

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

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

- i. Проект „Дигитални деца“ и Дейност 5 („Work Package 5“) от проектното изпълнение:
 - ✓ За НЦБИ и проектния консорциум
 - ✓ Основни цели на Дейност 5 от проектното изпълнение и на Застъпническия план. Цели и обхват на доклада

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

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

• Закон за закрила на детето
• Наказателен кодекс и Наказателно-процесуален кодекс
• Закон за подпомагане и финансова компенсация на пострадали от престъпления (ЗПФКПП)
• Закон за електронните съобщения
• Закон за защита на личните данни
• Закон за киберсигурност. Дирекция „Киберпрестъпност“ към ГДБОП
• Закон за МВР

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

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

• Конвенция на ООН за правата на детето. Общ коментар № 25 на Комитета по правата на детето на ООН
• Конвенция на Съвета на Европа за закрила на децата срещу сексуална експлоатация и сексуално насилие
• Директива 2011/93/ЕС за борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография
• Европейска стратегия за по-добър интернет за децата (2022 г.) (BIK+)

- Стратегия на Европейския съюз за по-ефективна борба със сексуалното насилие над деца
- Акт на ЕС за цифровите услуги (Регламент (ЕС) 2022/2065)
- Акт на ЕС за изкуствения интелект (Регламент (ЕС) 2024/1689)
- Директива (ЕС) 2024/1385 на Европейския парламент и на Съвета от 14.05.2024 г. относно борбата с насилието над жени и домашното насилие

VI. Списък с ключови препоръки, на основа проведения анализ

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

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

ii. 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**. Децата – 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 ЕСПАТ 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**

¹ Национална мрежа за децата, „Бележник 2024: Какъв е средният успех на държавата в грижата за децата“, 2024 г., стр. 55.

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);
- **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 експлоатация 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**

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/>

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

⁵ <https://lex.bg/laws/ldoc/2134925825>

информация и консултации, включително за рисковете в интернет пространството;

- **Задължение за съдействие (чл. 7)** – всички граждани и институции са длъжни да 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 унижително 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 оперативнo звено за изпълнение на мерките за закрила на детето са отделите 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 кодекс⁸ и Наказателно-процесуален кодекс⁹**

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,

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

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>

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 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 друго 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 друго 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 предполага 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) 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

¹⁰ <https://lex.bg/laws/ldoc/2135540550>

¹¹ <https://nmd.bg/pobedi-li-kauzata-na-nmd-za-sthadyastho-pravosadie-za-deczata-zhertvi-na-prestapleniya/>

– 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 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**

¹² <https://lex.bg/laws/ldoc/2135553187>

¹³ Вж. Решение № 2 на Конституционния съд от 2015 г. (<https://legislation.apis.bg/doc/2535725/0>)

съдебното производство или въз основа на мотивирано разпореждане на съдия от съответния първоинстанционен съд, постановено по искане на наблюдаващия прокурор в досъдебното производство.¹⁴¹⁵

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 данни¹⁶**

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;
- Минимизиране на събираните данни;

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>

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

Деца 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 киберсигурност¹⁸. Дирекция „Киберпрестъпност“ към ГДБОП**

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>

Законът за киберсигурност урежда дейностите по: 1). **организацията, управлението и контрола 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 документирание 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**.¹⁹²⁰

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

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>

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.

• Закон за МВР²¹

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

²¹ <https://lex.bg/laws/ldoc/2136243824>

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 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 иницирирана 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

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>

²⁴ <https://nmd.bg/nszd-odobri-proekta-na-nacjonalna-strategiya-za-deteto-2024-2030-g/>

– 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, сексторпън, непознати в мрежата, сигурност и хакнати профили;
- **5.4. Провеждане на обучителна програма „Киберскаут“** в училищата в България;
- **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

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-prevenciya-na-nasilieto-i-zloupotrebata-s-decza-2023-2026-g/>

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

i. Конвенция на ООН за правата на детето. Общ коментар № 25 на Комитета по правата на детето на ООН²⁷

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

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**

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>

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.

ii. Конвенция на Съвета на Европа за закрила на децата срещу сексуална експлоатация и сексуално насилие²⁹

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;
- Съзнателен достъп до материали със сексуална експлоатация на деца чрез

²⁹ <https://rm.coe.int/168046e1e6>

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.**

iii. Директива 2011/93/ЕС за борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография³⁰³¹

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).

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

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

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.

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 презгранично сътрудничество.**

iv. 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:

1. **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;
2. **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;
3. **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;

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>)

- 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 ВІК+ 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 (ВІК+) принципи, норми и цели неминуемо подчертават **необходимостта Националният център за безопасен интернет да получи устойчива държавна подкрепа.**

v. Стратегия на Европейския съюз за по-ефективна борба със сексуалното насилие над деца³⁷

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.

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

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

vi. 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.

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 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

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

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>

представяват 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 предложени 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 предложени специален ред ще се редуцират възможностите за избягване на отговорността по регламента, като същевременно се **запазват гаранциите за правото на защита 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 хулиганство⁴² 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

vii. 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,

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>

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

viii. Директива (ЕС) 2024/1385 на Европейския парламент и на Съвета от 14.05.2024 г. относно борбата с насилието над жени и домашното насилие⁴⁶

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

⁴⁵ Банова-Стоева, Р., „Актът за ИИ – пропуски и възможности от правозащитна гледна точка“, БЦНП, 2024 г. (<https://bcnl.org/>)

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

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

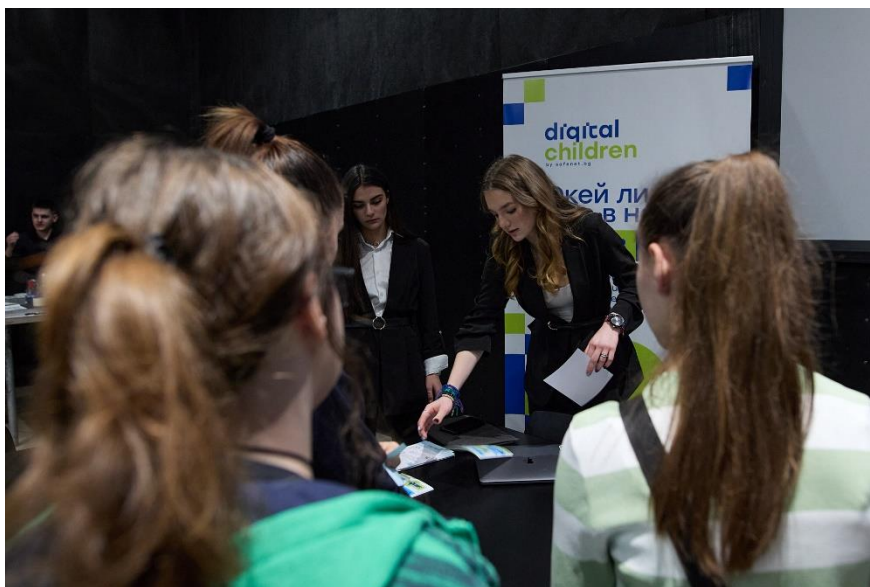
На база изложените по-горе констатации, проектният екип извежда следната **система от препоръки** за подобряване на нормативната база и институционалното сътрудничество, гарантиращи превенцията, разкриването и наказването на престъпни посегателства срещу деца в цифрова среда, а именно:

- 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 тежестта 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 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 **налична 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.



Кадр от събитие на НЦБИ по проект „Дигитални деца“, водено от представители на Младежкия панел към Центъра и младежи от варненската програма “Киберскаутс” – 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 пъления срок на проектно изпълнение, на база продължаващия **текущ проектен мониторинг и анализ на законодателство и политики**.



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.