet been created.

In the context of the online survey, a representative of the Ministry of Internal Affairs has specified that the process of monitoring results in the field of child online safety should be improved for the next cycle of policies. According to the representative of the Ministry of Economy and Infrastructure, it was difficult to monitor how the authorities have completed the actions of the plan, as they have not been receptive to reporting. Some authorities reported that it was impossible or difficult to put into practice the actions due to a lack of personnel and/or necessary material resources.

Relevance of the previous objectives in the current context

Based on the trends of use of the internet by children and the identified problem areas, the interviewed public authorities have stated that a great part of the objectives planned in the Action Plan promoting safety of children and teenagers online still remain relevant, specifically:

- Objective 1: Reduce the illegal content on the Internet and approach negative online behaviours;

- Objective 2: Promote a safer digital space for children and teenagers by through the collaboration of all parties involved;
- Objective 3: Raising awareness and informing all parties who are in direct contact with children about the risks of the online environment and generate recommendation on how to safely browse on the Internet;
- Objective 4: generate statistics and promote research in the field of child online safety.

However, it is necessary to review the way in which the planned objectives and actions are formulated, in order to ensure a good interpretation and implementation by the authorities concerned.

Main Findings:

1. Measures on child protection online and promoting child online safety are approached in a segmented manner in various policy documents, with no logical link between them. This creates obstacles in the evaluation of the impact the policies have in the field of child online safety, in determining the positive dynamic in the field of interest and in making the results obtained more efficient etc.;
2. There is a low level of knowledge and understanding of the subject by the authorities responsible for implementing child online safety policies;
3. The current model of coordinating efforts in the field of child online safety is absolutely inefficient, which leads to a superficial approach to the problem;
4. The efforts made by public authorities in the field of interest are parallel and fragmented;
5. The level of collaboration and involvement of partners in the implementation of activities is minimal, being limited to actions carried out within projects;
6. Despite the approval of a thematic policy document in the field of child online safety, a firm commitment from the public authorities to implement the planned actions is lacking.

3.

International standards and approaches

3.1. Ways of integrating child online safety into international policies

A distinct strategy dedicated to the subject

Internationally, the subject of child online safety has been approached and discussed since 1999, when Action Plan for a Safer Internet was approved for the years 1999 to 2004[31]. At the moment of its creation, the Internet was still at its incipient development stage, the priorities of the European Union (EU) involved combating illegal and harmful content and creating a network of Hotline services[32]; encouraging self-regulatory measures; developing content filters; and carrying out awareness activities.

In the last 20 years, the priorities of the EU have been revised. The most recent **European Strategy for a Better Internet for Children**[33] approved by the European Commission in 2012, comprises of the following fields of action:

- **Stimulating the quality online content for children** by encouraging the production of creative and educational online content for children and promoting positive online experiences for young children;
- **Digital and media literacy and teaching online safety in schools**;
- **Scaling up awareness activities and youth participation,** but also promoting tools for online content reporting;
- **Implementation of technical measures** that allow privacy settings, parental controls, content classification systems or stimulating self-regulation measures to protect children from inappropriate content;
- **Developing a framework and law enforcement** when it comes to identifying and supporting victims; taking action against abusers; stopping the flow of images that present child sexual abuse through detection and removal from the internet and preventing future uploads.

This approach entails the regulation of various measures that would be undertaken, including legislative measures, self-regulation and co-regulation measures, technical and educational measures, but also measures of awareness. In practice, the way of implementing the Strategy varies in every country. No country in the EU has implemented the European Strategy directly through transposing into a separate policy document focused on online safety aspects only. 50% of states (12 states) have developed a series of separate policies that directly address the subject of online safety, whereas the other 12 states approach the subject through broader policies[34].

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24190
[32] Hotline services – service used to report illegal content on the internet
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&-from=EN
[34] O'Neill, B. Dinh, The Better Internet for Kids Policy Map, Implementing the European Strategy for a Better Internet for Children in European Member States, March 2018

Awareness campaigns and activities that promote digital education and education on online safety are usually integrated into policies with a broader subject. Pillar 4 – Fighting against child sexual abuse and child sexual exploitation - from the European Strategy only targets the legal framework and the law enforcement agencies, both approached separately.

Integrating online safety into broader subject policy documents

Child online safety in the context of promoting children's rights

Unlike the policy framework used the countries of the EU, which are defined by a thematic sectorial policy on child protection online, the Council of Europe has regulated measures on child online safety in the **Council of Europe Strategy for the Rights of the Child for the years 2016-2021** – a more comprehensive policy document that approaches general measures of promoting children's rights. Therefore, one of the priority areas for intervention in this Strategy is the rights of the child in the digital environment, specifically the child' participation online, safeguarding children from online risks and educating children to use the Internet creatively, critically and safely.

The Committee of Ministers complements EU initiatives in this area in the following strategic directions:

- **Protecting children's rights online** (Recommendation CM/Rec(2018)7 of the Committee of Ministers on the Guidelines to respect, protect and fulfil the rights of the child in the digital environment[35]);
- **Promoting digital citizenship education**, which also includes online safety in the legislation, policies and practices in Education (Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education[36]).

The **Recommendation CM/Rec(2018)** mentions the need to take action on safeguarding children online from every state. Moreover, the need for good coordination and coherence of policies related to children online and the need for consistent measures to reinforce each other were recognized. This could involve either adopting an integrated strategy or an action plan that would regulate children's rights in the online environment, or integrating the subject into existing policies.

Regarding the measures that should be undertaken by the member states, the Recommendation establishes the need of a holistic approach that would regulate the following:

- Awareness measures on the subject;
- Measures concerning materials that include sexual abuse of children;

[35] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

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

- Measures to engage private companies as key-partners in promoting human rights by making commitments to safeguard children online;
- Developing services and products that account for children's interests;

Involving all the above-mentioned players (representatives from the education field, authorities responsible for protecting personal data, businesses, civil society members, youth organizations, direct participation of children etc.) in the process of development of policies and in the process of implementation is a key principle.

The right of the child to online protection and safety remains one of the areas in which action is recommended to reduce contact risks (sexual exploitation and abuse, grooming etc.), *content risks* (promoting the stereotyped and hypersexualized portrait of women and children; promoting violence online, etc.); conduct risks (bullying, non-consensual distribution of sexual images, hate speech, etc.) or risks to a child's health (excessive use of Internet, lack of sleep or physical harm).

Child online safety in policies regarding cybersecurity

There is no globally accepted definition for cybersecurity. Broadly, cybersecurity includes measures of protection of informational systems from unauthorised access, attacks and damages, actions to ensure confidentiality, integrity and availability of data. At the same time, cybersecurity involves the prevention, detection, response and recovery actions after a cyber-incident.

The definition of cybersecurity proposed by the International Telecommunication Union (hereafter ITU) emphasizes protecting the infrastructure, rather than the person: 'the collection of tools, policies, guidelines, risk management approaches, actions, trainings, good practices, assurance and technologies that could be **used to protect the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to the Government, private organizations and citizens**; these assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems and data in the cyber-environment[37]. **Therefore, these clearly mark the measures intended to contribute to child online safety** (focus on emotional, physical and sexual wellbeing of the child online) **and cybersecurity for children** (focus on protection of informational systems, information, devices that children have access to).

In the EU policies, cybersecurity is used in a broader context, not limited to network and information security. The term refers to any illegal activity carried out using digital technologies online, such as: launching computer virus attacks, payment frauds or **dissemination of materials that represent online sexu-**

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

al abuse of children. It can also cover disinformation campaigns to influence online debates and suspected electoral interference[38].

Integrating online safety into cybersecurity policies remains a controversial subject, because states use different practices; regulating 'child pornography' creates confusion in several international treaties and involves a fragmented response in the field. But, the developments from the past years have determined the need to introduce a new designated field – '**cyberviolence**' against women and children, which refers to the following offences covered by the Lanzarote Convention, Istanbul Convention and the Budapest Convention:

- Child online sexual abuse and exploitation;
- Cybercrimes;
- Hate crimes;
- Threats and physical violence;
- Privacy violations;
- Online harassment.

Online sexual exploitation of children is a field covered by the Lanzarote and Budapest Conventions. Although both refer to child pornography, the Lanzarote Convention has a more detailed and complex material legal framework. However, relevant procedural measures or means of international cooperation for the investigations undertaken using IT systems or electronic proof of evidence are lacking. Therefore, states should implement the tools and measures provided by the Budapest Convention in order to conduct the investigations; encourage the use of these tools to effectively address the cyber-dimension of sexual exploitation and sexual abuse of children, especially by applying the provisions of article 16 and 21 from the Budapest Convention into national legislation; and facilitate international cooperation on electronic evidence (articles 23-25 of the Budapest Convention)[39].

Regarding the content of national policies in the field of cybersecurity, the ITU Recommendations for the Development of National Strategies define the following 7 areas of intervention that need to be addressed: Governance; Risk management in the field of national cybersecurity; Training and Resilience; Critical infrastructure services and essential services; Capacity, capacity building and awareness; Legislation and regulations; International Cooperation. **Neither of these areas addresses online sexual exploitation of children, subject that is very specific and should not be addressed in the context of a national strategy on cybersecurity**.

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

[39] https://www.coe.int/en/web/cybercrime/-/t-cy-mapping-study-on-cyberviolence-recommendations

Main findings:

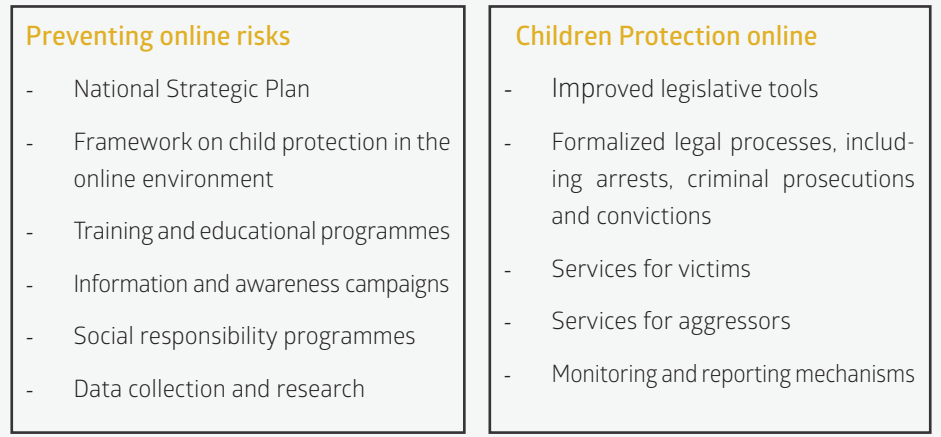
1. In international policy documents, child online safety is either the subject of specific thematic policies in the field, or it is integrated within documents with a broader topic (for example – protection of children's rights);
2. It is recommended to clearly delimit the measures intended to contribute to child online safety, which focus on the emotional, physical and sexual well-being of the child online from the ones that refer to the protection of information systems, information and devices the child has access to;
3. International recommendations and policies in the field of cybersecurity don't approach the subject of child online safety. Usually, prevention measures and measures of protection of children in the online environment are regulated in public policies that aim to ensure the protection of children's rights (Council of Europe Strategy for children's rights) or in thematic policies (European Strategy for a safer internet for children);
4. Cybersecurity can be an umbrella platform for all the measures of combating cyber-offences, including combating child pornography. These policies could regulate the actions intended to improve the response of law enforcement agencies or improve the investigative measures in cases of online sexual abuse or exploitation, as per the provisions in the Budapest Convention.

3.2. Dimensions of the policies in the field of online safety

A comprehensive approach to protecting/safeguarding children online that has been derived from the standards set out in the Budapest Convention, refers especially to two main pillars: Preventing online risks and Child Protection online. According to the international commitments taken on since the ratification of the Convention, the states have committed to take action in different dimensions (see Figure 4).

Dimensions of the policies in the field of online safety

Figure 4.



This approach is recommended by "We-Protect" as well – an international initiative aiming to improve the global capacity of combating sexual exploitation of children online[40]. In 2015, 43 states from the entire world, the United Nations Office on Drugs and Crime (hereafter UNDOC) and the Interpol have committed to take action in boosting national efforts of child protection online, based on the Model National Response elaborated in the initiative[41]. This model represents a unique international coordination framework that aims to evaluate the current response of the states to this issue, the prioritisation method of national efforts and the identification of gaps in the policies that need to be removed, in order to support the Governments in achieving the following objectives[42]:

- **Enhancing efforts to identify victims** and ensure that they receive the necessary assistance, support and protection;
- **Enhancing efforts to investigate cases** of online child sexual exploitation and to identify and prosecute offenders;

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

[41] Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, available at https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf

[42] Our Strategy to End the Sexual Exploitation of Children Online, WePROTECT Global Alliance, July 2016, available at https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/578408b5f7e0ab851b789e14/1479254482761/WePROTECT+Global+Alliance+Strategy.pdf

- **Enhancing efforts to increase public awareness** of the risks posed by children's activities online, including the grooming of children and self-production of images that result in the production and distribution of new child sexual abuse material online; and,
- **Reducing as much as possible the availability of child sexual abuse material online**, and thereby reducing the re-victimisation of children whose sexual abuse has been depicted.

The standards set by this instrument refer to the following aspects: measures intended to consolidate the coordination framework, public policies and legislation; measures to improve the manner in which investigations are carried out, as well as the services provided to the victims; measures that contribute to raising awareness in the society on online sexual exploitation of children and other similar matters (see Table 5).

Extract from the Model National Response for preventing and combating sexual abuse and exploitation of children online elaborated by the Global Alliance We-Protect

Table 5.

Policies and Governance	1.	**Leadership:** An accountable National Governance and Oversight Committee
	2.	**Research, Analysis and Monitoring:** National situational analysis of Child Sexual Exploitation and Abuse (CSEA) risk and response; measurements/indicators
	3.	**Legislation:** Comprehensive and effective legal framework to investigate offenders and ensure protection for victims
Criminal Justice	4.	**Dedicated Law Enforcement:** National remit; trained officers; proactive and reactive investigations; victim-focused; international cooperation
	5.	**Judiciary and prosecutors:** Trained; victim-focused
	6.	**Offender Management Process:** Prevent re-offending of those in the criminal justice system nationally and internationally
	7.	**Access to Image Databases:** National Database; link to Interpol database (ICSE)

Victim	8.	**End to end support:** Integrated services provided during investigation, prosecution and after-care
	9.	**Child Protection Workforce:** Trained, coordinated and available to provide victim support
	10.	**Compensation, remedies and complaints arrangements:** Accessible procedures
	11.	**Child Helpline:** Victim reporting and support; referrals to services for ongoing assistance
Societal	12.	**CSEA Hotline:** Public and industry reporting for CSEA offences – online and offline; link to law enforcement and child protection systems
	13.	**Education Programme:** For: children/young people; parents/carers; teachers; practitioners; faith representatives
	14.	**Child participation:** Children and young people have a voice in the development of policy and practice
	15.	**Offender Support Systems:** Medical, psychological, self-help, awareness.
Industry	16.	**Notice and Takedown Procedures:** Local removal and blocking of online CSEA content
	17.	**CSEA Reporting:** Statutory protections that would allow industry to fully and effectively report CSEA, including the transmission of content, to law enforcement or another designated agency
	18.	**Innovative Solution Development:** Industry engagement to help address local CSEA issues
	19.	**Corporate Social Responsibility:** Effective child-focused programme

Table 5.

Table 5.

Media and Communications	20.	**Ethical and informed media reporting:** Enable awareness and accurate understanding of problem
	21.	**Universal terminology:** Guidelines and application

This Model has been implemented by 43 states worldwide, committing to follow the Strategy of the Global Alliance in combating sexual abuse and exploitation online. Based on these standards, the signatory States, including the Republic of Moldova, have developed national response measures. The biggest challenge in implementing this Model is identifying unique vulnerabilities to the threat at the national level, and an understanding of 'what works' in tackling the threat[43].

Although the Republic of Moldova is a member of the Global Alliance, it did not adhere to the Strategy. Nevertheless, in 2014, the Republic of Moldova reported a partial completion of actions in the field, as per the four objectives mentioned above[44].

Main findings:

The practice of the European states in the field of child online safety indicate that the subject cannot be approached in a one single policy document. Child protection in the online environment can be ensured through a diverse spectrum of actions in the field of education, child protection, law enforcement along with committing to combat sexual abuse and exploitation online. Child protection in the online environment involves authorities in the field of education, child protection and law enforcement assuming responsibilities in combating sexual abuse and exploitation online.

[43] https://www.end-violence.org/sites/default/files/paragraphs/download/WePROTECT%20Global%20Alliance.pdf

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

3.3. Models of coordination of efforts

Studies carried out within the EU Programme *Kids Online* have established evaluation criteria and a classification of states based on their national policies in the field of child online safety[45]. According to the classification, the most developed policies for promoting online safety are in the states where the public sector has a high level of involvement in creating these policies, with the support of Safer Internet Centres[46]. At the same time, these states allocate financial resources for the implementation of said actions and the evaluation of the results from the public budget; they promote digital abilities of children and parents; and pro-actively approach risk mediation.

The countries with the most developed policies in this field are: Belgium, France, Germany, Greece, Spain and the United Kingdom. They are characterized by:

- The existence of a high profile agency that is specialized in the field of child online safety and has coordination responsibilities;
- Legal and normative framework, that is comprehensive and well-developed;
- A large variety of research initiatives in the field;
- The pro-active involvement of the public sector, that acts as a powerful engine in the field of education, and awareness and empowerment initiatives;
- A large variety of policy initiatives;
- Online safety centers[47] have an important role in the coordination of efforts or they complement the development of policies in the field.

A low level of political commitments is characterized by the lack of a structure that is responsible for the coordination of efforts; lack of research in the field and the lack of an evaluation framework for policies. Countries from Eastern Europe, such as Bulgaria, Cyprus, Czech Republic, Poland and Romania have the least developed policies in the field of online safety. These countries are characterized by a high level of online risks and an inefficient mediation of the risks. These countries show:

- A lack of coordination of policies on online safety;
- Relatively recent evolutions of policies;
- New initiatives are focused on developing the ICT sector;
- There is no monitoring and evalua-

[45] Policy influences and country clusters. A comparative analysis of Internet Safety Policy Implementation, LSE, London: EU Kids Online, O'Neill, B. (2014).
[46] Safer Internet Center – functional structures in the EU states that carry out initiatives, services and provide resources to ensure child online safety
[47] Online safety center- service that provides information, advice and assistance to children, young people and parents on how to deal with harmful content, negative contacts or harmful conduct.

tion framework of the policies;

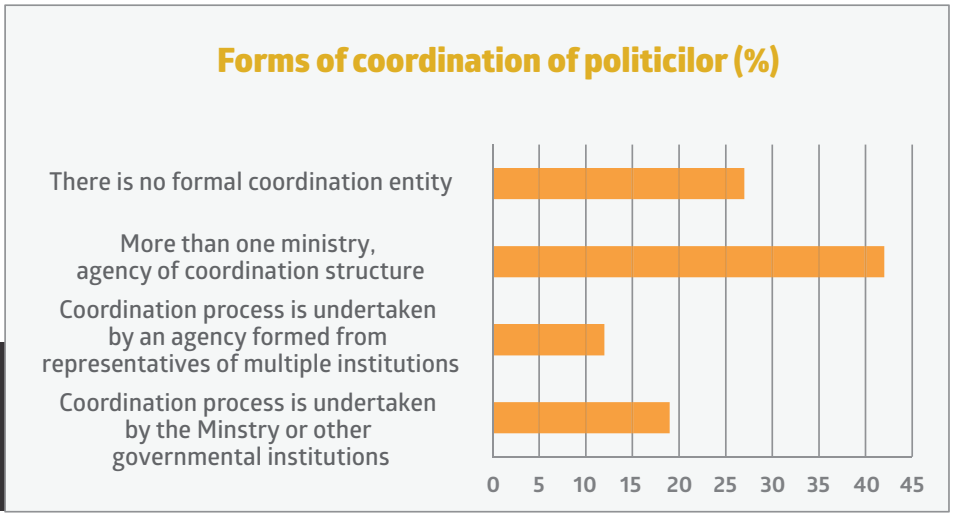
- Online safety centres are a platform of coordination of activities on online safety;
- The public sector is less involved than in other European regions;
- Financial resources for the implementation of these policies are not allocated from the public budget.

The Republic of Moldova is not the only country facing problems in efficiently coordinating efforts to promote online safety and child protection from online sexual abuse and exploitation. This problem is also influenced by the lack of clear international recommendations, including from the Lanzarote Committee – structure responsible for the coordination of monitoring actions of how the Lanzarote Convention is implemented by the member states, and also responsible for supplying explicative and informational support for a better understanding of the assumed commitments[48].

European countries have different coordination practices in the field of child online safety. Over 42% of the states have several ministries or coordination structures.

Forms of coordination of policies on online safety in European states.

Figure 5.



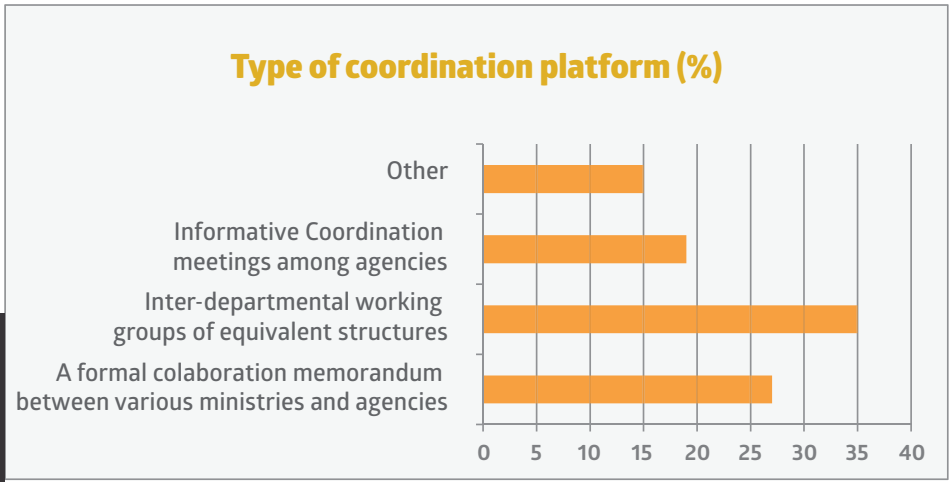
Source: A European Strategy to deliver a Better Internet for our Children

[48] Study of systemic problems that affect the response of the education system to sexual esploitation or abuse of children, Council of Europe 2019

In order to facilitate the cooperation among institutions and agencies in regards to policies on child online safety, 73% of states have created facilitation mechanisms to improve inter-departmental and inter-institutional coordination. The types of coordination platforms are mentioned in Figure 6.

Types of coordination platforms in EU states

Figure 6.



Source: A European Strategy to deliver a Better Internet for our Children

Main findings:

Setting up a mechanism of coordination of policies in the field of child online safety is a challenge for multiple European states. Since there are no recommendations regarding an efficient coordination of policies in the field, every state has developed its own governance practices, either by creating a high level specialized agency or through attributing this role to specialized structures (Online Safety Centres) or to ministries with policy implementation responsibilities.

One thing is certain, a precondition for the development of policies on child online safety is the efficient coordination of efforts, by actively involving the public sector, monitoring and evaluation of results and a comprehensive approach focused on the interests of the child.

General conclusions and recommendations

1. Child online safety is a subject of interest on several public policy platforms: child protection, cybersecurity, digital Moldova, information security, online safety. Thus, the efforts made by the public authorities are parallel and fragmentary, without a unique strategic vision, or comprehensive approach that would integrate all efforts in the field into one unique monitoring and evaluation framework. Coordination of policies has been limited to requesting implementation reports of the actions planned, without carrying out meetings with the relevant authorities.
2. The experience from the past few years indicates about a duplication of reported actions in the context of monitoring of several policy documents. Some actions have been reflected in implementation reports of the Action Plan on promoting safety online of children and teenagers for the years 2017-2020 and in the Report on the execution of the National cybersecurity Programme in the Republic of Moldova for the years 2016-2020.
3. Determining the stage of the implementation process of the National Action Plan is a challenge caused by contradictory evaluation and inconsistent data provided by various public authorities' representatives. Although the majority of activities have been reported as implemented, the data provided is insufficient, in some places it's contradictory or it does not match the regulated progress indicators. Therefore, it is hard to measure the progress and evaluate the factual situation, it impedes the establishment of priorities and the planning of further actions.
4. There is a lack of a firm commitment to implement the measures intended to promote child online safety. This is due to the lack of financial resources and specialized personnel. A great amount of the planned activities/actions haven't been carried out, they have been cancelled or delayed for various reasons. Although the RM has as-

sumed political commitments by ratifying the Lanzarote Convention, the authorities have not made any efforts in this sense.

5. Online safety is a generic concept often confused with other terms such as 'cybersecurity', 'online security' or 'information security'. Consequently, the actors responsible for implementing policies often focus on aspects concerning securing digital devices, maintaining information security or developing technology skills, while actions focusing on preventing and mitigating conduct and contact risks that children are exposed to are often neglected.
6. There is no approach that would be centred solely on the best interests of children, which is based on the need to reduce the risks (conduct, content and contact) that children are exposed to by developing critical thinking abilities in children and promoting services/tools for reporting online abuse.

Strategic recommendations

1. Since the RM is a member of the 'WeProtect' Global Alliance against Online Sexual Exploitation of Children, an update of the partnership and the assumed commitments is required, by adhering to the new Model of policies recommended for the prevention and combating of online sexual abuse and exploitation. At the same time, it is necessary to establish new priorities and national actions to ensure the gradual implementation of this model.
2. For the next cycle of policies, it is absolutely necessary to establish an adequate coordination mechanism in the field of child online safety. All existing options in the field should be taken into consideration: either through empowering a ministry under the auspices of which a technical working group can be created – one that would ensure both the efficient communication between authorities on the topic and the regular and a continuous monitoring of the efforts in the field; or through revising the competencies of the National Council for Child Rights Protection and attributing the responsibility to coordinate and monitor the efforts made in the field of child protection from the online risks.
3. Since the measures regarding online safety can be included in multiple policy documents, it is necessary to have inter-institutional coordination, to ensure the communication between the different structures responsible to develop policies, but also to ensure coherence of the policies among various measures/actions planned in policy documents.
4. Since several public policy documents that regulated online safety measures have recently expired (National Action Plan on Promoting Safety of children and adolescents on the Internet for the years 2017-2020; National Programme for cybersecurity of the Republic of Moldova for the years 2016-2020; and the Action Plan for the implementation of the programme etc.), it is imperative to plan actions that would continue the efforts in the field of

promoting child safety online. Thus, it is necessary to create a working group within the Ministry of Health, Labour and Social Protection, that would plan the full set of actions in the field of promoting safety online.

5. In the process of elaboration of policies in the field of child online safety, it is important to consider the international commitments assumed through signing the international treaties concerning child protection from online sexual abuse and exploitation, to ensure a complex approach that complies with international recommendations (Lanzarote Convention, Budapest Convention).

6. It is necessary to involve all public authorities and institutions responsible for the development of further policies in the field, to ensure the same level of understanding of the subject and taking on responsibilities by participating. At the same time, this would include promoting child online safety into the agendas of the Ministry of Health, Labour and Social Protection, the Ministry of Education, Culture and Research, Ministry of Internal Affairs, General Prosecutors' Office, Ministry of Economy and Infrastructure and other interested structures that have responsibilities in the field.

7. It is recommended to follow the international model of public policies in the field of child online safety – a plan that clearly states the goal of preventing and combating sexual abuse and exploitation, ensuring the protection of the physical, psychological and sexual well-being of the child in the online environment. Online security, which concerns the security of digital devices and information has to be approached separately in policies on cybersecurity or information security.

Operational recommendations

Following from the main findings and problem areas identified, it is recommended to take a complex approach to the risks that children are exposed to online, based on the following key-objectives:

1. Empowering children and developing resilience to online abuse

The Ministry of Education, Culture and Research should make sure that in the educational process, children are taught how to make informed decisions, avoid potential online risks and how to take response actions if faced with online abuse. In this context, it is necessary to:

- Revise the school curriculum and educational policies to integrate aspects of online safety in the activities with pupils of all ages. It is vital to ensure a clear delimitation between the aspects regarding the psycho-emotional wellbeing of the child in the online environment and the aspects concerning cybersecurity etc.
- Integrate child online safety into continuous teacher training programmes, in order to empower teachers to carry out educational activities with children on how to prevent online sexual abuse;
- Create and implement programmes that develop parental competencies on the benefits and risks of using ICT, focusing on educating children on safe behaviours online, solutions and support services available if facing abuse.

2. Improving the response of the judicial system to online sexual abuse and exploitation of children

The Ministry of Internal Affairs, Ministry of Justice, the General Prosecutors' Office and the General Police Inspectorate should ensure the adjustment of the legal framework to international standards and empowerment of the law enforcement agencies and judicial system, to make sure there is an adequate response to cases of online sexual abuse and exploitation. In this sense, it is necessary to:

Adjust the legal framework that criminalizes illegal actions of online sexual

abuse and exploitation according to the provisions of the Lanzarote Convention;

Adjust the legal framework that provides for the procedural measures of investigation and prosecution of crimes committed using ICT to the provisions of the Budapest Convention;

Develop guidelines for representatives of law enforcement agencies (policemen and prosecutors) on investigation and prosecution actions of crimes that represent online sexual abuse and exploitation, from the perspective child's right protection;

Develop and strengthen the scrutiny of illegal and harmful online content;

Professionally train the representatives of law enforcement agencies and representatives of the judicial system to adequately, and in the best interest of the child during the trial, identify, investigate and judge crimes of online sexual abuse and exploitation;

Maintain specialized structures within the Prosecutor's Office and among the police force responsible for the investigation and prosecution in cases of online sexual abuse and exploitation and ensure regular activities that would consolidate their capacities. Such an approach would ensure a focus on the victim's best interests and would comply with the international recommendations and best practices.

3. Provide support and assistance services for children-victims of online sexual abuse

The Ministry of Health, Labour and Social Protection and the Ministry of Education, Culture and Research should ensure the professional training of experts who are in contact with the child, so that they can identify and adequately intervene in cases of online abuse. In this sense, it is necessary to:

- Professionally train experts from the child protection system – how to evaluate the risk of online sexual abuse, what the intervention actions are, and how to provide assistance based on the identified needs;
- Develop the capacities of the experts who are in direct contact with children (teachers, school counsellors) – how to evaluate the risks that children are exposed to, how to identify signs of a potential abuse and what intervention actions should be undertaken;
- Develop institutional policies that promote online safety through a comprehensive approach, so that there is an efficient response procedure in place in cases of online abuse identified in the school, where the child has immediate access to specialized support and counselling services;
- Develop instructions for the experts in the child protection system and education system (social workers, teachers, school counsellors) on identifying and reporting cases of online sexual abuse of children to the police.

4. Research the latest tendencies in the field of online safety

The Ministry of Education, Culture and Research, the Information Society Development Institute but also other interested parties should take action in conducting research in the field of online safety, that would facilitate the development of policies in the field that would approach the following aspects:

- Evaluation of risks that children are exposed to online;
- Analysis of the vulnerability factors of children in the online environment and the educational measures to prevent these risks;
- Analysis of the abusers' behaviours in order to determine how they operate, to then find efficient measures of identification/investigation/prevention of these crimes based on the trends observed;

We recommend to follow international practices, which over the last 15 years have developed research that intends to improve the public policy framework in the field (EU Kids Online, Global Kids Online[49]); the internationally applied methodology, subjects studied and the ways in which these later help in the elaboration of policies in the field.

[49] https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online

References

1. Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, adopted by the Committee of Ministers on 27 September 2006 at the 974th meeting of the Ministers' Deputies, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805af669;
2. Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), adopted by the Committee of Ministers on 5 September 2001 at the 762nd meeting of the Ministers' Deputies, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804deb54;
3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children/*COM/2012/0196 final*/, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0196%3AFIN
4. Council of Europe Strategy for the Rights of the Child (2016-2021), available at Council of Europe Strategy for the Rights of the Child (2016-2021)
5. Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24190

6. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Strategy for a Better Internet for Children, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&from=ro

7. Recommendation CM/Rec(2018)7 of the Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, available at https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

8. Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, adopted by the Committee of Ministers on 21 November 2019 at the 1361st (Budget) meeting of the Minister's Deputies, available at https://library.parenthelp.eu/wp-content/uploads/2019/12/CoE-digital-citizenship-education-recommendations-CM_Rec201910E.pdf.

9. ITU, Guide to developing a national cybersecurity strategy, Strategic engagement in cybersecurity, available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

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

11. Government Decision no. 257 from 22.11.2018 on the approval of the Information Security Strategy for the RM for the years 2019-2024 and the Action Plan for its implementation, published on the 18.01.2019 in the 'Monitorul Oficial' journal no.13-21, art. 80

12. Law no. 299 from 21.12.2017 on the approval of the Cybersecurity concept of the RM

13. Government Decision no. 811 from 29.11.2015 regarding the National Cybersecurity Plan of the Republic of Moldova for the years 2016- 2020, published 13.11.2015 in the 'Monitorul Oficial' journal no. 306-310, art. 905.

14. Government Decision no. 212 from 05.04.2017 on approving the Action Plan regarding promoting safety of children and adolescents on the Internet for the years 2017-2020

15. Government Decision no. 857 from 31.10.2013 regarding the approval of the National Strategy for the Development of the Information Society "Digital Moldova 2020"

16. Report on the execution of the National cybersecurity plan of the Republic of Moldova for the years 2016-2020 during semester II of 2019, available at http://mei.gov.md/sites/default/files/raport_realizare_pnsc_sem_ii_2019_-_hg_811.pdf (Romanian)

17. Understanding cybercrime: phenomena, challenges and legal response, ITU, September 2012, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

18. WeProtect Global Alliance, Global Threat Assessment 2019, Working together to end the sexual exploitation of children online, available at https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef-23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf

19. The Better Internet for Kids Policy Map, Implementing the European Strategy for a Better Internet for Children in European Member States, March 2018, available at https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7.

20. Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 july 2018, adopted by the Cybercrime Convention Committee, Working group on other forms of online violence, especially against women and children, available at https://www.coe.int/en/web/cybercrime/-/t-cy-mapping-study-on-cyberviolence-recommendations

21. Child Sexual Abuse Material: Model legislation and Global review, ICMEC, 9th edition 2018, available at https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf

22. Statement of action by Governments to tackle online CSE: Abu Dhabi WeProtect Summit, 16-17 November 2015, available at https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e-8a4ec/1549388168335/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf

23. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, available at https://static1.squarespace.com/static/5630f-48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/We-PROTECT+Global+Alliance+Model+National+Response+Guidance.pdf

24. Our Strategy to End the Sexual Exploitation of Children Online, WePROTECT Global Alliance, July 2016, available at https://static1.squarespace.com/static/5630f-48de4b00a75476ecf0a/t/578408b5f7e0ab851b789e14/1479254482761/We-PROTECT+Global+Alliance+Strategy.pdf

25. The WeProtect Global Alliance, Working examples of model national response capabilities and implementation, available at https://www.end-violence.org/sites/default/files/paragraphs/download/WePROTECT%20Global%20Alliance.pdf

26. National Regulatory Agency for Electronic Communications and Information Technology, Annual Statistical Report, Developing electronic communications in the RM, available at https://www.anrceti.md/files/filefield/Anuar%20statistic%202019_22aprilie_2020.pdf (Romanian)

27. International Centre ,,La Strada Moldova", Child Online Safety, 2017, available at http://lastrada.md/files/resources/3/Siguranta_copiilor_pe_Internet__final.pdf (Romanian)

28. Factsheet Siguronline for 2019 available at http://lastrada.md/pic/uploaded/Siguronline%20Factsheet%202nd%20half%20of%202019.docx.pdf http://lastrada.md/pic/uploaded/CST%20factsheet%202nd%20half%20of%202019.docx.pdf

29. Factsheet Child Safeguarding Team for 2019, available at http://lastrada.md/pic/uploaded/CST%20factsheet%202nd%20half%20of%202019.docx.pdf

30. Factsheet Siguronline for the first half of 2020, available at http://lastrada.md/pic/uploaded/Siguronline%2520factsheet_1%2520sem._2020.pdf (Romanian)