ANALITICAL REPORT

Sofia, February 2025

Project: 101158515
"Digital Children: Protecting and Empowering Children in Digital Environment" - DIGITAL-2023-DEPLOY-04
Deliverable D5.1 – Analytical Report

Funded by the European Union. The views and opinions expressed are those of the author(s) alone and do not necessarily reflect those of the European Union or the European Executive Agency for Health and Digitalisation (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

CONTENTS

Project

I. Summary of the "Digital Children: Protecting and Empowering Children in Digital Environment" Project

ii. Digital Children Project and Work Package 5 from the Project implementation:

✓ SIC and the Project consortium

The project "Digital Children: Protecting and Empowering Children in Digital Environment" (hereinafter "Digital Children", "Project") is dedicated to the multifaceted challenges faced by children in the digital world not only in Bulgaria, but also throughout Europe. It is committed to increasing children's online safety by actively supporting the activities of the Bulgarian Safer Internet Center (SIC, "Center"), including the continued operation of the Centre's two key services, namely the Helpline for Online Safety of Children (the "Helpline") and the Hotline for Reporting Online Crimes against Children (the "Hotline").

11.02.2025 marked the 20th anniversary of the Center.

The SIC is the only structure of its kind in our country for the protection and support of Bulgarian children in the online space. The Helpline and Hotline adminitser record numbers of reports of child online abuse, and help thousands of parents and children with issues of online safety, harmful content, violence, etc. The Center is a trusted partner of the Cybercrime Directorate at the National Service for Combating Organized Crime, and at the international level – of the INHOPE and INSAFE networks, of Interpol, as well as of the large social platforms where children have profiles at large.

The SIC has a renewed consortium of organizations implementing the activities of the Digital Children project. Association "Parents", which was one of the founders of the Center in 2005, is the main coordinator, and the implementation of the activities of the Center is supported by the Bulgarian Association for Family Planning and Sexual Health (BASP), which is mainly engaged in large-scale training work under the Project, and by the National Network for Children (NNC), responsible for communication and advocacy activities (pursuant to Work Package No. 5 of Annex No. 1 to the project administrative agreement).

The NNC is the largest association of civil organizations and experts in Bulgaria (over 130), working with and for children and families. Among the key guiding principles of the organization are the promotion, protection and monitoring of the rights of the child, in accordance with the UN Convention on the Rights of the Child. The NNC believes that all policies and practices, which directly or indirectly affect children, ought to be designed, implemented and monitored taking into account the principle of the best interests of the child and with the active participation of children themselves.

✓ Main objectives of Work Package 5 the Project implementation and of the Analaytical Report. Objectives and scope of the Report

Work Package 5, entitled "National Communication, Collaboration and Advocacy", aims to implement advocacy and continuous awareness raising through the following activities:

1). conducting targeted communication and information campaigns and events;

2). development and distribution of resources and tools, based on needs assessments and findings from the work of the Hotline and Helpline;

3). advocacy for regulatory changes at the level of EU law and national legislation - with the aim of adopting effective legislation aimed at preventing, detecting and punishing the sexual exploitation of children committed online;

4). expert assistance in the monitoring and implementation of national policies aimed at the safety of children online, and at increasing digital media literacy, etc.

The present Analytical Report addresses the objectives of points No. 3 and No. 4 above. The Report analyzes the legal framework and provides a structural and functional assessment of existing systems aimed at ensuring children's online safety. It systematizes and advances recommendations for policy improvement and systemic changes needed to ensure the right of children to safely benefit from the opportunities of the digital world. The findings and recommendations within this Analytical Report are premised on the long-term research and advocacy work of the National Network for Children and its members and partners; the experience of the consortium operating the SIC; the ongoing analysis and monitoring of legislation and policies during the project implementation; and active communication with institutions, security authorities, the Cybercrime Directorate at the National Service for Combating Organized Crime, *et alia.*

II. Online safety of children in Bulgaria and globally at the beginning of 2025

At the beginning of 2025 the SIC reported a record number of cases processed through the Hotline – 1,749,747 reports, over 95% of which concerned online sexual exploitation of minors.

70,268 alerts have been reviewed and referred directly to the Cybercrime Directorate of the National Service for Combating Organized Crime, a trusted partner of the Centre.

This is the highest number of alerts processed in the 20-year history of the Center within one calendar year. The reasons for the drastic increase in cases are many and diverse (including the high operational efficiency of the SIC and the signal processing system optimization carried out in 2024; additional images and links found during inspections of illegally hosted content - each of which is reported separately; increased public recognition and trust in the Center, etc.), but it is definitely further indicative of the growing number, tools and scope of online abuse against children both in our country and globally.

Against this background, according to Eurostat data, only 58% of young people aged 16–24 in Bulgaria have basic or good digital skills, which is significantly below the EU average of 80%. 1 out of every 7 children in Bulgaria reports that they have been a victim of online bullying and stalking in social networks. According to UNICEF data, every second child (47%) in Bulgaria has suffered some form of violence. Within the emotional abuse section of the survey, children and young people are asked about online bullying and abuse, with at least 1 in 10 children and young people (10.9%) reporting experiencing online bullying. The place most frequently cited by children and young people for online bullying was social media websites - 60.7%, followed by online gaming platforms (17.12%), and chat apps (16.3%).

Data from an ECPAT and NSPCC survey conducted ahead of the EU Council vote on the Child Sexual Abuse Regulation shows that a total of 95% of Europeans want new regulations to effectively ensure children's online safety. This survey was conducted amongst 26,000 adults in the 27 Member States. In Bulgaria, the participants were 1050. According to Eurobarometer data, 71% of Europeans are ready to make some compromise with their personal lives online if this would help protect children from potential sexual abuse and exploitation online. Over 70% support detection and removal of child sexual abuse material on end-to-end encrypted platforms.

In 2022-2024, according to Europol's report on serious organized cybercrime, the latter has increased by more than 300% not only in Bulgaria and Europe, but also around the globe, and children are among the most vulnerable to cybercrime.

The alarming trend of increased frequency and variety of tools for online exploitation of children in Bulgaria corresponds to the rapid global increase. During the round table on the topic of "Combating online

sexual abuse of children: Trends, Possible Solutions, and Challenges" of the SIC under the Digital Children Project on 09.01.2025, hosted by the SACP in partnership with the International Association of Internet Hotlines INHOPE, the NNC presented the following global trends, systematized based on the experience of the Network's participation in ECPAT International exchange initiatives and in the WeProtect Global Alliance's 2024 Global Summit, namely:

- More than 300 million children annually become victims of online sexual abuse and exploitation;
- Financial sexual extortion and coercion of children, along with generation through artificial intelligence (AI) of sexual abuse material, are forms of abuse with an ever-widening scope;
- Resources and support for the non-governmental sector involved in the fight against violence and sexual exploitation of children are increasingly limited;
- 360% increase in 7-10 year olds' self-generated images of nudity from 2020 to 2022 alone (Internet Watch Foundation);
- Cases of mental suffering and suicide attempts of children are increasing, where child victims created an emotional connection with a generative AI chatbot imitating a partner / close friend;
- Globally, the main territory of abusers is online gaming platforms, where children become victims of violence in an average of 19 seconds from the moment of the first personal message;
- The Dark Web continues to be a "reservoir" for child sexual exploitation content; according to the US Department of Justice, a sexual abuse post on a Dark Web forum was viewed 1,025,680 times in 47 days (21,822 views per day) prior to being deleted;
- In a survey among Dark Web users, 39% responded that they had witnessed a live broadcast of child sexual exploitation;
- Tools for masking sexually exploitative content are increasing – e.g. through steganography (data hidden inside an image, audio file or other media format), by editing the image so the latter resembles AI-generated, etc.;
- Exponentially increasing cases of online violence and harassment between children;
- Cases of abuse in social networks and chat applications continue to be facilitated due to the lack of safety-by-design algorithms, policies and rules.

Given the described trends at the national and international level, it is particularly necessary for a comprehensive assessment of the legal framework, policies and practices in Bulgaria currently addressing these problems to be carried out.

III. National laws and regulations related to the online safety of children

Child Protection Act

The Child Protection Act (CPA) does not contain express provisions that specifically refer to the protection of children from abuse in the online environment. The CPA regulates the rights, measures and authorities for the protection of children in Bulgaria, based on principles such as respect for the personality of the child, ensuring the best interests and providing special protection for children at risk. The Act guarantees the right of every child to protection against physical, mental, sexual, etc. violence, as well as against use for prostitution, begging and distribution of pornographic material. The CPA provides a general regime for the protection of children, the measures in which can be applied in the context of abuse in a digital environment.

Specifically, the following provisions are relevant to children's online safety:

- Protection against violence and exploitation (Article 11) – this provision undoubtedly has applicability to harassment, abuse and sexual exploitation of children in a digital environment;
- Protection of the child's personality and confidentiality of personal information (Art. 11a and Art. 16) – this provision contains a prohibition of distribution of information about children without their parental (or the protection authority's) consent, which is also related to online privacy;
- Information and counseling (Article 13) – children have the right to access information and counseling, including concerning the risks in the Internet space;
- Obligation to cooperate (Article 7) – all citizens and institutions are obliged to notify the competent authorities in case of suspicion of abuse against a child, including on the Internet;
- Coordination mechanism in case of violence (Article 36d) - to ensure the protection of a child at risk or a victim of violence or exploitation, the Social Assistance Directorate establishes a multidisciplinary team, the members of which work together under a joint action plan aimed at protecting the child or preventing violence;
- Protection of children victims of violence or exploitation (Article 36e) - the protection of a child at risk or a victim of violence or exploitation is undertaken after the investigation of the case by the multidisciplinary team and according to the action plan proposed by the leading expert. The action plan contains health, social and educational measures for the prevention of violence or for the recovery of the child;
- The legal definition of "child at risk" under § 1, item 11, letter "b" from the Additional Provisions of the CPA covers cases of child victims of abuse, violence, exploitation or any other inhumane or degrading treatment or punishment within or outside the family, whilst in turn letter "c" of the cited provision covers the cases of children for whom there is a danger of potential damage to their physical, mental, moral, intellectual and social development, i.e. this provision also covers abuse (or the danger of such) within a digital environment.

The SACP, the Ministry of Internal Affairs and social workers have the main responsibility for the prevention and fight against violence, including in an online environment, assisted by NGOs, educational institutions and the private sector.

The CPA and the by-laws ought to be complemented with additional measures for prevention, monitoring and sanctions against digital risks for children. In this sense, by analogy with the paradigm of Art. 5b "Specialized protection of children in public spaces", a new provision with entitled "Specialized protection of children in the online environment" could be adopted, whilst the terms and conditions for guaranteeing this type of specialized protection are determined in detail through a special ordinance of the Council of Ministers, issued on the proposal of departmental institutions such as the Ministry of Labor and Social Policy, the Ministry of the Interior, the SACP (see Article 5b, Paragraph 2 of the CPA).

Further, the recommendations relevant to the better functioning of the multidisciplinary teams at the local level on the implementation of the Coordination Mechanism in cases of violence (Article 36d) are also valid for the teams' work on cases of abuse and risks in the online environment, namely:

- provision of the necessary additional financial, technical and human resources for the more effective work of the teams;
- establishment of a unified information system in which it is clear what goals and activities all involved institutions have set for implementation;

- clearly defining the roles and responsibilities of the teams and avoiding turnover and inconsistency;
- provision of detailed methodological guidelines for work on cases of online violence and exploitation;
- conducting regular joint trainings and working meetings of the representatives of the various institutions for work under the Coordination Mechanism, incl. on the subject of the specificities of online abuse.

The analysis of the CPA should not fail to highlight the deficiencies of the child protection system. The sole operational unit for the implementation of child protection measures presently are the protection departments of the Social Assistance Directorates, and there are still no requirements for specialized higher education and / or professional standards in the selection of employees, there is also a lack of quality training and resource provision, as well as no adequate subsequent training, supervision, and certification. The workload of the employees of the Child Protection units to the Social Assistance Directorates in too many places remains unbearably high, which leads to turnover and to the impossibility of ensuring the necessary quality.

In 2024, a Strategy for the Development of Human Resources in the Social Sphere (2024-2030) was adopted, and the analysis of the situation therein clearly shows the need for urgent investments in the system.

Criminal Code (CC) and Criminal Procedure Code (CPC)

In the catalog of criminal acts set out in the Bulgarian Criminal Code, there are crimes with the subject of abuse against children in the online environment, including:

- Fornication (Art. 149 *et seq.* of the CC) - whoever commits an act with the aim of arousing or satisfying sexual desire without intercourse in relation to a person under the age of 14, shall be punished for fornication with deprivation of liberty from one to six years;
- Incitement and coercion (Art. 155a - Art. 155c of the CC) - whoever, through information or communication technology or in any other way, provides or collects information about a person under the age of 18 in order to establish contact with them for committing a lewd act, sexual intercourse, prostitution, to create pornographic material or to participate in a pornographic performance, is punishable by imprisonment of three to ten years and a fine of ten thousand to twenty thousand BGN. The punishment is also imposed on the one who, through information or communication technology or in any other way, establishes contact with a person who has not reached the age of 14, for the purpose of committing fornication, intercourse, sexual intercourse, to create pornographic material or to participate in a pornographic performance. In 2024 (State Gazette, issue No. 39) an additional qualifying provision was adopted, which stipulates that when the act has had significant harmful consequences for the physical, mental or moral development of the victim, the penalty is imprisonment from five to twelve years.
- The norm of Art. 155b provides that whoever induces a person under the age of 14 to observe actual, virtual or simulated sexual intercourse between persons of the same or different sex or lascivious display of human genitals, sodomy, masturbation, sexual sadism or masochism, shall be punished with imprisonment from three to ten years. Whoever induces a person under the age of 14 to participate in actual, virtual or simulated sexual intercourse between persons of the same or different sex or lascivious display of human genitals, sodomy, masturbation, sexual sadism or

masochism shall be punished by imprisonment for five to ten years.

- In Art. 155c it is regulated that whoever, through the use of force or coercion, or by using a position of dependence or supervision induces a minor to observe an actual, virtual or simulated act of fornication, copulation, sexual intercourse, including sodomy, masturbation, sexual sadism or masochism, as well as lascivious display of human genitals, shall be punished by imprisonment for three to seven years. Whoever, by the use of force or threats, or by the use of a position of dependence or supervision, induces a minor to participate in an actual, virtual or simulated act of fornication, copulation, sexual intercourse, including sodomy, masturbation, sexual sadism or masochism, as well as in the lascivious display of human genitals, shall be punished by imprisonment for three to ten years.
- Art. 158a of the CC regulates the criminal acts incriminating the recruitment, assistance or use of a person under the age of 18, or a group of such persons, to participate in the so-called pornographic performance;
- Pornographic materials with persons who are victims of sexual exploitation (Article 159) – the cited norm stipulates that whoever creates, exposes, presents, broadcasts, offers, sells, rents or otherwise distributes pornographic material, shall be punished with imprisonment for up to one year and a imposed a fine of one thousand to three thousand BGN. Whoever exhibits, presents, offers, sells, rents or otherwise distributes pornographic material to a person under the age of 16 shall be punished by imprisonment for up to six years and imposed a fine of up to five thousand BGN. For this criminal act, the punishment is imprisonment from three to six years and a fine of up to ten thousand BGN, when a person under the age of 18, or a person who appears to be of such age, has been used to create the pornographic material (Article 159, Paragraph 4, Item 1 of the CC). Whoever keeps or procures for themselves or for another, through information or communication technology or in any other way, pornographic material, for the creation of which a person under the age of 18 was used, or a person who appears to be of such age, shall be punished by imprisonment for up to five years and a fine of up to ten thousand BGN.
- "Pornographic material" (the legal definition is contained in Art. 93, para. 1, item 28) is material prepared in any way, indecent, unacceptable or incompatible with public morals, the content of which depicts real or simulated fornication, copulation, sexual intercourse, including sodomy, masturbation, sexual sadism or masochism, as well as lascivious display of the genitals of person. "Pornographic performance" (the legal definition is contained in Art. 93, para. 1, item 30) is a live or real-time performance in front of another of a lascivious display of the genitals of a person under the age of 18, or the participation of such a person in a real or simulated lewd act, copulation, sexual intercourse, including sodomy, masturbation, sexual sadism or masochism;
- Other legal definitions related to online abuse against children are systematically included in the provision of Art. 93 of the CC - including definition of "information system" (paragraph 1, item 21), "computer data" (item 22), "provider of computer-information services" (item 23), etc.

The overall assessment of the Project team, based on the expert dialogue with the Cybercrime Directorate at the National Service for Combating Organized Crime, is that the punishments for these types of crimes, provided for in the Criminal Code, are consistent with the severity of the criminal acts committed, and that the main issues, as discussed below, arise from slowness and other vices of procedural and investigative actions, from the lack of sensitivity regarding the significance of acts in a digital environment on the part of prosecutors and judges throughout the country, etc.

As discussed below, the transposition of the EU Directive on Domestic Violence (the transposition term is until 13.06.2027) will require the expansion of the catalog of crimes against the individual committed online - including with the explicit criminalization in the Penal Code of the manipulation of intimate material generated by AI, the so-called cyberflashing, doxxing, etc.

Regarding the procedural provisions in the Code of Criminal Procedure (CPC), the regulation of procedural and investigative actions on cybercrimes and access to electronic evidence is considered adequate (computer service providers are obliged to assist investigative bodies in collecting electronic evidence; special intelligence tools can be used in serious intentional crimes, including cybercrimes), along with the procedural guarantees for child victims of crimes and the protective norms ensuring protection from secondary victimization.

The overall assessment of the Project team is that the legal framework is adequate, yet there are still gaps, whilst practice shows significant procedural and institutional challenges in detecting and punishing online abuse, caused by the following:

- The criminal process in relation to online abuse remains too formal, and the practice of criminal bodies is often controversial. For instance, some courts recognize a certain type of evidence collected by electronic means, while others do not, due to the lack of any uniform methodological framework;
- In the Criminal Procedure Code, there is no legally regulated mechanism for informing the police structure that conducted the inspection, in the presence of a refusal to initiate criminal proceedings. This makes it difficult for experts to appeal the refusals before a higher authority;
- Sometimes, at the discretion of the supervising prosecutor, they may not exercise their right to order the detention of the perpetrator for 72 hours, according to the order of the CPC, which presupposes the possibility that the perpetrators destroy electronic evidence;
- The CPC contains definition of "computer information systems", which is too general, without any unified methodology for differentiating cyber content with abuse of and over children, sexual content, etc. and without a mechanism in place to avoid the controversial practice of supervising prosecutors and magistrates;
- Since such crimes are committed online, there is often uncertainty about where to file the criminal charges. The lack of established judicial practice and specific legal norms sometimes prevents the initiation of pre-trial proceedings in the district where the perpetrator is located;
- Still quite a few prosecutors and judges across the country do not have enough in-depth knowledge and sensitivity regarding online abuse of children and do not pay due attention to these cases.

Act on Assistance and Financial Compensation of Crime Victims (AAFCCV)

The Act on Assistance and Financial Compensation of Crime Victims (AAFCCV) regulates the terms and conditions for assistance and financial compensation from the State to Bulgarian citizens or citizens of EU Member States who have suffered from crimes. Through amendments adopted by the National Assembly in 2023, a new Chapter Two "a" was incorporated in the AAFCCV, through which the list of procedural rights of the victims, incl. children victims and/or witnesses of crimes, has expanded.

Additional provisions aimed at ensuring more effective justice for child victims were added to it, including, as follows: 1). crime victims have the right to an individual assessment; 2). when the victim is a child, it is necessarily assumed that there are specific needs for protection, and the body performing the assessment immediately notifies the Child Protection Department at the Social Assistance Directorate at the child's

current or permanent address; 3). the authorities of the Ministry of Internal Affairs or the investigators who established initial contact with the victim carry out the individual assessment without undue delay on the basis of a conversation with the person. They may seek assistance from a psychologist, physician or other appropriate professional at their discretion; 4); a specific procedure for conducting an interrogation of child witnesses with a specific need for protection is in place – with the child being interviewed in the presence of a pedagogue or psychologist, and if necessary - in the presence of the parent, guardian or custodian.

The lack of opportunity for victim support organizations that have established initial contact with the victim to carry out individual assessments is evaluated negatively. The burden on the bodies of the Ministry of Internal Affairs with the complex activity of carrying out the individual assessment of the child victims implies a solid special training of police officers and investigators, which is currently not carried out everywhere. Further, practice shows that in many places there is ignorance of the new regulation and/or blanket use of the latter.

- **Act on Electronic Communications**

The Act on Electronic Communications (AEC) governs public relations relating to the transmission, broadcasting and reception of electronic communications by various technologies (wire, radio wave, optical or electromagnetic means). The main objectives of the Act include, as follows:

- ensuring the security and accessibility of electronic communication networks;
- development of competition and consumer protection;
- ensuring transparency in the provision of services;
- protection of national security and personal data of citizens.

Although the AEC does not emphasize the safety of children online, several key provisions relate to the protection of children, namely:

- The Act guarantees the inviolability of electronic communications, including the content of communications and personal data of users. This creates a legal basis for protecting children from abuse such as cyberbullying, extortion and other forms of online harm;
- Internet service providers have an obligation to cooperate with government authorities to limit access to content that endangers children, including child sexual abuse material. However, these measures are not detailed and need to be further specified through additional regulation;
- The AEC provides for mechanisms for law enforcement to access traffic data in investigations related to crimes against children on the Internet. This allows more effective identification and punishment of perpetrators of online abuse. There is a connection with the special provision of Art. 159a of the CPC, which sets out in a separate norm the obligation to provide data by the providers of public electronic communication networks and/or services. Service providers ought to provide data created in the course of their activity at the request of the court in the judicial proceedings or on the basis of a reasoned order of a judge of the relevant court of first instance, issued at the request of the supervising prosecutor in the pre-trial proceedings.

The main institutions responsible for the implementation of the Act and the protection of children in the digital environment are:

- Communications Regulatory Commission (CRCt) – monitors compliance with the legislation by Internet providers and telecommunications operators;

- Ministry of Internal Affairs (MIA) – responsible for the investigation of cybercrimes and assistance in the detection of online threats to children;
- State Agency for Child Protection (SACP) – has a role in developing online safety policies.

The Act on Electronic Communications does not contain special norms for the protection of children in the digital space. Among the main shortcomings of the latter are: lack of sufficiently specified and comprehensive obligations for Internet platforms; unclear and cumbersome content control mechanisms (blocking of harmful content depends on court orders, which delays the response of the authorities); limited coordination between institutions – there is no clear mechanism for coordinating actions between the CRCt, the Ministry of the Interior and the SACP regarding children's digital safety. Accordingly, it is necessary to introduce additional provisions on the obligations of online platforms, fast blocking of harmful content and better coordination between institutions.

In this regard, as discussed below, the draft Act amending the Act on Electronic Communications (AEC) (approved by Decision No. 829 of the Council of Ministers of 2024) aims to improve the AEC by ensuring the full implementation of the requirements of Regulation (EU) 2022/2065 of the EU.

Act on Protection of Personal Data

The Act on Protection of Personal Data (APPD) regulates the processing and protection of personal data of individuals in Bulgaria, introducing the mechanisms of the EU General Data Protection Regulation (GDPR). Children are considered a vulnerable group, and the APPD sets out special requirements for the processing of their personal data:

- Minimum age for consent to data processing - Art. 25c states that the processing of personal data of a child under the age of 14 is only legal should consent be given by a parent or guardian. This applies for digital services and social networks;
- Restrictions on disclosure of personal data - the distribution of personal data of children in the public space, including on the Internet, is limited, unless there is the express consent of the parent or if this is provided by law.

The control over the protection of personal data, including that of children, is carried out by the Commission for the Protection of Personal Data (CPPD), which possesses the authority to:

- Conduct investigations and impose sanctions on administrators who do not comply with the law;
- Develop guidelines and recommendations for secure processing of children's data;
- Work in cooperation with international authorities for the protection of personal data.

The APPD establishes a robust regulatory framework for the protection of personal data, yet gaps are reported in relation to the safety of children online, including:

- Lack of clear and reliable age verification mechanisms when registering in social networks and using digital services;
- Ambiguity regarding the regime of obligations of platforms and internet providers to take and report specific measures to protect children's personal data;
- Limited opportunities to quickly react to breaches such as data leaks or online abuse of personal

information.

The APPD thus needs additional provisions and mechanisms to more effectively enforce these protective norms.

Act on Cybersecurity. Cybercrime Directorate to the National Service for Combating Organized Crime

The Act on Cybersecurity regulates the activities of: 1). the organization, management and control of cyber security, incl. activities and projects on cyber defense and countering cybercrime; 2). taking the necessary measures to achieve a high general level of network and information security. It also defines the powers and functions of the competent authorities in the field of cyber security. The Act thus provides a framework for coordinated action between institutions and the private sector to effectively protect children from online threats, including sexual exploitation, fraud and online harassment.

The Ministry of Internal Affairs is the main body responsible for combating cybercrime, and the National Service for Combating Organized Crime operates within the latter's structure. A specialized Cybercrime Center operates within this Directorate, which investigates and documents computer crimes, including those directed against children (Article 14, Paragraph 2 of the Act on Cybersecurity). In the event of a threat or cyber-attack targeting children being identified, the National Service for Combating Organized Crime has the power to take investigative action, including investigating and stopping malicious online activities. Thus, when cases of online abuse, illegal content and malicious behavior are detected, the competent authorities are the Directorate of Social Assistance at the place of residence of the child and the specialized Cybercrime Directorate of the National Service for Combating Organized Crime.

In addition to the normative basis laid out within the Act on Cybersecurity, it should be stated that the Cybercrime Directorate performs tasks of countering organized criminal groups and individuals carrying out, among other things, production, possession and distribution of pornographic materials with minors.

Part of the functional competences of the Directorate is the work in the operative line of "targeting illegal content on the Internet". The employees of the Directorate are competent to take action upon receiving data on sexual exploitation of children on the Internet. Software products are used to monitor specialized child sexual exploitation file sharing networks. Internet traffic is monitored 24/7 in Bulgaria, and over 85% of it is filtered for illegal content. Both intentional and accidental access (especially by children) to sites with pornographic material is restricted. Every month, Interpol provides a list of "Worst of" websites based on our country's Internet space, containing illegal content, and the National Service for Combating Organized Crime blocks the sites and redirects their users to a stop page with information about the illegality of the relevant act.

An opportunity is provided for every citizen to submit a direct report to the National Service for Combating Organized Crime on the pages of www.cybercrime.bg and www.gdbop.bg, administered by experts of the Directorate. Prevention is an important part of the activity of the specialized Directorate. In order to reduce the number of child victims of sexual exploitation, trainings and seminars are periodically developed and implemented with students, parents and teachers, including in partnership with the National Safer Internet Center.

In this sense, the only identified recommendation herein is for the provision of more human and technical resources to support the activities of the Cybercrime Directorate.

Act on the Ministry of Internal Affairs

The Act on the Ministry of Internal Affairs regulates the principles, functions and activities of the Ministry, and its main purpose is to protect the rights and freedoms of citizens, combat crime, protect public order and national security. The Act contains provisions directly or indirectly affecting the protection of children in the digital environment:

- Operational-investigative activities (Articles 8 - 13) - the Ministry of Internal Affairs has the authority to carry out operational-investigative activity against crimes, including those committed in a digital environment. This includes hunting down individuals who commit crimes against children online, such as sexual exploitation, cyberbullying and other forms of online violence. The Act provides for the use of special intelligence tools and methods, including operational deployment and controlled delivery, that can be used to detect Internet crimes;
- Information activity (art. 18 - 25) - the Ministry of Internal Affairs collects, processes and provides information that can be used to protect children in a digital environment. This includes information about cybercrimes committed against children, as well as details regarding the perpetrators;
- Prevention activity (Article 30a) - the Ministry of Internal Affairs carries out activities aimed at preventing crimes, incl. those performed in a digital environment. This includes measures to establish and eliminate the causes and conditions for committing crimes against children online.

The Act does not contain specific provisions aimed at protecting children from online risks such as cyberbullying, sexual exploitation, extortion and other forms of violence in the digital environment. The regulation in the Act on Ministry of Internal Affairs is assessed as good and harmonized both with EU law and with relevant national legislative acts such as CPC and Act on Cybersecurity.

Notwithstanding, the Project team found gaps in the implementation of the provisions of the Act on Ministry of Internal Affairs in practice. For instance, once individual cases of online crimes against children are promptly reported by the Cybercrime Directorate to the relevant prosecutor's office, sometimes at the discretion of the supervising prosecutor, despite the specifics of the committed criminal act and contrary to the norm of Art. 39, para. 2, item 3 of the Act on Ministry of Internal Affairs, the conduct of procedural and investigative actions is assigned to another structure in the Ministry of Internal Affairs. This leads to continued work on the case by staff who do not have the necessary practical knowledge and technical competence.

IV. National strategies and policies for child protection in the digital environment

Draft National Strategy for the Child (2024 – 2030) – approved by the National Council for Child Protection at the SACP on 01.03.2024

As of February 2025, Bulgaria has been without an adopted National Strategy for the Child for the sixth consecutive calendar year, in violation of Art. 1, para. 3 of the CPA, pursuant to which the state policy for child protection is implemented on the basis of a National Strategy for the Child, adopted by the Parliament on the proposal of the Council of Ministers.

In 2023 – 2024, the SACP and an interdepartmental working group at the Agency prepared a new Draft of the National Strategy for the Child (2024 – 2030), in which the protection of children from online abuse is laid out in a key thematic section. Subsequently, within the 50th anniversary meeting of the National Council for Child Protection, held on 01.03.2024, the Council unanimously adopted the Draft National Strategy for the Child (2024 – 2030).

Despite this progress, there is no public discussion on the Strategy initiated by the current regular cabinet;

an explanatory campaign dedicated to the framework documents has not been conducted or planned, while the Strategy approved by the National Council for Child Protection is not even available on the SACP website, which severely limits opportunities for public participation and expert debate.

The NNC has been systematically advocating for years for the adoption of this much-needed framework document outlining holistic policies for children and families, incl. of intersectoral interaction in guaranteeing the rights and best interests of every child. Despite what has been achieved so far, the lack of political will to meaningfully advance the process of finalization (including an upgrade in the thematic section dedicated to online safety) and adoption of the Strategy remains a serious risk, which requires increased advocacy efforts and civil pressure on the responsible institutions.

National Program for the Prevention of Violence and Abuse of Children (2023 – 2026)

At the beginning of 2023, the Council of Ministers adopted the National Program for the Prevention of Violence and Abuse of Children (2023-2026) and an Action Plan for its implementation for the period of 2023-2024.

The National Program and the Action Plan address the problem of online abuse against children and provide measures and activities to respond to cyberbullying, sexual exploitation and other forms of violence against children on the Internet. For instance, Operational Objective No. 5 of the Plan concerns guaranteeing the right to protection of children from violence through information and communication technologies.

This goal includes the following sub-goals, as follows:

- **5.1.** Developing digital-media literacy of students in classes and extracurricular activities, incl. through implementing digital innovations and platforms for the development of digital-media literacy;
- **5.2.** Receiving and processing reports of online child abuse through the National Safer Internet Centre's Hotline;
- **5.3.** Conducting trainings for students of all educational levels on topics related to online risks such as online harassment, sexting, online sexual exploitation, sextortion, online strangers, security and hacked profiles;
- **5.4.** Conducting the training program "Cyber Scouts" throughout schools in Bulgaria;
- **5.5.** Conducting a campaign to increase the awareness of parents, teachers and professionals regarding online risks and the prevention of online violence.

The SIC is named as the responsible institution in the Action Plan for these functions, which is indicative of the value of the Center's work.

At the same time, this underlines the unacceptable current situation in which the Center implements State policies and commitments of Bulgaria under several EU directives and international conventions, is subject to assignment of responsibilities under national framework documents and action plans, yet continues to have no support from the State and to rely on donations from companies and limited project support from the EU.

Moreover, the mentioned strategic documents are criticized due to the lack of concreteness in the indicators and of clear links between objectives, measures and results.

Currently (February 2025), interdepartmental work is being carried out on the drafting of an Action Plan for

2025-2026, under the coordination of the SACP, with the project consortium under Digital Children advocating for the clarification of the goals (strategic and operational) and the measures regarding online safety, as well as for the Plan to be structured in view of the results already achieved during the implementation of the previous plan.

V. Compatibility of legislation and policies with international standards and with the law of the European Union:

i. UN Convention on the Rights of the Child. General Comment No. 25 of the United Nations Committee on the Rights of the Child

The UN Convention on the Rights of the Child, adopted in 1989 and ratified by Bulgaria in 1991, is the most widely ratified international treaty in the field of human rights. It affirms the basic rights of all children, incl. the right to life, development, protection from violence and participation in public life. The Convention obliges states to ensure the best interests of the child in all policies and decisions that affect children. It creates an international framework for the protection of children and the promotion of their rights. Many of the guiding principles enshrined in the Convention can be applied to children's digital safety issues.

Thus, Art. 16 provides for protection against unlawful interference with a child's privacy, which can be applied to an online environment; Art. 17 recognizes the important role of the mass media and promotes children's access to relevant information; Art. 19 obliges states to take all necessary measures to protect children from all forms of violence, including psychological harassment and abuse; Art. 28 and Art. 29 guarantee the right to education and the preparation of the child for an active and informed life in society (in the modern context this inevitably includes training in digital literacy, cyber security and critical thinking in an online environment); Art. 34 requires states to protect children from sexual exploitation; and the general norm of Art. 36, in turn, proclaims the protection of children against all other forms of exploitation affecting in any aspect the welfare of the child.

In addition, the UN Committee on the Rights of the Child's General Comment No. 25 (2021) on children's rights in the digital environment is rather relevant herein.

The Committee on the Rights of the Child is a body established under the CRC with a mandate to monitor the implementation of the Convention and its Optional Protocols by States Parties. The Committee issues general comments to interpret and clarify how children's rights should be guaranteed in the context of various social, economic and technological changes.

General Comment No. 25 (2021) focuses on the rights of children in the digital environment, clarifying how States should implement the Convention in light of the challenges and opportunities that digitization brings. The document emphasizes that the digital environment affects almost all aspects of children's lives and that access to digital technologies is inextricably linked to the exercise of the full catalog of children's civil, political, social, cultural and economic rights. Although digital technologies can improve children's access to education, information and services, they also pose severe risks, including from exploitation, violation of personal space, discrimination and unequal access to digital resources.

General Comment No. 25 highlights four main principles that States should respect in the regulation of the digital environment, namely: non-discrimination, guaranteeing the best interests of the child, the right to life, survival and development, as well as the right of children to participate in the processes affecting their future. Special attention is paid to the circumstance that the digital environment was not originally designed for children, yet they increasingly interact with it, which requires specific regulatory measures to protect their rights.

Among the Committee's key recommendations is that States adopt legislation, which integrates child protection into digital environment policies, incl. measures against online exploitation, violence and misinformation. National policies should ensure that children have safe and equal access to the Internet and digital technologies, avoiding the deepening of social and economic inequalities.

The Committee also recommends greater involvement of technology companies in efforts to protect children, by applying safeguarding principles as early as the design stage of digital platforms. General Comment No. 25 emphasizes that States bear the primary responsibility for protecting children in the digital environment, but also calls for joint efforts on behalf of the private sector, civil society and international organizations to build a safe and inclusive digital space for all children.

ii. Convention of the Council of Europe on the Protection of Children against Sexual Exploitation and Sexual Violence

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, 2007) is a legally binding international document that obliges states to criminalize all forms of sexual abuse of children, including those committed through the Internet and digital technologies. The Convention emphasizes that the increasing use of information and communication technologies (ICTs) facilitates the dissemination of child sexual exploitation material and creates new challenges for prevention and prosecution.

Art. 20 of the Convention provides for the adoption of mandatory criminal provisions against:

- Production, distribution, offering and transmission of materials with sexual exploitation of children;
- Conscious access to material with sexual exploitation of children through ICTs. Child pornography (*an anachronistic term – author's note*) is defined as any visual depiction of a child engaged in sexual acts, including simulated or digitally generated images.

The Convention requires States to introduce:

- Specialized procedures for investigating crimes, incl. mechanisms to analyze materials distributed through ICTs;
- Cooperation with the private sector – telecommunications operators, Internet providers and digital platforms should implement policies to prevent and report sexual exploitation;
- Victim protection through hotlines and psychological support for children affected by online violence.

The Convention promotes cooperation between States in the investigation and punishment of cross-border cases, including through the exchange of information and the extradition of perpetrators. Thus, the Lanzarote Convention outlines a solid legal framework to combat the online sexual exploitation of children. Its successful implementation depends on effective cooperation between state institutions, the technology sector and civil society. Bulgaria, a party to the Convention, should ensure its strict implementation by strengthening the monitoring of digital platforms.

iii. Directive 2011/93/EC on Combating Sexual Violence and Sexual Exploitation of Children, as well as Child Pornography

Directive 2011/93/EC on Combating Sexual Violence and Sexual Exploitation of Children, as well as Child Pornography is the EU's main legal instrument for protecting children from this type of serious crime. The Directive replaces Framework Decision 2004/68/JHA and introduces stricter criminal law provisions, enhanced victim support measures and mechanisms for international cooperation. In the context of the

online safety of children, the directive emphasizes the prosecution of crimes committed via the Internet, such as child pornography, establishing contact with children for sexual purposes (grooming) and illegal access to material containing the sexual exploitation of children.

The Directive obliges member states to criminalize all forms of child sexual exploitation, including:

- Creation, distribution and storage of pornographic materials with the involvement of children (Article 5);
- Conscious access to child pornography via the Internet (Article 5, Paragraph 3);
- Possession and acquisition of such materials (Article 5, Paragraph 2).

These provisions reinforce the commitment of Member States to enhance measures to investigate and prosecute crimes related to the online distribution of child pornography. The Directive introduces the criminalization of the practice of establishing contact with children for sexual purposes through internet platforms, social networks and communication applications (Article 6). This offense covers an offer by an adult to meet a child with the intention of sexual exploitation.

The Directive encourages Member States to take effective measures to remove or block access to websites containing child sexual exploitation material, especially where the servers are located in third countries (Article 25). States are encouraged to cooperate with ISPs and the technology sector to develop mechanisms to filter and remove illegal content.

Although the Directive does not provide specific obligations for social networks and technology companies, it emphasizes the need for the private sector to actively participate in the prevention and reporting of crimes against children on the Internet (Article 24). Telecommunications companies and online platforms should report cases of child pornography distribution. Notwithstanding, the lack of a mandatory mechanism for accountability of the private sector to national authorities in terms of security, outlined by the Directive, is considered a minus.

The Directive requires Member States to guarantee free legal and psychological support for child victims (Articles 16-20). Victims of online sexual exploitation should have access to specialized social and rehabilitation services. The right to anonymous telephone and Internet helplines for children to report abuse is regulated.

The Directive requires Member States to guarantee the confidentiality of the identity of victims in legal proceedings (Article 23). National authorities ought to apply special measures to prevent secondary victimization of children in the course of legal proceedings.

Although the Directive emphasizes the role of technology companies, it does not introduce mandatory requirements for monitoring and reporting cases of sexual exploitation in social networks. The Directive encourages Member States to cooperate with third parties to block and remove illegal content, but lacks concrete mechanisms and guarantees for effective enforcement (Article 25).

Practice shows that some jurisdictions outside the EU refuse to cooperate in the investigation of online crimes, which makes it difficult to trace the perpetrators. Member States apply different practices to investigate Internet crimes, which reduces the effectiveness of cross-border investigations. For example, there is a lack of uniform guidelines for using intelligence technologies to investigate crimes against children in the digital environment.

Effective implementation of Directive 2011/92/EU requires clearer mechanisms for monitoring social networks, tighter interaction with the technology sector and enhanced cross-border cooperation.

iv. European Strategy for a Better Internet for Children (2022) (BIK+)

The European Strategy for a Better Internet for Children (2022) (BIK+) is an updated EU strategy that aims to ensure a safe, inclusive and empowering digital world for children. It is part of the EU's vision for the Digital Decade (2020-2030) and is based on three main pillars:

1. Safe digital experience – ensuring protection from harmful content, cyberbullying and online exploitation through legislative measures, including the Audiovisual Media Services Directive and the EU Digital Services Act;
2. Digital empowerment – increasing digital literacy through training for children, parents and teachers, as well as improving mechanisms for age verification and personal data protection;
3. Active participation – guaranteeing children's right to be heard in the process of creating digital policies, including through children's advisory panels.

The strategy encourages cooperation between Member States, technology companies and the civil sector to build a safer and more accessible digital environment for all children in the EU. The main role of countries outlined by the Strategy is to implement existing European legislation, develop national strategies and invest in education and digital protection for children, specifically:

- Member States should fully implement the EU Digital Services Act (DSA), which obliges platforms to take measures to protect children, including banning targeted advertising based on child profiling;
- Implementation of the Audiovisual Media Services Directive (AVMSD), which requires video-sharing platforms to protect children from harmful content;
- Member States are invited to support the creation of National Strategies for Children's Online Safety;
- Improving age verification mechanisms and ensuring compatibility with the European Digital Identity (eID);
- The EU co-funds national Safer Internet Centers, but Member States are encouraged to provide additional funding and support for them;
- EU Safer Internet Centers offer training for children, parents and teachers, as well as platforms for reporting illegal content;
- Inclusion of digital literacy training in national curricula;
- A special focus is placed on the education of vulnerable groups of children (disabled, socially excluded children, etc.);
- Member States should report their progress in implementing BIK+ through the Safer Internet Expert Group;
- The creation of mechanisms for cooperation between governments, the technology sector and civil society is encouraged.

The principles, norms and goals laid down in the European Strategy for a Better Internet for Children (BIK+) inevitably emphasize the need for the National Safer Internet Center to receive sustainable state support.

v. Strategy of the European Union for a More Effective Fight against Child Sexual Abuse

The Strategy of the European Union for a More Effective Fight against Child Sexual Abuse represents a comprehensive framework of measures aimed at prevention, investigation and protection of victims, combining legislative initiatives, technological solutions and intersectoral cooperation. The Strategy covers

the period of 2020-2025 and includes eight key initiatives aimed at prevention, investigation and victim support. Specific commitments for Member States arising from the Strategy include:

- Implementation of Directive 2011/93/EU: Member States should complete the transposition of the directive, which establishes minimum rules for defining crimes and sanctions in the field of child sexual abuse. This includes prevention, investigation and victim support measures;
- Strengthen law enforcement: Member States should set up specialist victim identification teams and invest in technical capabilities to investigate online crime. Also, the systematic exchange of intelligence data with Europol should be ensured;
- Preventive measures: Member States should introduce prevention programs targeting potential perpetrators and raise awareness among children, parents and professionals. This also includes training to recognize early signs of abuse;
- Creation of a European Center for the Prevention and Counteraction of Sexual Violence against Children: The Center will support Member States in the fight against violence through coordination, prevention and support for victims;
- Involvement of the technology sector: Member States should encourage online platforms to detect and report cases of child sexual abuse, including in encrypted messages, while respecting the fundamental rights and freedoms of Union citizens;
- International cooperation: Member States should participate in global initiatives such as the WeProtect Global Alliance to increase international cooperation to protect children.

Member States are committed to implement these measures and to cooperate at the European and global level for more effective protection of children.

vi. EU Digital Services Act (Regulation (EU) 2022/2065)

Regulation (EU) 2022/2065 or Digital Services Act - DSA is an EU legislative act that regulates the responsibilities of online platforms and intermediary services (including Viber, WhatsApp, YouTube, etc.), aiming to ensure a safer and more transparent digital environment. The regulation introduces requirements for moderation of illegal content, consumer protection and measures against disinformation.

To ensure effective supervision and implementation of Regulation (EU) 2022/2065 within the Digital Single Market, a European Council for Digital Services was established, with each Member State appointing a national coordinator. In Bulgaria, this role ought to be performed by the Communications Regulatory Committee (CRCt), which is responsible for the control of intermediary service providers, with the exception of the very large online platforms directly supervised by the European Commission.

Like any legislative act with the status of a regulation, the Digital Services Act is binding in its entirety and produces the so-called direct effect, i.e. does not require transposition, yet at the same time the national legislation should be harmonized with it, by regulating the mechanism and structures provided for in the Act at the national level, ensuring effective supervision, cooperation and enforcement, which by the beginning of 2025 has not yet been fully realized in Bulgaria.

Thus, at the time of completion of this Report, the draft Act for amendment of the Act on Electronic Communications (AEC), approved by Decision No. 829 of the Council of Ministers of 2024, remains unvoted by the 51st National Assembly. The draft Act aims to ensure the implementation of the requirements of Regulation (EU) 2022/2065 and thus guarantee better state supervision of the activity of the providers of intermediary information services, resp. better protect children online.

The Act for amendment of the Act on Electronic Communications regulates the functions and powers of the competent authorities, including the Council for Electronic Media and the Commission for the Protection of Personal Data. The Council for Electronic Media is a competent authority under Art. 49 of the Regulation the provision of information society intermediary services within the meaning of the Act, which are video sharing platforms. The CRCt, in turn, ought to exercise control over the activities of information society intermediary service providers, which are not video sharing platforms, to fulfill their obligations under the regulation.

The draft Act provides for the introduction of mechanisms for certification of bodies for out-of-court dispute resolution between online platforms and users, as well as procedures for obtaining the status of a trusted flagger and an approved researcher. Trusted flaggers can be incl. non-governmental organizations, with the Act specifically mentioning as an example the centers of the INHOPE hotline network for reporting material showing child sexual abuse. The National Safer Internet Center is such an organization.

Under the draft Act, the CRCt is empowered to investigate the compliance of certified bodies and researchers. Measures are foreseen to limit access to digital services in case of established violations, as well as procedures for the preliminary implementation of certain decisions. A special procedure for the detection of violations and the imposition of sanctions is introduced, which aims at more efficient and rapid control, while preserving the guarantees of the right to defence.

The draft Act provides for the establishment of a special procedure, separate from the one under the Act on Administrative Violations and Penalties (AAVP), to establish violations of the Regulation. The proposed new procedure for establishing violations aims to optimize the procedure for imposing the administrative fine/proprietary sanction, which will achieve the objectives of recitals 114 and 117 of the Regulation, in particular – Member States should ensure that violations of the obligations under the Regulation can be sanctioned in a way that is effective, proportionate and dissuasive. In this regard, the establishment of violations and the imposition of penalties will be carried out in one administrative procedure, with the issuance of one document - a decision of the CRCt to establish the violation and impose the respective penalty.

Timeliness in the implementation of responsibility for violations of the Regulation is also aimed at by creating a process for establishing the committed violations, which is faster and more efficient. Through the proposed special order, the possibilities for avoiding responsibility under the Regulation will be reduced, while at the same time preserving the guarantees for the right to defense by appealing the decision under the Administrative Procedure Code.

The draft Act further complies with the requirement of Art. 52 of the Regulation obliging Member States to establish a system of sanctions that must be effective, proportionate and dissuasive, and the project team advocates for the bill's full and timely adoption.

vii. EU Act on Artificial Intelligence (Regulation (EU) 2024/1689)

Regulation (EU) 2024/1689 aims to establish a single legal framework for the development, supply and use of artificial intelligence (AI) systems in the European Union. The main focus is to ensure that AI is implemented in a way that protects the fundamental rights of citizens, incl. those of children while encouraging innovation. The Regulation requires member states to put in place harmonized measures to protect against the harmful effects of AI, especially as regards high-risk systems.

The Regulation recognizes the specific vulnerability of children in the digital environment and includes provisions that address their protection, incl. the following:

- The Regulation introduces an obligation to comply with the rights of children, provided for in Art. 24 of the EU Charter of Fundamental Rights and the UN Convention on the Rights of the Child. This means that any AI system that may affect children must be designed with their best interests in mind;
- Special consideration is rendered to General Comment No. 25 of the Committee on the Rights of the Child on the rights of children in the digital environment, which emphasizes the need for enhanced protection against exploitation, discrimination and manipulation through AI;
- The Regulation aims at limiting manipulative practices that can affect children, such as algorithms creating addiction to digital services or artificially directing children to certain content or behavior.

Although the Regulation lays the foundations for better protection of children online, several important aspects remain insufficiently addressed, namely:

- Lack of specific measures for social networks and platforms – while the Regulation mentions the protection of children, there are not enough specific requirements for companies operating platforms that use AI for personalized content;
- Unclear sanctioning mechanisms – although the Regulation introduces obligations to protect children, there are no clearly spelled out sanctioning norms aimed at companies that can potentially violate the regime introduced by the Regulation;
- Insufficient differentiation of different risks for children – AI can be used for different purposes, incl. educational, but there is no clear distinction between beneficial and harmful applications of this technology. At the heart of the regulation are not the standards for the protection of fundamental rights as an approach for assessing the safety of AI systems, but a different approach - based on 4 levels of risk, which will make the violation of rights more difficult to detect and assess.

viii. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14.05.2024 on Combating Violence against Women and Domestic Violence

Directive (EU) 2024/1385 aims to provide a uniform legal framework to prevent and combat violence against women and domestic violence across the EU. It introduces measures such as defining a catalog of crimes and punishments, victim protection and access to justice, victim support, data collection, prevention, coordination and cooperation. The Directive recognizes that violence against women and domestic violence constitute violations of fundamental rights, including the right to human dignity, life and integrity of the person, and emphasizes the need for special measures to protect vulnerable groups, incl. the children who are often affected directly or indirectly by such violence.

The transposition of the Directive (with a deadline of 13.06.2027) should include the introduction of additional crimes in the Criminal Code – namely, sharing intimate or manipulated material without consent (including manipulated intimate material generated by AI), surveillance, cyber flashing (sending unsolicited sexual content), doxxing (revealing personal information, passwords, geolocation, etc.), cyber incitement to violence and hate speech, etc. For every act that should be incriminated, there is a list of aggravating circumstances - one of which is precisely that the victim of the crime is a child.

The Project team believes that the introduction of the Directive shall help to upgrade and improve the legal framework ensuring the protection of children in the digital environment, and is committed to follow up and expertly support the transposition process.

VI. List of key recommendations based on the analysis

Based on the above findings, the Project team derives the following system of recommendations for improving the legal framework and institutional cooperation, thus guaranteeing the prevention, detection and punishment of criminal abuse against children in the digital environment, namely:

- Improving the effectiveness of the multidisciplinary teams at the local level in implementing the Coordination Mechanism in cases of violence (Art. 36d of the CPA) through: providing the necessary financial, technical and additional human resources for the effective work of the teams; creation of a unified information system, in which it is visible what goals and activities all involved institutions have set for implementation; defining clearly the roles and responsibilities of the teams and avoiding turnover and inconsistency; providing detailed methodological guidelines for working on cases of online abuse and exploitation; conducting regular joint trainings and workshops of the representatives of the various institutions for work on the Coordination Mechanism, incl. on the matters of online abuse and risks for children;
- By analogy with Art. 5b "Specialized protection of children in public places" from the CPA, a new provision named "Specialized protection of children in the online environment" should be standardized in the Act, whilst the terms and conditions for guaranteeing this type of specialized protection should be determined by a special ordinance adopted by the Council of Ministers;
- Taking measures to urgently reform and strengthen the child protection system by increasing its capacity (requirements for specialized higher education and professional standards in the selection of employees in Child Protection Departments; provision of quality training and resource provision, as well as subsequent training, supervision, certification, etc.);
- Adopting a unified methodological framework to support judges overseeing criminal cases of abuse against children in a digital environment, thereby avoiding conflicting judicial practice (introducing clarity on admissible evidence collected by electronic means, concrete rules on jurisdiction, etc.);
- In the CPC, a mechanism should be regulated for informing the police structure that conducted the inspection, in the presence of a refusal to initiate criminal proceedings, which would give the experts the opportunity to appeal the refusals received before a higher instance;
- Refinement of the general legal definition of "computer information systems" in the CPC, with the aim of clearly differentiating cyber content with abuse of children, sexual exploitation content, etc.;
- Providing sufficient specialized training for prosecutors and magistrates to increase their knowledge and sensitivity regarding online child abuse;
- Regulating within the AAFCCV of a possibility for victim support organizations, which established initial contact with the victim, to carry out the relevant individual assessments;
- Adopting the draft Act on the Amendment of the AEC (approved by Decision No. 829 of the Council of Ministers from 2024), which aims to improve the law by ensuring the application of the requirements of Regulation (EU) 2022/2065 of the EU and thus increasing the State's supervision of the activities of the providers of intermediary information services;
- Building on the protection provided under the AEC to require platforms to prevent and remove harmful content, incl. through better control of algorithms. In compliance with European and national legislation, the State ought to encourage platforms to integrate and report effective safety-

by-design algorithms, policies and rules;

- Upgrading the legal basis for the protection of children's personal data through changes in the APPD to ensure the implementation of reliable age verification mechanisms when registering in social networks and using digital services; introducing clarity on the regime of obligations of platforms and internet providers to take data protection measures; providing for rapid response capabilities for breaches such as data leaks or online misuse of personal information;
- Providing larger human and technical resources to support the activities of the Cybercrime Directorate to the National Service for Combating Organized Crime;
- Guaranteeing compliance with the norm of Art. 39, Para. 2, Item 3 of the Act on the Ministry of Internal Affairs, so that the conduct of procedural and investigative actions in cases related to online abuse against children is assigned only to structures in the Ministry of Internal Affairs with the necessary technical competences;
- Revising (including with an upgrade in the thematic section dedicated to the online safety of children) and adopting, pursuant to Art. 1, Para. 3 of the CPA, the Draft National Strategy for the Child (2024-2030), approved on 01.03.2024 by the National Council for Child Protection to the SACP;
- Adopting the Action Plan for 2025-2026 to the National Program for the Prevention of Violence and Abuse of Children (2023-2026), which should contain precise strategic and operational goals and clear measures regarding the online safety of children, and which ought to be structured according to the specific results already achieved from the implementation of the previous Action Plan (2023-2024);
- Transposition in full of Directive (EU) 2024/1385 on Preventing and Combating Violence against Women and Domestic Violence, thereby upgrading and improving the legal framework ensuring prevention, detection and punishment of crimes against children in the digital environment;
- Ensuring broad and meaningful inclusion of the subject of digital media literacy and safe internet in the school curricula;
- Formulating, adopting and implementing more measures aimed at improving children's mental health, in the context of increasing cases of cyberbullying against children;
- Ensuring sustainable State support for the National Safer Internet Centre, which fulfills Bulgaria's State policy and commitments under several EU directives and international conventions, and is subject to assignment of responsibilities under national framework documents and action plans;
- Ensuring, in implementation of General Comment No. 25 of the UN Committee on the Rights of the Child, authentic child and youth civic participation in the development, monitoring and evaluation of legislation and policies for online safety.

VII. Linkage of the Analytical Report with the Policy Paper developed under the Digital Children Project

Based on the present Analytical Report, a Policy Paper shall be prepared timely, which will present the identified gaps in the regulatory framework, along with the recommendations for improving the protection of children in the digital environment, in the form of an Action Plan addressed to the legislator and relevant state and local institutions.

This will provide a clear path for institutional accountability and effective monitoring of progress in children's digital safety. The National Network for Children, Association Parents and the Bulgarian Association for Family Planning and Sexual Health will present and elaborate on the findings and recommendations from the Analytical Report and the Policy Paper to MPs and institutions, and shall continuously advocate for the improvement of the regulatory framework and institutional work. Additionally, a key goal of the Project team under Digital Children is to dynamically update the Action Plan within the Policy Paper during the full term of Project implementation, based on ongoing monitoring and analysis of relevant legislation and policies.

The present Analytical Report (D5.1) under the project "Digital Children: Protecting and Empowering Children in Digital Environment" was developed by the National Network for Children and approved through a decision of the Project Consortium (comprised of Association Parents, Bulgarian Family Planning and Sexual Health Association, National Network for Children) rendered at a regular meeting of the latter.

АНАЛИТИЧЕН ДОКЛАД

гр. София
февруари 2025

Project: 101158515
“Digital Children: Protecting and Empowering Children in Digital Environment” - DIGITAL-2023-DEPLOY-04
Deliverable D5.1 – Analytical Report
Финансирано от Европейския съюз. Изразените възгледи и мнения са само на автора(ите) и не отразяват непременно тези на Европейския съюз или Европейската изпълнителна агенция за здравеопазването и цифровизацията (HaDEA). Нито Европейският съюз, нито HaDEA могат да носят отговорност за тях.

СЪДЪРЖАНИЕ

деца“

I. Резюме на проект „Дигитални деца: Закрила и овластяване на децата в дигитална среда“

iv. Проект „Дигитални деца“ и Дейност 5 („Work Package 5“) от проектното изпълнение:

✓ **За НЦБИ и проектния консорциум**

Проектът „Дигитални деца: Закрила и овластяване на децата в дигитална среда“ („Дигитални деца“, „Проектът“) е посветен на многостранните предизвикателства, пред които са изправени децата в дигиталния свят не само в България, но и в цяла Европа. Той се ангажира с повишаването на онлайн безопасността на децата, като активно подкрепя дейностите на българския Център за безопасен интернет (НЦБИ, „Центъра“), включително продължаващото функциониране на двете ключови услуги на Центъра, а именно Консултативната линия за онлайн сигурност на децата („Консултативна линия“) и Горещата линия за подаване на сигнали за онлайн престъпления срещу деца („Гореща линия“).

На 11.02.2025 г. се навършиха 20 години от основаването на Центъра.

НЦБИ е единствената по рода си структура у нас за защита и подкрепа на българските деца в онлайн пространството. Горещата линия и Консултативната линия за онлайн безопасност за деца 124 123 обработва рекорден брой сигнали за злоупотреби. Линиите и чатът на safenet.bg помагат на хиляди родители и деца при проблем с онлайн профил, онлайн насилие, вредно съдържание и др. Центърът е доверен партньор на дирекция „Киберпрестъпност” към ГДБОП, а на международно ниво – на мрежата INHOPE, на Интерпол, както и на големите социални платформи, в които децата масово имат профили.

НЦБИ е с обновен консорциум от организации, които изпълняват дейностите на проекта „Дигитални деца“. Асоциация „Родители“, която е от основателите на Центъра през 2005 г., е главен координатор, а реализирането на дейността на Центъра се подкрепя от Българската асоциация по семейно планиране и сексуално здраве (БАСП), ангажирана преимуществено с мащабната обучителна работа по проекта, и от Сдружение „Национална мрежа за децата“ (НМД), **отговорно за комуникационните и застъпнически дейности** (съгласно описаното в Дейност № 5 от Приложение № 1 към проектния административен договор).

НМД е най-голямото обединение на граждански организации и експерти в България (над 130), работещи с и за деца и семейства. Сред ключовите ръководни начала на организацията попадат **насърчаването, защитата и спазването на правата на детето, съобразно Конвенцията за правата на детето на ООН**. НМД вярва, че всички политики и практики, които засягат пряко или косвено децата, следва да се изготвят, прилагат и наблюдават, като се взема предвид принципът за висшия интерес на децата и с активното участие на самите деца.

✓ **Основни цели на Дейност 5 от проектното изпълнение и на Застъпническия план. Цели и обхват на доклада**

Дейност № 5 („Work Package 5“) от Проекта, с наименование „**Комуникация, сътрудничество и застъпничество на национално равнище**“, цели осъществяването на застъпничество и непрекъснато повишаване на осведомеността чрез следните дейности:

1). провеждане на целеви комуникационни и информационни кампании и събития;

2). разработване и разпространение на ресурси и инструменти, въз основа на оценки на нуждите и изводи от работата на Горещата и Консултативната линия;

3). застъпничество за нормативни промени на равнище право на ЕС и национално право – с цел **приемане на ефективно законодателство за предотвратяване, разкриване и наказване на сексуалната експлоатация на деца във виртуална среда**;

4). експертно съдействие в **мониторинга и реализирането на национални политики, насочени към безопасността на децата онлайн**, повишаване на дигитално-медийната грамотност и др.

Настоящият Аналитичен доклад адресира целите по точки № 3 и № 4 по-горе. Докладът анализира правната рамка и предоставя структурен и функционален анализ на съществуващи системи за гарантиране на онлайн безопасността на децата. Той систематизира и аргументира препоръки за подобряване на политиката и за системни промени, необходими за гарантиране на правото на децата да се възползват безопасно от възможностите на цифровия свят.

Изложеното в настоящия Аналитичен доклад почива на дългогодишната изследователска и застъпническа работа на Национална мрежа за децата и нейните членове и партньори; опита на консорциума, управляващ НЦБИ; текущия анализ и мониторинг на законодателство и политики в хода на проектното изпълнение; комуникация с институции, органи по закрила, дирекция „Киберпрестъпност“ към ГДБОП и др.

II. Онлайн безопасността на децата в България и в глобален план в началото на 2025 г.

В началото на 2025 г. Националният център за безопасен интернет отчете **рекорден брой случаи на Горещата телефонна линия за подаване на сигнали за онлайн престъпления срещу деца – 1 749 747 сигнала**, като над 95% от тях са за онлайн сексуална експлоатация на малолетни и непълнолетни.

70 268 сигнала са окомплектовани и изпратени към дирекция „Киберпрестъпност“ към ГДБОП, доверен партньор на Центъра.

Това **е най-високият брой сигнали, обработени в 20-годишната история на Центъра в рамките на една календарна година.** Причините за драстичното нарастване на казусите са много и разнородни (вкл. висока оперативност на НЦБИ и оптимизирана през 2024 г. система за обработване на сигналите; открити при проверки на незаконно хоствано съдържание допълнителни изображения и линкове – всеки от които бива докладван поотделно; повишена обществена разпознаваемост и доверие към Центъра и др.), но то категорично е индикативно за **нарастващите по брой, инструментариум и обхват онлайн посегателства срещу деца у нас и в глобален план.**

На този фон, по данни на Евростат **само 58% от младежите на възраст 16–24 г. в България имат основни или добри дигитални умения**, което е значително под средната стойност за ЕС, възлизаща на 80%. **1 от всеки 7 деца у нас съобщава, че е било жертва на онлайн тормоз и**

преследване в социалните мрежи.[1] Според данни на УНИЦЕФ, в България всяко второ дете (47%) е претърпяло някаква форма на насилие. В раздела на проучването за емоционално насилие децата и младите хора са запитани за онлайн тормоз и злоупотреба, като **поне 1 от всеки 10 деца и млади хора (10,9%) съобщава за случаи на преживян онлайн тормоз.** Деца – познати на жертвата, са най-често посочваните извършители на онлайн тормоз и злоупотреба. Най-често посочваното от децата и младите хора място за онлайн тормоз са **уебсайтовете на социалните медии – 60,7%**, следвани от **платформи за онлайн игри (17,12%)** и **чат приложения (16,3%).**

Данните от проучване на ECPAT и NSPCC, проведено в навечерието на гласуването в Съвета на ЕС на Регламента за сексуалното насилие над деца показват, че **общо 95% от европейците искат нови регулации, които да гарантират ефективно безопасността на децата в интернет.** Проучването е проведено сред 26 000 пълнолетни лица в 27-те държави членки. В България участниците са 1050. Според данните от „Евробарометър“ **71% от европейците са готови да направят известен компромис с личния си живот онлайн**, ако това ще помогне за защитата на децата от потенциална сексуална злоупотреба и експлоатация онлайн. А **над 70% подкрепят откриването и премахването на материали със сексуална злоупотреба с деца** в криптирани от край докрай платформи.[2]

През 2022 – 2024 г., според доклада на Европол за тежката организирана киберпрестъпност, същата има увеличение с над 300% не само в България и Европа, но и в цял свят, а децата са сред най-уязвимите към киберпрестъпления.

Тревожната тенденция на нарастваща честота и разнообразие на инструментите за онлайн експлоатация на деца в България съответства на глобалния ръст на този проблем и задълбочаването на насилието в дигитална среда. По време на кръглата маса на тема „**Противодействие на онлайн сексуалната злоупотреба с деца: тенденциите, възможни решения и предизвикателства**“ на НЦБИ по проект „Дигитални деца“ от 09.01.2025 г., организирана с домакинството на ДАЗД и в партньорство с Международната асоциация на интернет Горещи линии INHOPE,[3] НМД представи следните **глобални тенденции**, систематизирани на база опита от участието на Мрежата в инициативи по обмен на международния алианс ECPAT International и в Глобалната среща на върха на обединението WeProtect (WeProtect Global Alliance's 2024 Global Summit),[4] а именно:

• **Повече от 300 милиона деца годишно** стават жертви на сексуална злоупотреба и експлоатация онлайн;

• **Финансовото сексуално изнудване и принуда** на деца, **заедно с генерирането на материали за сексуално насилие от изкуствен интелект** (ИИ), са форми на насилие с все по-широк обхват;

• **Все по-ограничени са ресурсите и подкрепата за неправителствения сектор,** ангажиран в борбата срещу насилието и сексуалната експлоатация на деца;

• **360% увеличение на самогенерираните от 7-10-годишни деца изображения** с голота само за периода от 2020 до 2022 г. (Internet Watch Foundation);

---

[1] **Национална мрежа за децата, „Бележник 2024: Какъв е средният успех на държавата в грижата за децата“, 2024 г., стр. 55.**
[2] *Ibid.*
[3] **https://nmd.bg/nmd-predstavi-danni-i-globalni-tendenczii-za-onlajn-zloupotrebite-nad-decza-na-kragla-masa-na-naczionalniya-czentar-za-bezopasen-internet-i-dazd/**
[4] **https://nmd.bg/nmd-predstavi-pozicziyata-na-evropa-za-po-bezopasen-czifrov-svyat-za-deczata-v-ramkkite-na-globalnata-srestha-na-varha-2024-na-aliansa-weprotect-v-abu-dabi/**

• **Нарастват случаите на психични страдания и суицидни опити на деца – създали емоционална връзка с генеративен ИИ чатбот**, имитиращ партньор / близък;

• В глобален план основна територия на похитителите **са платформите за онлайн игри**, където деца стават жертви на насилие средно **за 19 секунди от първото лично съобщение;**

• **Тъмната мрежа (Dark Web)** продължава да е „резервоар“ за съдържание със сексуална експоатация на деца; по данни на Министерството на правосъдието на САЩ, **една подобна публикация във форум в Тъмната мрежа е била видяна 1 025 680 пъти за 47 дни (21 822 гледания на ден) преди да бъде свалена;**

• В проучване сред ползватели на Тъмната мрежа, 39% заявяват, че са ставали **свидетели на излъчване на живо на сексуална експлоатация на дете;**

• Увеличават се **инструментите за маскиране на съдържание на сексуална експлоатация** – напр. чрез **стеганография** (данните са скрити вътре в изображение, аудио файл или друг медиен формат), чрез редактиране на изображението, така че да наподобява AI-генерирано и др.;

• **Нарастващи експоненциално** случаи на онлайн насилие и тормоз **между** деца;

• Случаите на посегателства в социални мрежи и чат приложения продължават да се способстват от **липсващи т.нар. safety by design („безопасност по дизайн“) алгоритми, политики и правила.**

Предвид описаните тенденции на национално и международно равнище, особено необходимо е да бъде направена **обхватна оценка на нормативната база, политиките и практиките в България**, адресиращи тези проблеми понастоящем.

III. Национални законови нормативни актове, свързани с онлайн безопасността на децата

Закон за закрила на детето

Законът за закрила на детето (ЗЗДет)[5] **не съдържа изрични разпоредби**, които конкретно да се отнасят до защита на децата от посегателства в онлайн среда. ЗЗДет урежда правата, мерките и органите за закрила на децата в България, като се основава на принципи като зачитане на личността на детето, осигуряване на най-добрите интереси и обезпечаване на особена закрила за деца в риск. Законът гарантира правото на всяко дете на защита срещу физическо, психическо, сексуално и др. насилие, както и срещу използване за проституция, просия и разпространение на порнографски материали. ЗЗДет предвижда **общ режим** за закрила на децата, **мерките в който могат да бъдат приложени в контекста на посегателствата в цифрова среда.** Конкретно, относими към онлайн безопасността на децата са следните разпоредби:

- **Закрила срещу насилие и експлоатация (чл. 11)** – има приложимост спрямо онлайн тормоза, кибернасилието и сексуалната експлоатация на деца в дигитална среда;
- **Закрила на личността на детето и тайна на информацията (чл. 11а и чл. 16)** – регламентирана забрана за разпространение на сведения за деца без тяхното или родителско (респ. на органа по закрила) съгласие, което има отношение към онлайн поверителността;
- **Информиране и консултиране (чл. 13)** – децата имат право на достъп до информация и консултации, включително за рисковете в интернет пространството;
- **Задължение за съдействие (чл. 7)** – всички граждани и институции са длъжни да

[5] https://lex.bg/laws/ldoc/2134925825

сигнализират компетентните органи при подозрение за посегателство срещу дете, включително в интернет;

- **Координационен механизъм при насилие (чл. 36г)** - за осигуряване на защита на дете в риск или жертва на насилие или експлоатация дирекция „Социално подпомагане“ създава мултидисциплинарен екип, членовете на който работят заедно до приключване на случая и който разработва план за действие за защита на детето или за предотвратяване на насилието;
- **Защита на дете – жертва на насилие или експлоатация (чл. 36д)** - -защитата на дете в риск или жертва на насилие или експлоатация се предприема след проучване на случая от мултидисциплинарния екип и съгласно предложения от него план за действие. Планът за действие съдържа здравни, социални и образователни услуги за превенция на насилието или за възстановяване на детето;
- **Легалната дефиниция за „дете в риск“ по § 1, т. 11, б. „б“ от ДР на ЗЗДет.** обхваща случаите на деца жертви на злоупотреба, насилие, експлоатация или всякакво друго нехуманно или унизително отношение или наказание в или извън семейството, а на свой ред **б. „в“ от цитираната норма** – случаите на деца, за които съществува опасност от увреждане на тяхното физическо, психическо, нравствено, интелектуално и социално развитие, т.е. нормата обхваща и посегателствата (респ. опасността от такива) в цифрова среда.

ДАЗД, МВР и социалните служби носят основната отговорност за превенцията и борбата срещу насилието, в т.ч. в онлайн среда, като съдействие оказват неправителствените организации, образователните институции и частният сектор.

Удачно е допълване на ЗЗДет и подзаконовата нормативна уредба със специфични мерки за превенция, мониторинг и санкции срещу дигиталните рискове за децата. В този смисъл, по модела на чл. 5б „Специализирана закрила на деца на обществени места“, би могла да бъде добавена **нова разпоредба с наименование „Специализирана закрила на деца в онлайн среда“**, като в т.ч. **условията и реда за гарантиране на този вид специализирана закрила се определят в детайли с нарочна наредба на Министерския съвет**, по предложение на ресорни институции като МТСП, МВР, ДАЗД (вж. чл. 5б, ал. 2 от ЗЗДет).

Също така, релевантните към действието на мултидисциплинарните екипи на местно ниво по прилагане на Координационния механизъм при насилие (чл. 36г) критики и препоръки са валидни и за работата по случаи на посегателства и рискове в онлайн среда, в т.ч. за:

- осигуряване на необходимите **финансови, технически и допълнителни човешки ресурси** за ефективната работа на екипите;
- създаване на **единна информационна система**, в която да е видно какви цели и дейности са заложили за изпълнение всички ангажирани институции;
- **ясно дефиниране на ролите и отговорностите** на екипите и избягване на текучеството и несъгласуваността;
- предоставяне на подробни **методически указания за работа по случаи на онлайн насилие и експлоатация**;
- провеждане на **редовни съвместни обучения и работни срещи** на представителите на различните институции за работа по Координационния механизъм, вкл. с предмет онлайн посегателства.[6]

Анализът на ЗЗДет не бива да пропуска маркиране и **на дефицитите на системата на закрила на детето.** Единственото оперативно звено за изпълнение на мерките за закрила на детето са отделите

[6] **Доклади на ДАЗД за прилагане на Координационния механизъм за взаимодействие при работа в случаи на деца, жертви на насилие и за взаимодействие при кризисна интервенция (https://sacp.government.bg).**

за закрила към дирекциите „Социално подпомагане“, като продължават да **липсват изисквания за специализирано висше образование и професионални стандарти при подбора на служителите**, **липсва качествена подготовка и ресурсна обезпеченост, както и последващи обучения, супервизия, атестация.** Натовареността на служителите на ОЗД на твърде много места остава непосилно висока, което закономерно води до текучество и невъзможност за осигуряване на необходимото качество.

През 2024 г. беше **утвърдена Стратегията за развитие на човешките ресурси в социалната сфера (2024-2030 г.)**,[7] а анализът на състоянието ясно показва необходимостта от **спешни инвестиции в системата.**

Наказателен кодекс[8] и Наказателно-процесуален кодекс[9]

В каталога от престъпни деяния в Наказателния кодекс фигурират състави с предмет посегателства срещу деца в онлайн среда, вкл.:

- **Разврат (чл. 149 и сл. от НК) -** който извърши **действие с цел да възбуди или удовлетвори полово желание без съвкупление по отношение на лице, ненавършило 14-годишна възраст**, се наказва за блудство с лишаване от свобода от една до шест години;
- **Подбуждане и принуда (чл. 155а – чл. 155в от НК)** - който чрез информационна или съобщителна технология или по друг начин **предоставя или събира информация за лице, ненавършило 18-годишна възраст**, за да се установи контакт с него за извършване на блудствено действие, съвкупление, полово сношение, проституция, за създаване на порнографски материал или за участие в порнографско представление, се наказва с лишаване от свобода от три до десет години и с глоба от десет хиляди до двадесет хиляди лева. Наказанието се налага и на онзи, който **чрез информационна или съобщителна технология или по друг начин установи контакт с лице, ненавършило 14-годишна възраст**, с цел извършване на блудствено действие, съвкупление, полово сношение, за създаване на порнографски материал или за участие в порнографско представление. През 2024 г. (ДВ, бр. 39) беше приета **допълнителна квалифицираща разпоредба**, която предвижда, че когато от деянието са настъпили **значителни вредни последици за физическото, душевното или моралното развитие на пострадалия**, наказанието е лишаване от свобода от пет до дванадесет години. Нормата на чл. 155б предвижда, че който склонява **лице, ненавършило 14-годишна възраст, да *наблюдава* действителни, виртуални или симулирани полови сношения** между лица от еднакъв или различен пол или похотливо показване на човешки полови органи, содомия, мастурбация, сексуален садизъм или мазохизъм, се наказва с лишаване от свобода от три до десет години. Който **склонява лице, ненавършило 14-годишна възраст, да *участва* в действителни, виртуални или симулирани полови сношения** между лица от еднакъв или различен пол или похотливо показване на човешки полови органи, содомия, мастурбация, сексуален садизъм или мазохизъм, се наказва с лишаване от свобода от пет до десет години. В чл. 155в е регламентирано, че който чрез употреба на сила или заплашване, или чрез използване на положение на зависимост или надзор **склонява непълнолетно лице да *наблюдава* действително, виртуално или симулирано блудствено действие, съвкупление, полово**

[7] https://www.mlsp.government.bg/uploads/1/strategia-2024-2030.pdf
[8] https://lex.bg/laws/ldoc/1589654529
[9] https://lex.bg/laws/ldoc/2135512224

сношение, включително содомия, мастурбация, сексуален садизъм или мазохизъм, както и похотливо показване на човешки полови органи, се наказва с лишаване от свобода от три до седем години. Който чрез употреба на сила или заплашване, или чрез използване на положение на зависимост или надзор склонява непълнолетно лице **да *участва* в действително, виртуално или симулирано блудствено действие, съвкупление, полово сношение, включително содомия, мастурбация, сексуален садизъм или мазохизъм, както и за похотливо показване на човешки полови органи**, се наказва с лишаване от свобода от три до десет години.

- **В чл. 158а от НК** са уредени **престъпните състави, инкриминиращи набирането, подпомагането или използването на лице, ненавършило 18-годишна възраст**, или група от такива лица, за **участие в т.нар. порнографско представление**;
- **Порнографски материали с лица, жертва на сексуална експлоатация** (**чл. 159**) – цитираната норма предвижда, че който създава, излага, представя, излъчва, предлага, продава, дава под наем или по друг начин разпространява порнографски материал, се наказва с лишаване от свобода до една година и глоба от хиляда до три хиляди лева. Който излага, представя, предлага, продава, дава под наем или по друг начин разпространява порнографски материал **на лице, ненавършило 16 години**, се наказва с **лишаване от свобода до шест години** и глоба до пет хиляди лева. За това престъпно деяние наказанието е лишаване от свобода от три до шест години и глоба до десет хиляди лева, **когато за създаването на порнографския материал е използвано лице, ненавършило 18-годишна възраст, или лице, което изглежда като такова (чл. 159, ал. 4, т. 1 от НК).** Който **държи или набавя за себе си или за другиго** чрез информационна или съобщителна технология или по друг начин порнографски материал, за създаването на който е **използвано лице, ненавършило 18 години, или лице, което изглежда като такова**, се наказва с лишаване от свобода **до пет години** и с глоба до десет хиляди лева.
- **„Порнографски материал“** (легалната дефиниция се съдържа в чл. 93, ал. 1, т. 28) е изготвен по какъвто и да е начин, неприличен, неприемлив или несъвместим с обществения морал материал, чието съдържание изобразява реално или симулирано блудствено действие, съвкупление, полово сношение, включително содомия, мастурбация, сексуален садизъм или мазохизъм, както и похотливо показване на половите органи на лице. **„Порнографско представление“** (легалната дефиниция се съдържа в чл. 93, ал. 1, т. 30) е **представяне на живо или в реално време** пред другиго на похотливо показване на половите органи **на лице, ненавършило 18-годишна възраст, или на участието на такова лице в реално или симулирано** блудствено действие, съвкупление, полово сношение, включително содомия, мастурбация, сексуален садизъм или мазохизъм;
- Други относими към онлайн посегателствата срещу деца легални дефиниции са поместени систематично в разпоредбата на чл. 93 от НК – в т.ч. определение за **„информационна система“** (ал. 1, т. 21), **„компютърни данни“** (т. 22), **„доставчик на компютърно-информационни услуги“** (т. 23) и пр.

Общата оценка на проектния екип, на база в т.ч. експертния диалог с дирекция „Киберпрестъпност“ към ГДБОП, е че наказанията за този вид престъпления, предвидени в Наказателния кодекс, **са съобразени с тежестта на извършените престъпни деяния**, и че основните проблеми, както е разгледано по-долу, произтичат от **бавност** и **други пороци на процесуално-следствените действия**, от **липсата на чувствителност** по отношение на значимостта на деянията в цифрова

среда у част от прокурорите и съдиите в страната и др.

Както е разгледано по-долу, транспонирането на Директивата на ЕС за домашното насилие (считано до 13.06.2027 г.) **ще изисква разширяването на каталога от престъпления** срещу личността, извършвани онлайн – в т.ч. с изричното инкриминиране в Наказателния кодекс на **манипулирането на интимен материал, генерирано от изкуствен интелект; т.нар. киберфлашинг, доксинг** и др. престъпни състави.

Що се касае процесуалноправната уредба в Наказателно-процесуалния кодекс (НПК), като адекватна се отчита регламентацията на **процесуално-следствените действия по киберпрестъпления и достъпа до електронни доказателства** (доставчиците на компютърни услуги са длъжни да подпомагат разследващите органи при събиране на електронни доказателства; специални разузнавателни средства могат да се използват при тежки умишлени престъпления, вкл. киберпрестъпления); **процесуалните гаранции за деца жертви на престъпления** и защитните норми, осигуряващи **закрила от вторична виктимизация.** Отчита се в т.ч. **транспонирането на Директива (ЕС) 2016/800 относно процесуалните гаранции за децата – заподозрени или обвиняеми в рамките на наказателното производство**, завършено през 2023-2024 г.

Общата оценка на проектния екип е, че законовата уредба е добра, но все пак са налице **пропуски**, като същевременно практиката показва съществени процесуални и институционални предизвикателства в разкриването и наказването на онлайн посегателства, породени от следното:

- Наказателният процес по отношение на онлайн посегателствата остава твърде формален, а **практиката на наказателните състави - противоречива**. Така например, някои съдилища признават определен вид събрани с електронни средства доказателства, а други – не, поради **липсата на единна методологическа рамка**;
- В Наказателно-процесуалния кодекс **няма правно-регламентиран механизъм за запознаване на полицейската структура, водила проверката, при наличие на отказ** за образуване на наказателно производство. Това затруднява възможността експертите **да обжалват получените откази** пред по-горна инстанция;
- Понякога, по преценка на наблюдаващия прокурор, същият може да не упражни правото си за постановяване задържане на извършителя за 72 часа, по реда на НПК, което предпоставя **възможността извършителите да унищожат електронни доказателства;**
- В закона присъства **твърде общата дефиниция „компютърни информационни системи", без да има единна методология на диференциране на киберсъдържание със злоупотреба с и над деца, сексуално съдържание и пр**. и без да е налице механизъм, с който да се избягва противоречивата практика на наблюдаващи прокурори и магистрати;
- Тъй като престъпленията се извършват онлайн, често има **неясноти относно мястото за повдигане на обвинението.** Липсата на утвърдена съдебна практика и конкретни правни норми **възпрепятства образуването на досъдебно производство в подсъдния район** по местонахождението на извършителя, въпреки че жертвите му са от различни населени места;
- Все още немалко прокурори и съдии в страната **нямат достатъчно задълбочени познания и чувствителност** по отношение на онлайн посегателствата над деца и **не отдават дължимото внимание на тези случаи.**

Закон за подпомагане и финансова компенсация на пострадали от престъпления (ЗПФКПП)[10]

Законът за подпомагане и финансова компенсация на пострадали от престъпления (ЗПФКПП)

[10] https://lex.bg/laws/ldoc/2135540550

урежда условията и реда за подпомагане и финансова компенсация от държавата на пострадали от престъпления български граждани или граждани на държави членки на ЕС. С приетите от НС през 2023 г. промени бе създадена нова Глава втора „а“ в ЗПФКПП, чрез която списъкът на процесуалните права на пострадалите, в това число на **децата, жертви и/или свидетели на престъпления**, се разшири.[11] Към него бяха добавени допълнителни норми, имащи за цел да гарантират по-ефективно правосъдие за децата жертви, в т.ч., както следва: 1). пострадалите от престъпления имат **право на индивидуална оценка**; 2). когато пострадалият е дете, **задължително се приема, че са налице специфични нужди от защита**, като извършващият оценката орган незабавно уведомява отдел „Закрила на детето“ към дирекция „Социално подпомагане“ по настоящия или постоянен адрес на детето; 3). **органите на МВР или следователите, установили първоначален контакт с пострадалия, извършват без излишно забавяне индивидуалната оценка** на основата на разговор с лицето. Те могат да поискат **съдействие от психолог, лекар или друг подходящ специалист** по своя преценка; 4); **специфичен ред за провеждане на разпит на децата свидетели със специфични нужда от защита** – в присъствие на педагог или психолог, а при необходимост – и в присъствието на родителя, настойника или попечителя.

Негативно се оценява **липсата на възможност организациите за подкрепа на пострадали, установили първоначален контакт с жертвата, да извършват индивидуални оценки.** Натоварването на органите на МВР с комплексната дейност по осъществяване на индивидуалната оценка на пострадалите деца предполага солидна специална подготовка на полицаи и следователи, каквато към момента не се осъществява навсякъде. Също така, практиката показва, че на много места е налице **непознаване на новата уредба** и/ли нейното **бланкетно използване**.

Закон за електронните съобщения[12]

Законът за електронните съобщения (ЗЕС) урежда обществените отношения, свързани с предаването, излъчването и приемането на електронни съобщения чрез различни технологии (проводник, радиовълни, оптични или електромагнитни средства). Основните цели включват:

- гарантиране на **сигурността и достъпността** на електронните съобщителни мрежи;
- развитие на конкуренцията и **защита на потребителите**;
- осигуряване на **прозрачност** при предоставянето на услуги;
- защита на националната сигурност и **личните данни на гражданите**.

Въпреки че ЗЕС не поставя акцент върху безопасността на децата онлайн, няколко ключови разпоредби имат касателство към защитата на децата, а именно:

- Законът гарантира **неприкосновеността на електронните съобщения**, включително съдържанието на комуникациите и личните данни на потребителите. Това създава правна основа за защита на децата от злоупотреби като кибертормоз, изнудване и други посегателства;
- Доставчиците на интернет услуги имат **задължение да сътрудничат на държавните органи за ограничаване на достъпа до съдържание, което застрашава децата**, включително детска порнография и насилие. Тези мерки обаче не са детайлно разписани и имат нужда от допрецизиране чрез дълнителна регулация;
- ЗЕС предвижда **механизми за достъп на правоохранителните органи до трафични**

[11] https://nmd.bg/pobedi-li-kauzata-na-nmd-za-sthadyastho-pravosadie-za-deczata-zhertvi-na-prestapleniya/
[12] https://lex.bg/laws/ldoc/2135553187

данни при разследвания, свързани с престъпления срещу деца в интернет.[13] Това позволява по-ефективно идентифициране и наказване на извършители на онлайн посегателства. Ключова е привръзката със **специалната разпоредба на чл. 159а от НПК**, която извежда в отделна норма задължението за предоставяне на данни от страна на доставчиците на обществени електронни съобщителни мрежи и/или услуги. Доставчиците на услуги следва да предоставят данни, създадени при осъществяване на тяхната дейност, **по искане на съда в съдебното производство или въз основа на мотивирано разпореждане на съдия от съответния първоинстанционен съд**, постановено по искане на наблюдаващия прокурор **в досъдебното производство**.[14][15]

Основните институции, отговорни за прилагането на закона и защитата на децата в цифрова среда, са:

- **Комисията за регулиране на съобщенията (КРС)** – наблюдава спазването на законодателството от страна на интернет доставчиците и телекомуникационните оператори;
- **Министерството на вътрешните работи (МВР)** – отговаря за разследването на киберпрестъпления и съдействието при разкриване на онлайн заплахи за деца;
- **Държавната агенция за закрила на детето (ДАЗД)** – има роля в разработването на политики за онлайн безопасност.

Законът за електронните съобщения не съдържа специални норми за защита на децата в дигиталното пространство. Сред основните липси са: **липса на достатъчно прецизирани и обхватни задължения за интернет платформите**; **неясни и тромави механизми за контрол на съдържанието** (блокирането на вредно съдържание зависи от съдебни разпореждания, което забавя реакцията на органите); **ограничена координация между институциите** – няма ясен механизъм за координиране на действията между КРС, МВР и ДАЗД по отношение на дигиталната сигурност на децата. Респективно, необходимо е въвеждане на **допълнителни разпоредби за задълженията на онлайн платформите**, **бързо блокиране на вредно съдържание** и **по-добра координация между институциите**.

В тази връзка, по-долу е разгледан **одобреният с Решение № 829 на Министерския съвет от 2024 г. проект на Закон за изменение и допълнение на Закона за електронните съобщения (ЗЕС)**, който има за цел да усъвършенства ЗЕС, като осигури прилагането в пълнота на изискванията на Регламент (ЕС) 2022/2065 на ЕС.

Закон за защита на личните данни[16]

Законът за защита на личните данни (ЗЗЛД) регламентира обработването и защитата на личните данни на физическите лица в България, като **въвежда механизмите на Общия регламент на ЕС относно защитата на данните (GDPR).** Основните принципи на закона включват:

- Законосъобразност и прозрачност на обработката на лични данни;

[13] **Вж. Решение № 2 на Конституционния съд от 2015 г. (https://legislation.apis.bg/doc/2535725/0)**
[14] **Млъчков, Б., „Събирането на трафични данни в Република България“, 06.01.2025 г., „Lex.bg“ (https://news.lex.bg/)**
[15] **Млъчков, Б., „Съхраняването на трафични данни в Република България“ (https://www.challengingthelaw.com/informacionno-pravo/syhranyavaneto-na-trafichni-danni/)**
[16] **https://lex.bg/laws/ldoc/2135426048**

- Минимизиране на събираните данни;
- Ограничаване на целите на обработване;
- Гарантиране на сигурност и поверителност;
- Право на коригиране и изтриване на личните данни.

Децата се считат за уязвима група, като законът поставя **специални изисквания към обработването на техните лични данни**:

- **Минимална възраст за съгласие** за обработка на данни - чл. 25в постановява, **че обработването на лични данни на дете под 14 г. е законно само ако съгласието е дадено от родител или настойник**. Това важи особено за дигитални услуги и социални мрежи;
- Ограничения за разкриване на лични данни - **разпространението на лични данни на деца в публичното пространство, включително в интернет, е ограничено**, освен ако има изрично съгласие на родителя или ако това е предвидено от закона.[17]

Контролът върху защитата на личните данни, включително тези на децата, се осъществява от **Комисията за защита на личните данни (КЗЛД)**, която има правомощия да:

- Провежда разследвания и налага санкции на администратори, които не спазват закона;
- Разработва насоки и препоръки за сигурно обработване на детски данни;
- Работи в сътрудничество с международни органи за защита на личните данни.

ЗЗЛД създава нормативна основа за защита на личните данни, но се отчитат пропуски по отношение на сигурността на децата онлайн, в т.ч.:

- Липса на ясни и надеждни механизми за проверка на възрастта при регистрация в социални мрежи и ползване на дигитални услуги;
- Неяснота относно режима от задължения на платформите и интернет доставчиците да предприемат мерки за защита на личните данни на децата;
- Ограничени възможности за бърза реакция при нарушения като изтичане на данни или онлайн злоупотреби с лична информация.

Така ЗЗЛД предоставя защита за децата в цифровата среда, но се нуждае от **допълнителни разпоредби и механизми за по-ефективно прилагане на тези защитни норми**.

Закон за киберсигурност[18]. Дирекция „Киберпрестъпност“ към ГДБОП

Законът за киберсигурност урежда дейностите по: 1). **организацията, управлението и контрола**

[17] **Комисия за защита на личните данни, „Твоите права за защита на личните данни“ (текст на информационно-разяснителна брошура, предназначена за деца)** (https://cpdp.bg/%d1%82%d0%b2%d0%be%d0%b8%d1%82%d0%b5-%d0%bf%d1%80%d0%b0%d0%b2%d0%b0-%d0%b7%d0%b0-%d0%b7%d0%b0%d1%89%d0%b8%d1%82%d0%b0-%d0%bd%d0%b0-%d0%bb%d0%b8%d1%87%d0%bd%d0%b8%d1%82%d0%b5-%d0%b4%d0%b0%d0%bd%d0%bd/)

[18] https://lex.bg/bg/laws/ldoc/2137188253

на киберсигурността, вкл. дейности и проекти по киберотбрана и по **противодействие на киберпрестъпността**; 2). предприемане на необходимите мерки за постигане на **високо общо ниво на мрежова и информационна сигурност**. С него се определят и **правомощията и функциите на компетентните органи** в областта на киберсигурността. По този начин законът осигурява рамка за координирани действия между институциите и частния сектор с цел ефективна защита на децата от онлайн заплахи, включително сексуална експлоатация, измами и онлайн тормоз.

Министерството на вътрешните работи е основният орган, отговорен за противодействие на киберпрестъпността, като в неговата структура действа Главна дирекция „Борба с организираната престъпност“ (ГДБОП). В рамките на тази дирекция функционира **специализиран Център по киберпрестъпност**, който извършва разкриване, разследване и документиране на компютърни престъпления, включително такива, които са насочени срещу деца (чл. 14, ал. 2 от Закона за киберсигурност). В случай на установяване на заплаха или кибератака, насочена към деца, ГДБОП има правомощие да предприема **оперативно-издирвателни действия**, включително разследване и прекратяване на вредоносни онлайн дейности.

Така при констатиране на случаи на **кибертормоз, незаконно съдържание и поведение** в мрежата компетентни органи са дирекция „Социално подпомагане“ по местопребиваване на детето и **специализираната дирекция „Киберпрестъпност“ към ГДБОП**.[19][20]

В допълнение към нормативната основа в Закона за киберсигурност, следва да бъде посочено, че дирекция „Киберпрестъпност“ изпълнява задачи по противодействие на организирани престъпни групи и отделни лица, извършващи в т.ч. **производство, държане и разпространение на порнографски материали с непълнолетни лица**.

Част от функционалните компетентности на дирекцията е **работата по линия „Противоправно съдържание в интернет“.** Служителите на дирекцията са компетентни да вземат отношение при получени данни за сексуална експлоатация на деца в интернет. Използват се софтуерни продукти, с които се **наблюдават специализирани мрежи за обмен на файлове с детска сексуална експлоатация.** Извършва се 24/7 мониторинг на интернет трафика в България, като **над 85% от него се филтрира за незаконно съдържание.** Ограничава се **както умишлен, така и случаен достъп (особено от деца) до сайтове с порнографски материали**. Ежемесечно от Интерпол се предоставя списък с уеб сайтове „Worst of“, базирани в интернет пространството на страната ни, съдържащи противоправно съдържание, като ГДБОП блокира сайтовете и пренасочва потребителите им към стоп страница с **информация за противоправността на съответното деяние**.

Осигурена е възможност и всеки гражданин да подава **директен сигнал към ГДБОП на страници www.cybercrime.bg и www.gdbop.bg**, администрирани от експерти на дирекцията. Превенцията е важна част от дейността на специализираната дирекция. За намаляване на броя на децата жертви на сексуална експлоатация, периодично се разработват и реализират обучения и семинари с ученици, родители и учители, в т.ч. при партньорство с Националния център за безопасен интернет.

В този смисъл, единствената идентифицирана препоръка е за **осигуряването на повече човешки и технически ресурси** в подкрепа на дейността на дирекция „Киберпрестъпност“ към ГДБОП.

[19] https://sacp.government.bg/%D0%B7%D0%B0-%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8/%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D0%B7%D0%B0

[20] https://www.gdbop.bg/bg/cyber

Закон за МВР[21]

Законът за МВР урежда принципите, функциите и дейностите на министерството, като основната му цел е защита на правата и свободите на гражданите, противодействие на престъпността, опазване на обществения ред и националната сигурност. Законът съдържа **разпоредби, пряко или косвено засягащи защитата на децата в цифрова среда**:

- **Оперативно-издирвателна дейност (чл. 8 - 13)** - МВР има правомощия да извършва оперативно-издирвателна дейност срещу престъпления, включително тези, извършени в цифрова среда. Това включва издирване на лица, които извършват престъпления срещу деца онлайн - като сексуална експлоатация, кибертормоз и други форми на онлайн насилие. Законът предвижда използването на **специални разузнавателни средства** и методи, включително оперативно внедряване и контролирана доставка, които могат да бъдат използвани за разкриване на престъпления в интернет;
- **Информационна дейност (чл. 18 - 25)** - МВР **събира, обработва и предоставя информация**, която може да бъде използвана за защита на децата в цифрова среда. Това включва информация за киберпрестъпления, извършени срещу деца, както и данни за извършителите. Законът предвижда защита на личните данни, което е особено важно при работа с деца;
- **Дейност по превенция (чл. 30а)** - МВР извършва превантивна дейност, насочена към предотвратяване на престъпления, вкл. тези, извършени в цифрова среда. Това включва **мероприятия за установяване и отстраняване на причините и условията за извършване на престъпления срещу деца онлайн**.

Законът не съдържа специфични разпоредби, насочени към защитата на децата от онлайн рискове като кибертормоз, сексуална експлоатация, изнудване и други форми на насилие в цифрова среда. Уредбата в ЗМВР се оценява като **добра и хармонизирана и с правото на ЕС, и с относими нормативни актове като НПК и Закона за киберсигурност**.

Проектният екип обаче констатира **пропуски в изпълнението на разпоредбите на ЗМВР на практика**. Така например, след като отделни случаи на онлайн престъпления срещу деца бъдат докладвани своевременно от дирекция „Киберпрестъпност“ към съответната прокуратура, **понякога по преценка на наблюдаващия прокурор**, въпреки спецификата на реализираното престъпно деяние и в противоречие с нормата на чл. 39, ал. 2, т. 3 от ЗМВР,[22] **провеждането на процесуално-следствените действия се възлага на друга структура в МВР.** Това води до продължаване на работата по случая от служители, които **нямат необходимите практически знания и технически компетенции**.

IV. Национални стратегии и политики за защита на децата в цифровата среда

Проект на Национална стратегия за детето (2024 – 2030 г.) – одобрен от Националния съвет за закрила на детето към ДАЗД на 01.03.2024 г.[23]

Към м. февруари 2025 г. Р. България **вече шеста поредна календарна година е без приета**

[21] https://lex.bg/laws/ldoc/2136243824

[22] Цитираната разпоредба гласи, че ГДБОП е национална специализирана структура за осъществяване на дейностите по отношение на организирана престъпна дейност, свързана с „*компютърни престъпления или престъпления, извършени във или чрез компютърни мрежи и системи, включително и престъпления срещу половата неприкосновеност на личността, извършвани спрямо малолетни и непълнолетни лица чрез използване на информационна или съобщителна технология.*“

[23] https://sacp.government.bg/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B8%D1%8F%D1%82-%D1%81%D1%8A%D0%B2%D0%B5%D1%82-%D0%B7%D0%B0-%D0%B7%D0%B0%D0%BA%D1%80%D0%B8%D0%BB%D0%B0-3

Национална стратегия за детето, в нарушение на чл. 1, ал. 3 от ЗЗДет, съгласно който държавната политика за закрила на детето се осъществява въз основа на приета от Парламента по предложение на Министерския съвет Национална стратегия за детето, изградена върху принципите на този закон.

През 2023 – 2024 г. ДАЗД и междуведомствена работна група към Агенцията изготвиха нов Проект на **Национална стратегия за детето (2024 – 2030 г.), в който ключов тематичен дял е именно закрилата на децата от онлайн посегателства.** Впоследствие, в рамките на 50-тото юбилейно заседание на Националния съвет за закрила на детето, проведено на 01.03.2024 г., **Съветът единодушно прие Проекта на Национална стратегия за детето (2024 – 2030 г.).** Въпреки този напредък, липсва инициирана от действащия редовен кабинет публична дискусия по проекта; не е проведена или планирана разяснителна кампания, посветена на Стратегията, като същевременно **одобреният от НСЗД стратегически документ дори не е достъпен на уебсайта на ДАЗД**, което сериозно ограничава възможностите за обществено участие и експертен дебат.

НМД от години системно се застъпва за приемането на този така необходим рамков документ, очертаващ едрите линии на политиките за децата и семействата, вкл. на междусекторното взаимодействие в гарантирането на правата и най-добрите интереси на всяко дете. Въпреки постигнатото до момента, липсата на политическа воля за реално придвижване на процеса по финализиране (в т.ч. надграждане в тематичния дял, посветен на онлайн безопасността) и приемане на Стратегията остава сериозен риск, който изисква **засилени застъпнически усилия и граждански натиск** върху отговорните институции.[24]

Национална програма за превенция на насилието и злоупотребата с деца (2023 – 2026 г.)[25]

В началото на 2023 г. Министерският съвет прие прие Национална програма за превенция на насилието и злоупотребата с деца (2023-2026 г.) и **План за действие за нейното изпълнение за периода 2023-2024 г.**[26]

Националната програма и Планът за действие **адресират проблема на онлайн посегателствата срещу деца** и предвиждат мерки и дейности за реакция срещу кибертормоза, сексуалната експлоатация и другите форми на насилие над деца в интернет. Така например, Оперативна цел № 5 от Плана касае **гарантиране правото на закрила на децата от насилие чрез информационните и комуникационните технологии**.

Към тази цел попадат следните подцели, както следва:

- **5.1. Развиване на дигитално-медийна грамотност на учениците в часовете и извънкласните дейности**, вкл. чрез разработване и прилагане на дигитални иновации и платформи за развитие на дигитално-медийна грамотност;
- **5.2. Получаване и обработка на сигнали за онлайн насилие над деца** чрез Гореща линия на Националния център за безопасен интернет;
- **5.3. Обучения на ученици от всички образователни етапи по теми, свързани с онлайн рисковете** като онлайн тормоз, секстинг, онлайн сексуална експлоатация, сексторшън, непознати в мрежата, сигурност и хакнати профили;
- **5.4. Провеждане на обучителна програма „Киберскаути“** в училищата в България;

[24] https://nmd.bg/nszd-odobri-proekta-na-naczionalna-strategiya-za-deteto-2024-2030-g/
[25] https://sacp.government.bg/%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8/%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0-%D0%B7%D0%B0-8
[26] https://nmd.bg/pravitelstvoto-prie-naczionalna-programa-za-prevencziya-na-nasilieto-i-zloupotrebata-s-decza-2023-2026-g/

- **5.5.** Провеждане на **кампания за повишаване на информираността на родители, учители и професионалисти** по отношение на онлайн рисковете и превенцията на насилието в Интернет.

Като отговорна институция в Плана за действие по тези пера е **посочен именно НЦБИ**, което е индикативно за ценността на работата на Центъра.

Същевременно, подобно посочване подчертава **неприемливата текуща ситуация**, при която Центърът **изпълнява държавна политика и ангажименти на Р. България по няколко директиви на ЕС и международни конвенции, обект е на възлагане на отговорности по национални рамкови документи и планове за действие**, но продължава да няма подкрепа от държавата и да разчита на дарителски акции от дружества и на ограничена проектна подкрепа от ЕС.

На следващо място, посочените стратегически документи търпят критика поради **липса на конкретика** в индикаторите и на **ясни връзки между цел, мярка и резултат**.

Понастоящем (м. февруари 2025 г.) се осъществява междуведомствена работа по разписването на **План за действие за 2025 – 2026 г.**, при координация от ДАЗД, като проектният консорциум по „Дигитални деца“ се застъпва за **прецизиране на целите (стратегически и оперативни) и на мерките, касаещи онлайн безопасността**, както и за това Планът да бъде **структуриран с оглед на вече постигнатите** при изпълнението на предходния план резултати.

V. Съвместимост на законодателство и политики с международни стандарти и конвенции и с правото на Европейския съюз

ix. Конвенция на ООН за правата на детето. Общ коментар № 25 на Комитета по правата на детето на ООН[27]

Конвенцията за правата на детето на ООН (КПД), приета през 1989 г. и ратифицирана от Р. България през 1991 г., е **най-широко ратифицираният международен договор в областта на правата на човека.** Тя утвърждава основните права на всички деца, вкл. правото на живот, развитие, **защита от насилие** и участие в обществения живот. Конвенцията задължава държавите да осигурят най-добрите интереси на детето във всички политики и решения, които засягат децата. Чрез нея се създава международна рамка за защита на децата и насърчаване на техните права. Много от ръководните начала, възведени в КПД, могат да бъдат приложени към въпросите на дигиталната сигурност на децата.

Така например, чл. 16 предвижда **защита срещу незаконна намеса в личния живот на детето**, което може да бъде приложено към онлайн среда; чл. 17 признава **важната роля на средствата за масова информация** и насърчава достъпа на децата до подходяща информация; чл. 19 задължава държавите да предприемат всички необходими мерки за **закрила на децата от всякакви форми на насилие**, включително психологически тормоз и злоупотреба; чл. 28 и чл. 29 гарантират правото на образование и подготовката на детето за **активен и информиран живот** в обществото (в съвременния контекст това неминуемо включва обучението по дигитална грамотност, киберсигурност и критично мислене в онлайн среда); чл. 34 изисква от държавите **да защитават децата от сексуална експлоатация**; а общата норма на чл. 36, на свой ред, прогласява **защитата на децата срещу всички други форми на експлоатация**, засягащи в какъвто и да е аспект благосъстоянието на детето.

В допълнение, ключов е **Общ коментар № 25 (2021 г.)** на Комитета по правата на детето на ООН относно **правата на децата във връзка с цифровата среда**.[28]

---

[27] https://www.unicef.org/bulgaria/sites/unicef.org.bulgaria/files/2018-09/CRC_bg.pdf
[28] https://www.unicef.org/bulgaria/media/10591/file

Комитетът по правата на детето е орган, създаден съгласно КПД, който има мандат да следи за прилагането на Конвенцията и нейните факултативни протоколи от държавите, страни по нея. Комитетът **постановява общи коментари**, за да тълкува и разяснява как правата на децата следва да бъдат гарантирани в контекста на различни социални, икономически и технологични промени.

Общ коментар № 25 (2021) се фокусира върху правата на децата в цифровата среда, като изяснява **как държавите следва да прилагат Конвенцията с оглед на предизвикателствата и възможностите, които дигитализацията носи**. Документът подчертава, че цифровата среда засяга почти всички аспекти от живота на децата и че достъпът до дигитални технологии е **неразривно свързан с упражняването на пълния каталог от граждански, политически, социални, културни и икономически права на децата.** Въпреки че цифровите технологии могат да подобрят достъпа на децата до образование, информация и услуги, те също така създават рискове, вкл. от експлоатация, нарушаване на личното пространство, дискриминация и неравен достъп до дигитални ресурси.

Коментарът подчертава четири основни принципа, които държавите следва да спазват в регулирането на цифровата среда, а именно: **недискриминация, гарантиране на висшите интереси на детето, на правото на живот, оцеляване и развитие, както и на правото на участие на децата** в процесите, засягащи тяхното бъдеще. Специално внимание е отделено на обстоятелството, че цифровата среда не е проектирана изначално за деца, но те все по-често взаимодействат с нея, което изисква **специфични регулаторни мерки за защита на правата им.**

Сред ключовите препоръки на Комитета е държавите да приемат законодателство, което **интегрира защитата на детето в политиките за цифровата среда**, вкл. **мерки срещу онлайн експлоатацията, насилието и дезинформацията**. Националните политики следва да гарантират, че децата имат безопасен и равен достъп до интернет и цифрови технологии, като се избягва задълбочаване на социалните и икономическите неравенства.

Комитетът също така препоръчва по-голямо участие на технологичните компании в усилията за защита на децата, чрез прилагане на принципите на защита **още на етапа на проектиране на дигиталните платформи.** Общ коментар № 25 подчертава, че държавите носят основната отговорност за закрилата на децата в цифровата среда, но също така призовава за **съвместни усилия от страна на частния сектор, гражданското общество и международните организации** за изграждането на безопасно и приобщаващо цифрово пространство за децата.

x. Конвенция на Съвета на Европа за закрила на децата срещу сексуална експлоатация и сексуално насилие[29]

Конвенцията на Съвета на Европа за защита на децата срещу сексуална експлоатация и сексуално насилие (Конвенцията от Ланзароте, 2007 г.) е правнообвързващ международен документ, който **задължава държавите да инкриминират всички форми на сексуална злоупотреба с деца, включително тези, извършени чрез интернет и дигитални технологии.**

Конвенцията подчертава, че нарастващото използване на информационни и комуникационни технологии (ИКТ) **улеснява разпространението на материали със сексуална експлоатация на деца** и създава нови предизвикателства за превенцията и наказателното преследване.

Чл. 20 на Конвенцията предвижда приемането на **задължителни наказателни разпоредби** срещу:

- **Производство, разпространение, предлагане и предаване на материали със сексуална експлоатация на деца**;

[29] https://rm.coe.int/168046e1e6

- **Съзнателен достъп до материали със сексуална експлоатация на деца чрез ИКТ**. Детската порнография (анахроничен термин – бел. авт.) се дефинира като **всяко визуално изобразяване на дете, участващо в сексуални действия**, включително **симулирани или дигитално генерирани изображения.**

Конвенцията изисква държавите да въведат:

- **Специализирани механизми за разследване** на престъпления, вкл. възможност за анализ на материали, разпространявани чрез ИКТ;
- **Сътрудничество с частния сектор** – телекомуникационни оператори, интернет доставчици и дигитални платформи следва да прилагат политики за предотвратяване и докладване на сексуална експлоатация;
- **Закрила на жертвите** чрез горещи телефонни линии и психологическа подкрепа за деца, пострадали от онлайн насилие.

Конвенцията насърчава **сътрудничеството между държавите в разследването и наказването на трансгранични случаи**, включително посредством обмен на информация и екстрадиция на извършители.

Така Конвенцията от Ланзароте очертава **солидна правна рамка** за борба с онлайн сексуалната експлоатация на деца. Успешното ѝ прилагане зависи от ефективното сътрудничество между държавните институции, технологичния сектор и гражданското общество. Р. България, страна по Конвенцията, следва да гарантира стриктното ѝ прилагане, като **засили мониторинга върху дигиталните платформи**.

xi. Директива 2011/93/ЕС за борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография[30][31]

Директива 2011/92/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие, сексуалната експлоатация на деца и детската порнография представлява основен правен инструмент на ЕС за защита на децата от този вид тежки престъпления. Директивата заменя Рамково решение 2004/68/ПВР и въвежда **по-строги наказателноправни разпоредби, засилени мерки за подпомагане на жертвите и механизми за международно сътрудничество**.

В контекста на онлайн безопасността на децата, директивата поставя акцент върху **наказателното преследване на престъпления, извършени чрез интернет**, като детска порнография, установяване на контакт с деца за сексуални цели (*grooming*) и незаконен достъп до материали, съдържащи сексуална експлоатация на деца.

Директивата задължава държавите членки **да инкриминират всички форми на детска порнография**, включително:

- **Създаване, разпространение и съхранение** на порнографски материали с участие на деца (чл. 5);
- **Съзнателен достъп** до детска порнография чрез интернет (чл. 5, ал. 3);
- **Притежание и придобиване** на подобни материали (чл. 5, ал. 2).

Тези разпоредби засилват ангажимента на държавите членки да разширят мерките за разследване и наказателно преследване на престъпления, свързани с онлайн разпространението на порнографски

[30] https://eur-lex.europa.eu/eli/dir/2011/93/oj?locale=bg
[31] https://www.europarl.europa.eu/doceo/document/A-8-2017-0368_BG.html

материали с участие на деца.

Директивата въвежда **криминализацията на практиката за установяване на контакт с деца за сексуални цели чрез интернет платформи, социални мрежи и комуникационни приложения (чл. 6).**[32] Това престъпление обхваща предложение от възрастен да се срещне с дете с намерение за сексуална експлоатация.

Директивата насърчава държавите членки да предприемат **ефективни мерки за премахване или блокиране на достъпа до уебсайтове, съдържащи материали със сексуална експлоатация на деца**, особено когато сървърите са разположени в трети държави (чл. 25).[33]

Държавите се насърчават **да сътрудничат с интернет доставчици и технологичния сектор** за разработване на механизми за филтриране и премахване на незаконно съдържание.

Макар директивата да не предвижда конкретни задължения за социалните мрежи и технологичните компании, тя подчертава нуждата **частният сектор да участва активно в превенцията и докладването на престъпления срещу деца в интернет (чл. 24)**. Телекомуникационните компании и онлайн платформи следва да сигнализират за случаи на разпространение на материали с детска порнография. Въпреки това, като минус се отчита **липата на очертан от директивата задължителен механизъм** за отчетност на частния сектор пред националните органи по отношение на сигурността.

Директивата поставя изискване държавите членки да гарантират **безплатна правна и психологическа подкрепа за децата жертви (чл. 16-20).** Жертвите на онлайн сексуална експлоатация следва да имат достъп до специализирани социални и рехабилитационни услуги. Нормирано е правото на **анонимни телефонни и интернет линии за помощ**, чрез които децата да могат да съобщават за злоупотреби.

Директивата изисква от държавите членки да гарантират конфиденциалност на самоличността на жертвите в съдебните производства (чл. 23). Националните органи следва да прилагат **специални мерки за предотвратяване на вторична виктимизация** на децата в хода на съдебните производства.[34]

Макар директивата да подчертава ролята на технологичните компании, тя не въвежда задължителни изисквания за мониторинг и докладване на случаи на сексуална експлоатация в социалните мрежи. Директивата насърчава държавите членки да си сътрудничат с трети страни за блокиране и премахване на незаконно съдържание, но липсват конкретни механизми и гаранции за ефективно прилагане (чл. 25). Практиката показва, че **някои юрисдикции извън ЕС отказват да съдействат за разследване на онлайн престъпления**, което затруднява проследяването на извършителите. Държавите членки прилагат различни практики за разследване на интернет престъпления, което намалява ефективността на трансграничните разследвания.

Така например, **липсват единни насоки за използване на разузнавателни технологии за разследване на престъпления срещу деца** в дигиталната среда.

Ефективното прилагане на Директива 2011/92/ЕС изисква **по-ясни механизми за мониторинг на социалните мрежи, по-строго взаимодействие с технологичния сектор и засилено презграничо сътрудничество.**

32 Вж. анализа на относимите разпоредби на НК по-горе.

33 Вж. анализа на дейността на дирекция „Киберпрестъпност“ по-горе.

34 Вж. анализа на относимите разпоредби на НПК и ЗПФКПП по-горе.

xii. Европейска стратегия за по-добър интернет за децата (2022 г.) (BIK+)[35]

Европейската стратегия за по-добър интернет за децата (BIK+) е актуализирана стратегия на ЕС, която цели да **гарантира безопасен, приобщаващ и овластяващ дигитален свят за децата.** Тя е част от **визията на ЕС за цифровото десетилетие (2020 – 2030 г.)**[36] и се основава на три основни стълба:

4. **Безопасен дигитален опит** – осигуряване на защита от вредно съдържание, кибертормоз и онлайн експлоатация чрез законодателни мерки, включително Директивата за аудиовизуалните медийни услуги и Акта на ЕС за цифровите услуги;
5. **Дигитално овластяване** – повишаване на цифровата грамотност чрез обучения за деца, родители и учители, както и подобряване на механизмите за проверка на възрастта и защита на личните данни;
6. **Активно участие** – гарантиране на правото на децата да бъдат чути в процеса на създаване на дигитални политики, включително чрез детски консултативни панели.

Стратегията насърчава сътрудничеството между държавите членки, технологичните компании и гражданския сектор, за да се изгради по-безопасна и достъпна дигитална среда за всички деца в ЕС. Основната роля на държавите, очертана от Стратегията, е **да прилагат съществуващото европейско законодателство, да разработват национални стратегии и да инвестират в образование и дигитална защита за децата**, като конкретно:

- Държавите членки следва да прилагат в пълнота **Акта на ЕС за цифровите услуги (DSA)**, който задължава платформите да предприемат мерки за защита на децата, включително забрана на таргетирана реклама въз основа на профилиране на деца;
- Изпълнение на **Директивата за аудиовизуалните медийни услуги (AVMSD)**, която изисква от платформите за видеосподеляне да защитават децата от вредно съдържание;
- Държавите членки се приканват да подкрепят създаването на **Национални стратегии за онлайн безопасност на децата;**
- Подобряване на механизмите за **проверка на възрастта** и гарантиране на съвместимост с Европейската цифрова идентичност (eID);
- ЕС съфинансира националните центрове за безопасен интернет, но държавите членки са насърчени да осигурят **допълнително финансиране и подкрепа** за тях;
- Центровете за безопасен интернет в ЕС предлагат обучения за деца, родители и учители, както и платформи за сигнализиране на незаконно съдържание;
- Включване на **обучения по цифрова грамотност** в националните учебни програми;
- Специален фокус е поставен върху **обучение на уязвими групи деца** (деца с увреждания, социално изключени и др.);
- Държавите членки следва да докладват напредъка си в изпълнението на BIK+ чрез **Експертната група за по-безопасен интернет**;
- Поощрява се създаването на **механизми за сътрудничество** между правителствата, технологичния сектор и гражданското общество.

Заложените в Европейската стратегия за по-добър интернет за децата (BIK+) принципи, норми и цели неминуемо подчертават **необходимостта Националният център за безопасен интернет да получи устойчива държавна подкрепа.**

xiii. Стратегия на Европейския съюз за по-ефективна борба със сексуалното насилие над

35 https://digital-strategy.ec.europa.eu/bg/policies/strategy-better-internet-kids

36 Вж. Първи доклад за състоянието на цифровото десетилетие (2023 г.) и анекс, посветен на оценка на ситуацията в Р. България (https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade)

деца[37]

Стратегията на ЕС за по-ефективна борба със сексуалното насилие над деца представлява цялостна рамка от мерки, насочени към **превенция, разследване и защита** на жертвите, като съчетава законодателни инициативи, технологични решения и междусекторно сътрудничество. Стратегията обхваща **периода 2020-2025 г.** и включва осем ключови инициативи, насочени към превенция, разследване и подкрепа за жертвите. Конкретни ангажименти за държавите членки, произтичащи от Стратегията, включват:

- **Прилагане на Директива 2011/93/ЕС:** държавите членки следва да завършат транспонирането на директивата, която установява минимални правила за определяне на престъпленията и санкциите в областта на сексуалното насилие над деца. Това включва мерки за превенция, разследване и подкрепа за жертвите;
- **Укрепване на правоприлагането:** държавите членки следва да създадат **специализирани екипи за установяване на жертви** и да инвестират в технически възможности за разследване на онлайн престъпления. Също така, следва да се осигурява системният обмен на разузнавателни данни с Европол;
- **Превентивни мерки:** държавите членки следва да въведат **програми за превенция, насочени към потенциални извършители**, и да повишат осведомеността сред деца, родители и професионалисти. Това включва и обучение за разпознаване на ранни признаци на насилие;
- **Създаване на Европейски център за предотвратяване и противодействие на сексуалното насилие над деца:** Центърът ще подкрепя държавите членки в борбата с насилието чрез координация, превенция и подкрепа за жертвите;
- **Ангажираност на технологичния сектор:** държавите членки следва да насърчават онлайн платформите **да откриват и докладват случаи** на сексуално насилие над деца, включително в криптирани съобщения, при спазване на основните права и свободи на гражданите на Съюза;
- **Международно сътрудничество:** държавите членки следва да участват в глобални инициативи като **Световния алианс WeProtect** за повишаване на международното сътрудничество за защита на децата.

Националните държави членки са ангажирани да прилагат тези мерки и да сътрудничат на европейско и глобално ниво за по-ефективна защита на децата.

xiv. Акт на ЕС за цифровите услуги (Регламент (ЕС) 2022/2065)[38]

Регламент (ЕС) 2022/2065 или **Актът за цифровите услуги (Digital Services Act – DSA)**, е законодателен акт на ЕС, който регулира **отговорностите на онлайн платформите и посредническите услуги (в т.ч. Viber, WhatsApp, YouTube и др.)**, като цели да осигури по-безопасна и по-прозрачна цифрова среда. Регламентът въвежда изисквания за модериране на незаконно съдържание, защита на потребителите и мерки срещу дезинформацията.

За осигуряване на ефективен надзор и прилагане на Регламент (ЕС) 2022/2065 в рамките на Единния цифров пазар беше създаден **Европейски съвет за цифровите услуги**, като всяка държава членка определи национален координатор. В Р. България тази роля следва да се изпълнява от **Комисията за регулиране на съобщенията (КРС), която отговаря за контрола върху доставчиците на посреднически услуги**, с изключение на много големите онлайн платформи, които са под надзора пряко на Европейската комисия.

37 https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:52020DC0607

38 https://www.consilium.europa.eu/bg/policies/digital-services-act/

Както всеки законодателен акт със статут на регламент, Актът за цифровите услуги е **задължителен в своята цялост и произвежда т.нар. директен ефект**, т.е. не изисква транспониране,[39] но същевременно националното законодателство следва да бъде хармонизирано с него, като се регламентират предвидените в Акта механизъм и структури на национално ниво, осигуряващи **ефективен надзор, сътрудничество и правоприлагане**, което **към началото на 2025 г. все още е не е реализирано в пълнота в Р. България.**

Така например, към момента на завършване на настоящия доклад **остава негласуван в пленарна зала от 51-ото НС одобреният с Решение № 829 на Министерския съвет от 2024 г. проект на Закон за изменение и допълнение на Закона за електронните съобщения (ЗЕС)**, който има за цел да осигури прилагането на изискванията на Регламент (ЕС) 2022/2065 и така да гарантира **по-добър надзор на държавата върху дейността на доставчиците на посреднически информационни услуги**, респ. по-добра защита на децата онлайн.

ЗИД на ЗЕС **регламентира функциите и правомощията на компетентните органи, включително Съвета за електронни медии (СЕМ) и Комисията за защита на личните данни.** Съветът за електронни медии е компетентен орган по чл. 49 от Регламента предоставянето на посреднически услуги на информационното общество по смисъла на Акта, които представляват платформи за споделяне на видеоклипове. Комисията за регулиране на съобщенията, на свой ред, следва да осъществява контрол върху дейността на доставчиците на посреднически услуги на информационното общество, които не представляват платформи за споделяне на видеоклипове, за изпълнение на задълженията им по регламента.

Законопроектът предвижда въвеждането на **механизми за сертифициране на органи за извънсъдебно решаване на спорове между онлайн платформи и потребители**, както и **процедури за получаване на статут на доверен подател на сигнали и одобрен изследовател.** КРС получава правомощие да разследва съответствието на сертифицираните органи и на изследователите. Предвиждат се мерки за ограничаване на достъпа до цифрови услуги при установени нарушения, както и **процедури за предварително изпълнение на определени решения**. Въвежда се **специален ред за установяване на нарушения и налагане на санкции**, който цели по-ефективен и бърз контрол, като същевременно се запазват гаранциите за правото на защита.

Предвижда се създаване на **специална процедура, различна от тази по Закона за административните нарушения и наказания (ЗАНН), по която да бъдат установявани нарушенията на регламента.** С предложения нов ред за установяване на нарушения се цели оптимизиране на процедурата по налагане на административната глоба/имуществената санкция, с което ще се постигнат целите по съображения 114 и 117 от регламента, по-специално – **държавите членки следва да гарантират, че нарушенията на задълженията по регламента могат да бъдат санкционирани по начин, който е ефективен, пропорционален и възпиращ.** В тази връзка установяването на нарушенията и налагането на наказанията ще се осъществява в една административна процедура, с издаването на един документ – **решение на КРС за установяване на нарушението и налагане на наказанието.**

Цели се и своевременност при осъществяването на отговорността за нарушения на регламента чрез създаването на процес по установяване на извършените нарушения, който е по-бърз и по-ефективен. Чрез предложения специален ред ще се редуцират възможностите за избягване на отговорността по регламента, като същевременно се **запазват гаранциите за правото на защита**

[39] https://www.europarl.europa.eu/factsheets/bg/sheet/6/%D0%B8%D0%B7%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D1%86%D0%B8-%D0%B8-%D0%BE%D0%B1%D1%85%D0%B2%D0%B0%D1%82-%D0%BD%D0%B0-%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D1%82%D0%BE-%D0%BD%D0%B0-%D0%B5%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B8%D1%81%D0%BA%D0%B8%D1%8F-%D1%81%D1%8A%D1%8E%D0%B7

чрез обжалване на решението по реда на Административнопроцесуалния кодекс. (Подобен подход е познат на българското законодателство. **Аналогична уредба** действа и към момента в Закона за защита на конкуренцията,[40] в Закона за енергетиката,[41] в Указ № 904 от 28.12.1963 г. за борба с дребното хулиганство[42] и др.). Проектът е съобразен и с изискването на чл. 52 от Акта, задължаващ държавите членки да установят система от санкции, които трябва да бъдат **ефективни, пропорционални и възпиращи**, и проектният екип се застъпва за срочното му приемане.[43]

xv. Акт на ЕС за изкуствения интелект (Регламент (ЕС) 2024/1689)[44]

Регламент (ЕС) 2024/1689 има за цел да установи **единна правна рамка** за развитието, предлагането и използването на **системи с изкуствен интелект (ИИ)** в Европейския съюз. Основният фокус е да се гарантира, че ИИ се прилага по начин, който защитава основните права на гражданите, вкл. тези на децата, като същевременно насърчава иновациите. Регламентът изисква от държавите членки да въведат **хармонизирани мерки за защита срещу вредните последици от ИИ**, особено що се отнася до високорисковите системи.

Регламентът признава специфичната уязвимост на децата в цифровата среда и включва разпоредби, които се отнасят до защитата им, вкл. следното:

- Регламентът въвежда задължение за съобразяване с правата на децата, предвидени в **чл. 24 на Хартата на основните права на ЕС** и **Конвенцията на ООН за правата на детето**. Това означава, че всяка система с ИИ, която може да засегне деца, трябва да бъде проектирана с оглед на техните най-добри интереси;
- Специално се взема предвид **Общ коментар № 25 на Комитета по правата на детето** относно правата на децата в цифровата среда, което подчертава необходимостта от засилена защита срещу експлоатация, дискриминация и манипулация чрез ИИ;
- Ограничават се **манипулативните практики**, които могат да въздействат на децата, като например **алгоритми, създаващи зависимост** от дигитални услуги или **изкуствено насочващи децата към определено съдържание или поведение**.

Въпреки че регламентът поставя основите за по-добра защита на децата онлайн, няколко важни аспекта остават уредени недостатъчно прецизно:

- **Липса на конкретни мерки за социалните мрежи и платформи** – докато в регламента се споменава защитата на децата, няма достатъчно конкретни изисквания към компаниите, управляващи платформи, които използват ИИ за персонализирано съдържание;
- **Неясни санкционни механизми** – въпреки че регламентът въвежда задължения за защита на децата, няма ясно разписани санкционни норми с адресат компаниите, които потенциално могат да нарушат режима, въведен с Регламента;
- **Недостатъчно разграничаване на различните рискове за децата** – ИИ може да бъде използван за различни цели, вкл. образователни, но няма ясно разграничаване между ползотворните и вредните приложения на тази технология. В основната на регламента са залегнали не стандартите за защита на основните права като подход за оценка на безопасността на ИИ системите, а различен подход – основан на 4 нива на риск, което **ще направи нарушаването на права по-трудно установимо**.[45]

[40] https://lex.bg/laws/ldoc/2135607845
[41] https://lex.bg/laws/ldoc/2135475623
[42] https://lex.bg/bg/laws/ldoc/-1632842751
[43] https://nmd.bg/s-pismo-do-ministerski-savet-nmd-nastoyava-za-18-speshni-merki-v-podkrepa-na-deczata-i-semejstvata-v-balgariya/
[44] https://eur-lex.europa.eu/legal-content/bg/ALL/?uri=CELEX:32024R1689
[45] Банова-Стоева, Р., „Актът за ИИ – пропуски и възможности от правозащитна гледна точка“, БЦНП, 2024 г. (https://bcnl.org/)

xvi. Директива (ЕС) 2024/1385 на Европейския парламент и на Съвета от 14.05.2024 г. относно борбата с насилието над жени и домашното насилие[46]

Директива (ЕС) 2024/1385 на Европейския парламент и на Съвета от 14 май 2024 г. има за цел да осигури **единна правна рамка за предотвратяване и борба с насилието над жени и домашното насилие** в целия ЕС. Тя въвежда мерки като определяне на **каталог от престъпления и наказания**, защита на жертвите и достъп до правосъдие, подкрепа за жертвите, събиране на данни, превенция, координация и сътрудничество. Директивата признава, че насилието над жени и домашното насилие представляват нарушения на основните права, в т.ч. правото на човешко достойнство, живот и неприкосновеност на личността, и подчертава необходимостта от **специални мерки за защита на уязвимите групи, вкл. децата**, които често са засегнати пряко или косвено от подобно насилие.

Транспонирането на директивата (с краен срок **до 13.06.2027 г.**) ще включва въвеждането на допълнителни престъпни състави, като част от тези деяния са свързани с престъпни посегателства в цифрова среда - **споделяне на интимен или манипулиран материал без съгласие** (в т.ч. манипулиран интимен материал, **генериран от ИИ**), **наблюдение, киберфлашинг (изпращане на непоискано сексуално съдържание), доксинг (разкриване на лична информация, пароли, геолокация и т.н.), кибер подбуждане към насилие и омраза** и др. Към всяко деяние, което следва да бъде инкриминирано, има списък от отегчаващи обстоятелства – едно от които е именно **жертва на престъплението да е дете.**

Проектният екип счита, че въвеждането на директивата ще спомогне за **надграждане и усъвършенстване на нормативната база**, осигуряваща закрилата на деца в цифрова среда, и се ангажира да проследява и подкрепя експертно процеса по транспониране.

VI. Списък с ключови препоръки, на основа проведения анализ

На база изложените по-горе констатации, проектният екип извежда следната **система от препоръки** за подобряване на нормативната база и институционалното сътрудничество, гарантиращи превенцията, разкриването и наказването на престъпни посегателства срещу деца в цифрова среда, а именно:

- Да се **подобри ефективността на мултидисциплинарните екипи на местно ниво по прилагане на Координационния механизъм при насилие (чл. 36г)** чрез: осигуряване на необходимите финансови, технически и допълнителни човешки ресурси за ефективната работа на екипите; създаване на единна информационна система, в която да е видно какви цели и дейности са заложили за изпълнение всички ангажирани институции; ясно дефиниране на ролите и отговорностите на екипите и избягване на текучеството и несъгласуваността; предоставяне на **подробни методически указания за работа по случаи на онлайн насилие и експлоатация**; провеждане на редовни съвместни обучения и работни срещи на представителите на различните институции за работа по Координационния механизъм, вкл. **с предмет онлайн посегателства и рискове за децата**;
- По модела на чл. 5б „Специализирана закрила на деца на обществени места“ от ЗЗДет, в

[46] https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:32024L1385

закона да бъде нормирана **нова разпоредба с наименование „Специализирана закрила на деца в онлайн среда“**, като в т.ч. **условията и реда за гарантиране на този вид специализирана закрила бъдат определени с нарочна наредба на Министерския съвет;**

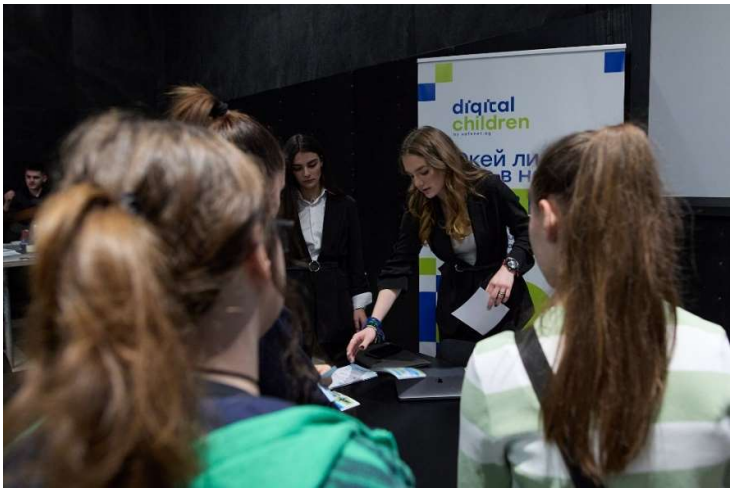
- Да бъдат предприети мерки, чрез които да се **реформира и укрепи в спешен порядък системата на закрила на детето**, като се повиши нейният капацитет (изисквания за специализирано висше образование и професионални стандарти при подбора на служителите в ОЗД; осигуряване на качествена подготовка и ресурсна обезпеченост, както и на последващи обучения, супервизия, атестация и др.);
- Да бъде приета **единна методологическа рамка** в подкрепа на съдии, разглеждащи наказателни дела за посегателства срещу деца в цифрова среда, с което да се избегне противоречивата съдебна практика (да се въведе яснота относно допустимите събирани с електронни средства доказателства, правилата относно подсъдността и др.);
- В НПК да бъде регламентиран **механизъм за запознаване на полицейската структура, водила проверката, при наличие на отказ за образуване на наказателно производство**, който да дава възможност на експертите да обжалват получените откази пред по-горна инстанция;
- Да бъде **прецизирана общата дефиниция за „компютърни информационни системи” в НПК**, с цел ясно диференциране на киберсъдържание със злоупотреба с и над деца, съдържание със сексуална експлоатация и пр.;
- Да се осигуряват достатъчно специализирани обучения за прокурори и магистрати, които да повишават техните **познания и чувствителност** по отношение на онлайн посегателствата над деца;
- Да се въведе в ЗПФКПП възможност **организациите за подкрепа на пострадали**, установили първоначален контакт с жертвата, **да извършват индивидуалните оценки**;
- Да бъде приет одобреният с Решение № 829 на Министерския съвет от 2024 г. **проект на ЗИД на ЗЕС,** който има за цел да усъвършенства текста на закона, като осигури прилагането на изискванията на Регламент (ЕС) 2022/2065 на ЕС и така повиши надзора на държавата върху дейността на **доставчиците на посреднически информационни услуги**;
- Да бъде надградена закрилата, осигурявана съгласно ЗЕС, така че да се изисква от платформите да предотвратяват и премахват вредно съдържание, вкл. чрез по-добър контрол на алгоритмите. В изпълнение на европейското и национално законодателство, държавата да насърчава платформите да интегрират и отчитат ефективни **safety by design**

(„безопасност по дизайн“) алгоритми, политики и правила;

- Да бъде **надградена нормативната основа за защита на личните данни на децата чрез промени в ЗЗЛД**, които да гарантират прилагането на **надеждни механизми за проверка на възрастта** при регистрация в социални мрежи и ползване на дигитални услуги; яснота относно режима от задължения на платформите и интернет доставчиците да предприемат **мерки за защита на данните**; възможности за **бърза реакция** при нарушения като изтичане на данни или онлайн злоупотреба с лична информация;
- Да бъдат осигурени по-големи човешки и технически ресурси в **подкрепа на дейността на дирекция „Киберпрестъпност“ към ГДБОП**;
- Да се гарантира съблюдаване на нормата на чл. 39, ал. 2, т. 3 от ЗМВР, така че провеждането на **процесуално-следствените действия** по дела, свързани с онлайн посегателства срещу деца, да бъде възлагано **единствено на структури в МВР с необходимите технически компетенции**;
- Да бъде **актуализирана (в т.ч. с надграждане в тематичния дял, посветен на онлайн безопасността на децата) и приета** изработената през 2024 г. от междуведомствена работна група, на основание чл. 1, ал. 3 от ЗЗДет. и решение на Съвета за развитие към МС, и одобрена на 01.03.2024 г. от Националния съвет за закрила на детето към ДАЗД, **Национална стратегия за детето (2024-2030 г.)**;
- Да бъде приет **План за действие за 2025 – 2026 г.** към Националната програма за превенция на насилието и злоупотребата с деца (2023-2026 г.), който да съдържа **прецизирани стратегически и оперативни цели и ясни мерки**, касаещи онлайн безопасността на децата, и който да е структуриран съобразно вече постигнатите от изпълнението на предходния план конкретни резултати;
- Да бъде **транспонирана в пълнота Директива (ЕС) 2024/1385** за предотвратяване и борба с насилието над жени и домашното насилие, като по този начин бъде **надградена и усъвършенствана нормативната база**, осигуряваща превенция, разкриване и наказване на престъпления срещу деца в цифрова среда;
- Да се осигури **широко и съдържателно включване на темата за дигитално-медийната грамотност и безопасния интернет** в учебните програми;
- Да бъдат формулирани, приети и прилагани повече мерки, насочени към **подобряване на детското психично здраве**, в контекста на увеличаващите се случаи на кибертормоз над деца;
- Да бъде осигурено **устойчива държавна подкрепа за Националния център за**

безопасен интернет, който изпълнява държавна политика и ангажименти на Р. България по няколко директиви на ЕС и международни конвенции, и е обект на възлагане на отговорности по национални рамкови документи и планове за действие;

- Да бъде гарантирано, в изпълнение на Общ коментар № 25 на Комитета по правата на детето на ООН, **автентично детско и младежко гражданско участие** в създаването, мониторинга и оценката на законодателство и политики за онлайн безопасност.



Снимка: Отбелязване на Международния ден за безопасен интернет на НЦБП по проект „Дигитални деца“, водено от представители на Младежкия панел към Центъра и младежи-доброволци от Дирекция превенции на Община Варна – 11.02.2025 г. | Фотограф: Антон Василев

VII. Обвързаност на Аналитичния доклад с Политическия документ по проект „Дигитални деца“

На основата на настоящия Аналитичен доклад, в кратки срокове ще бъде изготвен **Политически документ**, който ще представи констатираните пропуски и празноти в регулаторната рамка, наред с препоръките за подобряване на защитата на децата в дигиталната среда, под формата на **План за действие („*Action Plan*“), адресиран към законодателя и институциите.**

Това ще осигури **ясен път за институционална отговорност и ефективен мониторинг на напредъка** в областта на дигиталната безопасност на децата.

Национална мрежа за децата, Асоциация „Родители“ и Българската асоциация по семейно планиране и сексуално здраве ще представят и обосноват пред народни представители и институции констатациите и препоръките от Аналитичния доклад и Политическия документ и ще се застъпват за усъвършенстване на нормативната рамка, институционалната работа и политиките за закрила. В допълнение, ключова цел на проектния екип по „Дигитални деца“ е Планът за действие в Политическия документ да бъде **актуализиран в динамика** в хода на пълния срок на проектно изпълнение, на база продължаващия **текущ проектен мониторинг и анализ на законодателство и политики**.

дигитални деца by safenet.bg

гр. София, февруари 2025

Project: 101158515 "Digital Children: Protecting and Empowering Children in Digital Environment" - DIGITAL-2023-DEPLOY-04

Deliverable D5.1 – Analytical Report

Финансирано от Европейския съюз. Изразените възгледи и мнения са само на автора(ите) и не отразяват непременно тези на Европейския съюз или Европейската изпълнителна агенция за здравеопазването и цифровизацията (HaDEA). Нито Европейският съюз, нито HaDEA могат да носят отговорност за тях.