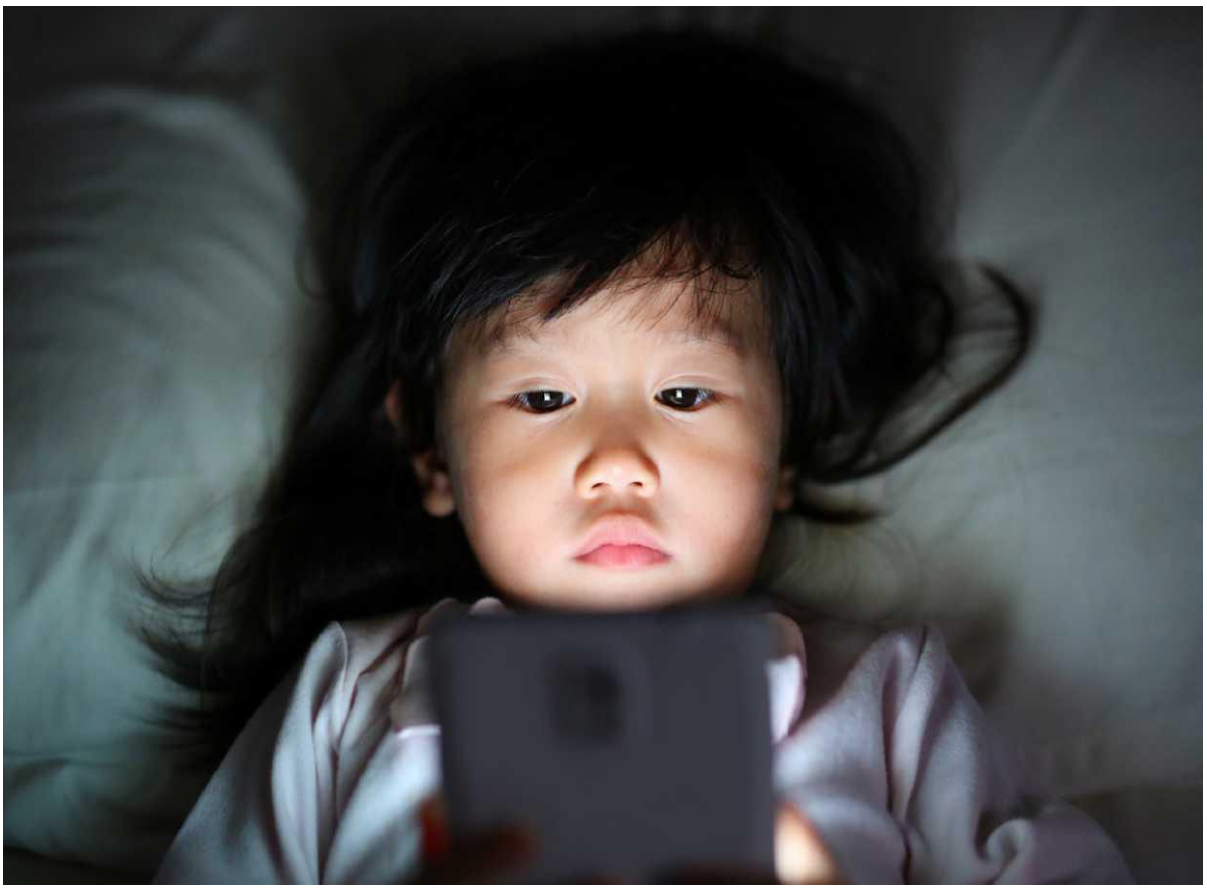
Насоки за създателите на политики в областта на защитата на децата онлайн

2020



Признателност

Тези Насоки са разработени от Международния съюз по далекосъобщения (МСД) и работна група автори от водещи институции в сектора на информационните и комуникационните технологии (ИКТ), както и в областта на защитата на децата (онлайн), и включват следните организации:

ECPAT International, Global Kids Online Network, Глобалното партньорство за прекратяване на насилието срещу деца, проект HABLATAM, Мрежа от центрове за по-безопасен Интернет (Insafe), Интерпол, Международния център за изчезнали и експлоатирани деца (ICMEC), Международния съюз за хората с увреждания, Международния съюз по далекосъобщения МСД, Фондацията за наблюдение на Интернет (IWF), Лондонското училище по икономика, Службата на специалния представител на генералния секретар по въпросите на насилието срещу деца и специалния докладчик относно продажбата и сексуалната експлоатация на деца, Privately SA, RNW Media, Центровете за по-безопасен Интернет в Обединеното кралство, Световния алианс WePROTECT (WPGA) и Световната фондация за детство в САЩ.

Работната група е председателствана от David Wright (Центрове за по-безопасен Интернет в Обединеното кралство /SWGfL) и координирана от Fanny Rotino (МСД).

Тези Насоки не биха били възможни без отделеното време, ентусиазма и отдадеността на допринеслите автори. Безценен принос бе получен и от COFACE-Families Europe, Съветът на Европа, австралийският комисар по електронната безопасност, Европейската комисия, e-Worldwide Group (e-WWG), Организацията за икономическо сътрудничество и развитие (ОИСР), Младежта и медиите в Центъра за Интернет и общество „Беркман Клайн“ в Харвардския университет, както и отделни национални правителства и заинтересовани страни от промишлеността, които споделят общата цел Интернет да се превърне в по-добро и по-безопасно място за децата и младите хора.

МСД е благодарен на следните партньори, които отдадоха ценното си време и знания: (изброени по азбучен ред на организацията)

- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Council of Europe)
- John Carr (ECPAT International)
- Julia Fossi and Ella Serry (eSafety Commissioner)
- Manuela Marta (European Commission)
- Salma Abbasi (e-WWG)
- Amy Crocker and Serena Tommasino (Global Partnership to End Violence Against Children)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Insafe)[1]

[1] *В рамките на Механизма за свързване на Европа (МСЕ) Европейската училищна мрежа управлява от името на Европейската комисия платформата „По-добър Интернет за децата“, която включва координацията на мрежата за*

- Lucy Richardson (International Disability Alliance)
- Matthew Dompier (Interpol)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Sonia Livingstone (London School of Economics & Global Kids Online)
- Elettra Ronchi (OECD)
- Manus De Barra (Office of the Special Representative of the Secretary-General on Violence against Children)
- Deepak Tewari (Privately SA)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (United Nations Special Rapporteur on the sale and sexual exploitation of children)
- David Wright (UK Safer Internet Centres/SWGfL)
- Iain Drennan and Susannah Richmond (WePROTECT Global Alliance)
- Lina Fernandez and Dr. Joanna Rubinstein (World Childhood Foundation USA)
- Sandra Cortesi (Youth and Media)

ISBN

978—92—61—3021—7 (хартиена версия)

978—92—61—30451—5 (електронна версия)

978—92—61—30111—8 (версия на EPUB)

978—92—61—30461—4 (моби версия)

безопасен Интернет на европейските центрове за по-безопасен Интернет. Повече информация може да бъде намерена на адрес: www.betterinternetforkids.eu

УВОД

В свят, в който Интернет засяга почти всеки аспект на съвременния живот, грижата за безопасността на младите потребители онлайн се очертава като все по-спешен въпрос за всяка страна.

МСД разработи първия си набор от Насоки за онлайн защита на децата още през 2009 г. Оттогава Интернет еволюира отвъд всички очаквания. Въпреки че се превърна в безкрайно богат ресурс за децата да играят и учат, той стана и много по-опасно и съпътствано от рискове място за тях. От въпроси, свързани с неприкосновеността на личния живот, насилие и неподходящо съдържание, до Интернет измамници в спектъра на онлайн сприятеляването с цел сексуална злоупотреба, сексуално насилие и експлоатация, днешните деца са изправени пред много рискове. Заплахите се умножават и извършителитедействат едновременно в много различни правни юрисдикции, което ограничава ефикасността на специфичните за всяка държава ответни действия и правна защита.

Освен това глобалната пандемия от КОВИД-19 отбеляза рязко нарастване на броя на децата, които се присъединяват за първи път към онлайн света, за да подпомогнат образованието си и да поддържат социално взаимодействие. Ограниченията, наложени от вируса, накараха много по-малки деца да започнат да взаимодействат онлайн много по-рано, отколкото родителите им планират, а необходимостта от жонглиране с трудовите ангажименти остави много родители в невъзможност да упражняват надзор над децата си, като по този начин младите хора бяха изложени на риск от достъп до неподходящо съдържание или станаха цел на престъпници за производството на материали, съдържащи сексуално насилие над деца.

Повече, отколкото преди, поддържането на безопасността на децата онлайн изисква съвместна и координирана международна реакция с активното участие и подкрепа на широк кръг заинтересовани страни — от промишлеността, включително платформите от частния сектор, доставчиците на услуги и операторите на мрежи, до правителствата и гражданското общество.

Отчитайки това, през 2018 г. държавите членки на МСД поискаха нещо повече от своевременно актуализиране на Насоките за защитата на детето онлайн, което се предприемаше периодично в миналото. Вместо това тези нови преразгледани Насоки бяха преосмислени, пренаписани и преработени от самото начало, така че да отразяват значителните промени в цифровата среда, в която се намират децата.

Освен че отговаря на новите развития в областта на цифровите технологии и платформи, в това ново издание се разглежда и положението, в което се намират децата с увреждания, за които онлайн светът предлага жизнено важна възможност за пълноценно социално участие. Беше обърнато внимание и на специалните нужди на децата мигранти и на други уязвими групи.

Надяваме се, че за създателите на политики, тези Насоки ще послужат като солидна основа за разработване на приобщаващи национални стратегии с участието на множество заинтересовани страни/multi-stakeholder, включително за открити консултации и диалози с деца, за разработване на по-целенасочени мерки и по-ефикасни действия.

При разработването на тези нови Насоки Международният съюз по далекосъобщения и неговите партньори се стремяха да създадат силно използваема, гъвкава и адаптивна рамка, основана твърдо на международни стандарти и споделени цели — по-специално на Конвенцията за правата на детето и целите на ООН за устойчиво развитие. В истинския дух на ролята на Международния съюз по далекосъобщения като световен обединител, се гордея с факта, че тези преразгледани Насоки са резултат от глобални съвместни усилия и са съавторство на международни експерти от широката общност на множество заинтересовани страни.

Радвам се също така да ви представя новия ни талисман на Инициативата за онлайн защита на децата, Санго (Sango), приятелски настроен, непоколебим и безстрашен, създаден изцяло от група деца, като част от новата международна младежка програма на Международния съюз за далекосъобщения.

Във възрастта, в която все повече млади хора са онлайн, тези COP Насоки са по-важни от всякога. Създателите на политики, промишлеността, родителите и преподавателите — както и самите деца — имат жизненоважна роля. Благодарна съм, както винаги, за Вашата подкрепа и с нетърпение очаквам да продължим тясното си сътрудничество по този критичен въпрос.

Дорийн Богдан-Мартин

Директор, Бюро за развитие на далекосъобщенията

ПРЕДГОВОР

Преди тридесет години почти всички правителства се ангажираха да зачитат, защитават и насърчават правата на децата. Конвенцията на ООН за правата на детето (КПД) е най-широко ратифицираният международен договор за правата на човека в историята. Въпреки че през последните три десетилетия беше постигнат значителен напредък, продължават да съществуват значителни предизвикателства и се появяват нови области на риск за децата.

През 2015 г. всички нации подновиха ангажимента си към децата по отношение на програмата до 2030 г. и 17-те универсални цели за устойчиво развитие (ЦУР). Цел 16.2 например призовава за прекратяване на злоупотребите, експлоатацията и всички форми на насилие и изтезания срещу деца до 2030 г. Защитата на децата е общ лайтмотив в рамките на 11 от 17-те ЦУР. УНИЦЕФ поставя децата в центъра на програмата до 2030 г., както е показано на фигура 1.

Фигура 1: Деца, ИКТ и ЦУР

Според Програмата до 2030 г. за устойчиво развитие ИКТ могат да бъдат ключов фактор за постигането на ЦУР. Разпространението на информационните и комуникационните технологии и глобалната взаимосвързаност имат потенциала да ускорят човешкия напредък, да преодолеят цифровото разделение и да развият обществата на знанието. Освен това в нея се определят конкретни цели за използването на ИКТ за устойчиво развитие в образованието (цел 4), равенството между половете (цел 5), инфраструктурата (цел 9 — универсален достъп до Интернет на достъпни цени) и цел 17 — партньорства и средства за изпълнение [2]. ИКТ имат силата да

[2] ПРООН, Цели за устойчиво развитие | ПРООН, undp.org, посетен на 29 януари 2020 г., https://www.undp .org/content/undp/en/home/stainable- development-goals.html; Хулин Зао, „Защо ИКТ са толкова решаващи за постигането на ЦУР“, *МСД*, ITU News Magazines, 48, посетен на 29 януари 2020 г., https://www.itu.int/en/

трансформират дълбоко икономиката като цяло, бидейки движеща сила за постигането на всяка една от 17-те ЦУР. ИКТ вече се изявиха, като дадоха повече възможности на милиарди хора по света - чрез предоставяне на достъп до образователни ресурси и здравеопазване, както и до услуги като електронното управление и социалните медии.

Експлозията на информационните и комуникационните технологии създаде безпрецедентни възможности за децата и младите хора да общуват, да се свързват, споделят, учат, да получават достъп до информация и да изразяват мненията си по въпроси, които засягат техния живот и техните общности.

Но по-широкият и по-лесен достъп до Интернет и мобилни технологии създава и значителни предизвикателства за безопасността и благосъстоянието на децата - както онлайн, така и офлайн. За да се намалят рисковете на цифровия свят, като същевременно се даде възможност на повече деца и млади хора да се възползват от неговите ползи, правителствата, гражданското общество, местните общности, международните организации и промишлеността трябва да се обединят в обща цел. Необходими са създатели на политики, за да се постигне международната цел децата да бъдат в безопасност онлайн.

За да се отговори на предизвикателствата, породени от бързото развитие на ИКТ и свързани със защитата на децата, през ноември 2008 г. Международният съюз по далекосъобщения стартира Инициативата за онлайн защита на децата като многостранна международна инициатива. Тази инициатива има за цел да обедини партньори от всички сектори на световната общност, за да създаде указания за безопасност и да предостави онлайн права за децата по света.

Конференцията на пълномощните представители на Международния съюз по далекосъобщения, проведена в Дубай през 2018 г., потвърди значението на инициативата COP и я призна като платформа за повишаване на осведомеността, за обмен на най-добри практики и за предоставяне на помощ и подкрепа на държавите членки, особено на развиващите се страни, при разработването и прилагането на пътните карти на COP. Тя признa значението на защитата на децата онлайн в рамките на Конвенцията на ООН за правата на детето и други договори в областта на правата на човека, чрез насърчаване на сътрудничеството между всички заинтересовани страни, участващи в защитата на децата онлайн.

Конференцията призна Програмата до 2030 г. за устойчиво развитие, която разглежда различни аспекти на защитата на децата онлайн в целите за устойчиво развитие, по-специално ЦУР 1, 3, 4, 5, 9, 10 и 16; както и Резолюция 175 (Rev. Dubai, 2018 г.) относно достъпността за хора с увреждания и лица със специфични нужди до телекомуникации/информационни и комуникационни технологии, Резолюция 67 (Rev. Buenos Aires, 2017) на Световната конференция за развитие на далекосъобщенията

itunews/Documents/2017—03/2017 ITUNews03-en.pdf.

(WTDC) и ролята на сектора на развитието на далекосъобщенията на Международния съюз по далекосъобщения (ITU-D) за защитата на децата онлайн.

В края на 2019 г. Комисията за широколентов достъп на МСД/ЮНЕСКО за устойчиво развитие публикува Доклада за безопасността на децата онлайн с приложими препоръки за това, как да се направи Интернет по-безопасен за децата.

През 2009 г. Международният съюз по далекосъобщения издаде първия набор от Насоки относно защитата на децата онлайн в контекста на инициативата COP. През последното десетилетие Насоките COP бяха преведени на много езици и бяха използвани от много държави по света като отправна точка за пътните карти и националните стратегии, свързани със защитата на децата онлайн. Те са служили на националните правителствени органи, организациите на гражданското общество, институциите за грижи за децата, промишлеността и много други заинтересовани страни в усилията им за защита на децата онлайн.

Насоките бяха използвани за изготвянето, разработването и прилагането на национални стратегии за защита на децата онлайн в много държави членки като Камерун, Габон, Гамбия, Гана Кения, Сиера Леона, Уганда и Замбия в региона на Африка; Бахрейн и Оман в арабския регион; Бруней, Камбоджа Кирибати, Индонезия, Малайзия, Мианмар и Вануату в Азиатско-тихоокеанския регион; и Босна, Грузия, Молдова, Черна гора, Полша и Украйна в региона на Европа.

Освен това Насоките изградиха основата за регионални прояви като Регионалната конференция по въпросите на защитата на децата онлайн (ACOP): Овластяване /предоставяне на права на бъдещите цифрови граждани в Кампала, Уганда (2014 г.) и Регионалната конференция на АСЕАН по въпросите на защитата на децата онлайн, проведена в Банкок, Тайланд (2020 г.). Съгласно Резолюция 179 (Rev. Dubai, 2018 г.) Международният съюз за далекосъобщения, в сътрудничество с партньорите по инициативата COP и заинтересованите страни, получи указания да актуализира четирите набора от ННасоки, като вземе предвид технологичното развитие в телекомуникационната индустрия, включително Насоките относно децата с увреждания и децата със специфични нужди.

В резултат на този процес Насоките бяха значително актуализирани и преразгледани от експерти и заинтересовани страни, като бяха формулирани широк набор от препоръки за опазване на безопасността на децата в цифровия свят. Те са резултат от съвместните усилия на множество заинтересовани страни, които използват знанията, опита и експертизата на много организации и професионалисти от цял свят в областта на защитата на децата онлайн. Те имат за цел да създадат основите на безопасен и сигурен кибер свят за бъдещите поколения. Предназначени са да действат като план, който може да бъде адаптиран и използван по начин, който е в съответствие с националните или местните обичаи и закони. Освен това в настоящите Насоки се разглеждат въпроси, които засягат всички деца и млади хора на възраст под 18 години, като се отчитат различните потребности на всяка възрастова група. Те имат за цел и да

отговорят на нуждите на децата при различни условия на живот и на децата със специални нужди, и увреждания. Насоките увеличават обхвата на защитата на децата онлайн, като отчитат всички рискове, заплахи и вреди, с които децата могат да се сблъскат онлайн, за да се балансират внимателно с ползите, които цифровият свят може да донесе за живота на децата.

Надяваме се, че тези Насоки не само ще доведат до изграждането на по-приобщаващо информационно общество, но и ще дадат възможност на държавите членки на МСД да изпълнят задълженията си за защита и осъществяване на правата на децата, както е посочено в Конвенцията на ООН за правата на детето,[3] приета с Резолюция 44/25 на Общото събрание на ООН от 20 ноември 1989 г. и документа за резултатите от Световната среща на върха по въпросите на информационното общество[4] (WSIS).

Чрез издаването на тези Насоки инициативата COP призовава всички заинтересовани страни да прилагат политики и стратегии, които ще защитават децата в киберпространството и ще насърчават техния по-безопасен достъп до всички изключителни възможности, които могат да предоставят онлайн ресурсите.

[3] УНИЦЕФ, „Конвенция за правата на детето“, uncief.org, посетен на 29 януари 2020 г., https://www.unicef .org/child-rights-convention

[4] WSIS се проведе на два етапа: в Женева (10—12 декември 2003 г.) и в Тунис (16—18 ноември 2005 г.). WSIS завърши с подчертан ангажимент „да изгради ориентирано към хората и развитието, приобщаващо информационно общество, в което всеки може да създава, да има достъп, да използва и споделя информация и знания“.

СЪДЪРЖАНИЕ

1. ПРЕГЛЕД НА ДОКУМЕНТИТЕ

1.1. Цел

Националните правителства са задължени да осигурят защита на децата, както във физическия, така и във виртуалния свят. И тъй като новите технологии вече са добре интегрирани в живота на много деца, и млади хора по редица начини, вече няма смисъл да се опитваме да поддържаме строги разграничения между събитията от реалния свят и онлайн събитията. Двете са все по-преплетени и взаимозависими.

Създателите на политики [5] и всички други заинтересовани страни имат много важна роля. Скоростта, с която технологиите се развиват, означава, че много от традиционните методи за създаване на политики вече не отговарят на тази цел. От създателите на политики се изисква да разработят правна рамка, която да е адаптивна, приобщаваща и подходяща за целта на бързо променящата се цифрова ера за защита на децата онлайн.

Целта на настоящите Насоки е да се предложи на създателите на политики в държавите членки на МСД лесна за ползване и гъвкава рамка за разбиране и изпълнение на тяхното правно задължение да осигурят защита на децата както в реалния, така и във физическия и виртуалния свят.

Насоките правят това, като разглеждат няколко важни въпроса за създателите на политики:

1) Какво представлява защитата на децата онлайн?
2) Защо аз като създател на политики трябва да се грижа за защитата на децата онлайн?
3) Какъв е правният, социално-политическият контекст и контекстът на развитие на моята страна?
4) Как създателите на политики следва да започнат да обмислят и формират ефективна и устойчива политика за защита на децата онлайн в своята страна?

Насоките се основават на съществуващите модели, рамки и ресурси, за да предложат контекст и представа за добрите практики от цял свят.

1.2 Обхват

Обхватът на защитата на децата онлайн засяга всички вреди, на които са изложени децата онлайн, като посочва широк спектър от рискове, които застрашават безопасността и благосъстоянието на децата. Това е сложно предизвикателство, към което трябва да се подходи от различни гледни точки, включително законодателство, управление, образование, политика и общество.

[5] Терминът „създатели на политики“ тук се отнася до всички заинтересовани страни, които отговарят за разработването и прилагането на политиката, особено тези в рамките на правителството.

Освен това защитата на децата онлайн трябва да се основава на разбиране както на общите, така и на специфичните за всяка държава рискове, заплахи и вреди, пред които са изправени децата в цифрова среда. Това изисква ясни определения и установяване на ясни параметри за намеса, които включват и разграничават деянията, съставляващи престъпление, и тези, които, въпреки че не са незаконни, представляват заплаха за благосъстоянието на детето.

За тази цел в Насоките се прави преглед на настоящите заплахи и вреди, пред които са изправени децата в цифровата среда. Въпреки това скоростта, с която технологията и свързаните с нея заплахи и вреди се развиват, означава, че традиционната скорост и метод на разработване на политики не могат да бъдат в синхрон. Създателите на политики в ерата на цифровите технологии трябва да изградят правни и политически рамки, които да са достатъчно адаптивни и приобщаващи, за да се справят със съществуващите предизвикателства и, доколкото е възможно, да предвиждат бъдещите предизвикателства. За тази цел е необходимо сътрудничество с всички заинтересовани страни, включително сектора на ИКТ, научноизследователската общност, гражданското общество, обществеността и самите деца. Този процес може да бъде подкрепен от разглеждане на всеобхватните принципи в областта на защитата на децата онлайн.

1.3 Общи принципи

Единадесет хоризонтални принципа, изложени тук, взети заедно, ще спомогнат за разработването на ориентирана към бъдещето и цялостна национална стратегия за защита на децата онлайн.

Редът на тези принципи отразява по-скоро логическо послание, отколкото ред на важност.

Националната стратегия за защита на децата онлайн следва да:

- се основава на цялостна визия, която включва правителството, промишлеността и обществото;
- е резултат от всеобхватно разбиране и анализ на цялостната цифрова среда, които са съобразени с обстоятелствата и приоритетите на страната;
- зачита и да бъде в съответствие с основните права на децата, залегнали в Конвенцията на ООН за правата на детето и други ключови международни конвенции и закони;
- зачита и да бъде в съответствие със съществуващите, подобни и свързани с тях национални закони и стратегии, като например законите относно малтретирането на деца или стратегиите за безопасност на децата;
- зачита гражданските права и свободи на децата, които не следва да се жертват при защитата;
- се разработва с активното участие на всички съответни заинтересовани страни, включително децата, като се обръща внимание на техните нужди и отговорности и

се задоволяват потребностите на малцинствените и маргинализираните групи;

- е разработена така, че да бъде приведена в съответствие с по-широките правителствени планове за икономически и социален просперитет и да увеличи максимално приноса на ИКТ за устойчивото развитие и социалното приобщаване;
- използва най-подходящите налични политически инструменти за осъществяване на своята цел, като се имат предвид специфичните обстоятелства в страната;
- бъде поставена на най-високо управленско ниво, което ще отговаря за определянето на съответните роли и отговорности и разпределянето на достатъчно човешки и финансови ресурси;
- подпомага изграждането на цифрова среда, в която децата, родителите/настойниците и заинтересованите страни могат да имат доверие;
- насочва усилията на заинтересованите страни за оправомощаване и образоване на децата по отношение на цифровата грамотност, за да се защитят онлайн.

1.4 Използване на настоящите Насоки

В настоящите Насоки се разглеждат съответните научни изследвания, съществуващите модели и материали, и се формулират ясни препоръки за разработването на национална стратегия за защита на децата онлайн.

- Раздел 2 въвежда защитата на децата онлайн и дава представа за последните научни изследвания, включително аспектите, свързани с нововъзникващите технологии, ключовите заплахи и вредите за децата.
- В раздел 3 се посочва как да се подготви национална стратегия за защита на децата онлайн, включително съответните заинтересовани страни, съществуващите примери за реагиране на онлайн заплахи и вреди и ползи от наличието на национална стратегия.
- Раздел 4 обхваща препоръките за рамкиране и изпълнение.
- В раздел 5 са очертани националните контролни списъци за разработване на национална стратегия за защита на децата онлайн.
- Раздел 6 съдържа полезни справочни материали

2. ВЪВЕДЕНИЕ

През 2019 г. повече от половината от световното население използва Интернет. Най-голямата група потребители са тези на възраст под 44 години, като използването е еднакво високо сред 16—24-годишните и 35—44-годишните. В световен мащаб едно на всеки три деца използва Интернет (0-18 години)[6]. В развиващите се страни децата и младите хора са водещи в използването[7]на Интернет и според оценките през следващите пет години това население ще се увеличи повече от два пъти. Новите поколения израстват с Интернет и повечето от тях се свързват с технологията на мобилните мрежи, особено в глобалния юг [8].

Въпреки че достъпът до Интернет е от основно значение за упражняването на правата на децата, все още съществуват значителни регионални, национални, свързани с пола и други различия в достъпа, които ограничават възможностите за момичетата, децата с увреждания, децата от малцинствата и други уязвими групи. Що се отнася до цифровото разделение между половете, изследванията показват, че във всеки регион, с изключение на Съединените американски щати, потребителите на Интернет мъже в голяма степен превъзхождат броя на жените потребители. В много държави момичетата не разполагат със същите възможности за достъп като момчетата, а там, където ги имат, момичетата не само се наблюдават и ограничават в много по-голяма степен в използването на Интернет, но и безопасността им в усилията им за достъп до Интернет може да е в рискИнтернет[9]. Ясно е, че децата и младите хора, които нямат цифрови умения или говорят малцинствени езици, не могат лесно да намерят подходящо съдържание онлайн и че децата от селските райони имат по-малко цифрови умения, прекарват повече време онлайн (особено игри) и получават по-малко родителско посредничество и мониторинг[10].

При все това не може да се проведе никакъв разговор за рискове и заплахи, без да се признае изключително обогатяващият и овластяващ характер на цифровите технологии. Интернет и цифровите технологии преобразяват начина, по който живеем, и разкриват много нови начини за общуване, игра, наслаждаване на музика и участие в широк спектър от културни, образователни и повишаващи уменията дейности. Интернет може да осигури изключително важен достъп до здравни и образователни услуги, както

---

[6] ОИСР, "Нови технологии и деца през 21-ви век: Последни тенденции и резултати, работен документ на ОИСР в областта на образованието № 179 (Дирекция „Образование и умения“, ОИСР), посетен на 27 януари 2020 г., https://www .oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage =En.

[7] Ofcom, "Деца и родители: Media Use and Attitudes Report 2018" (Ofcom), посетен на 17 януари 2020 г., https://www.ofcom.org.uk/ data/assets/pdf file/0024/134907/Children-and-parents-media-use-and —attitudes-2018.pdf.

[8] ITU, “Measuring the Information Society Report,” accessed January 16, 2020, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

[9].Младите юноши и цифровите медии: Uses, Risks and Opportunities in Low- and Middle-Income Countries (Използвания, рискове и възможности в страните с ниски и средни доходи),"GAGE, посетен на 29 януари 2020г., https://www.gage.odi.org/publication/digital-media-risks —възможности/.

[10] Livingstone, S., Kardefelt Winther, D. и Hussein, M. (2019 г.). *Global Kids Online Comparative Report, Innocenti Research Report*. Служба за научни изследвания на УНИЦЕФ — Innocenti, Флоренция, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html. Това може да доведе до неочаквани резултати, например изследвания, проведени от HABLATAM в пет латиноамерикански държави, показват, че в уязвимите общности децата могат да използват платформи за запознанства, видеоигри и социални мрежи за извършване на парични транзакции за незаконни цели. Contectados al Sur network, „Hablatam,“ Hablatam Project 2020, посетен на 6 февруари 2020 г., https://hablatam.net/.

и информация по теми, които са важни за младите хора, но могат да бъдат табу в техните общества.

Точно както децата и младите хора често са начело в приемането и адаптирането към новите възможности, предоставяни от Интернет, те са изложени и на редица въпроси, свързани с безопасността и благосъстоянието, които трябва да бъдат признати и пред които обществото трябва да се изправи. От съществено значение е открито да се обсъдят рисковете, които съществуват за децата и младите хора онлайн. Дискусията отваря платформа, от която децата и младите хора могат да бъдат научени как да разпознават риска и да предотвратяват или да се справят с вредите, ако те се материализират, както и предимствата и възможностите, които Интернет може да предложи.

В много части на света младите хора добре разбират някои от рисковете, пред които са изправени онлайн.[1112] Изследванията показват например, че по-голямата част от децата и младите хора са в състояние да разграничат кибертормоза от шегите или закачките онлайн. Те разбират, че кибертормозът има обществено измерение и е предназначен да навреди, но балансирането на онлайн възможностите и рисковете на децата продължава да бъде предизвикателство[13].

За държавите членки на Международния съюз по далекосъобщения, защитата на децата и младите хора онлайн продължава да бъде приоритет, който трябва да бъде внимателно балансиран с усилията за насърчаване на възможностите за децата и младите хора онлайн[14]и че това трябва да се прави по начин, който защитава децата и младите хора, без да се засяга техният достъп или достъпът на широката общественост до информация, или възможността да се ползват от свободата на словото, изразяването и сдружаването.

Налице е очевидна необходимост от целенасочени инвестиции и творчески решения за справяне с рисковете, пред които са изправени децата и младите хора, не на последно място поради цифровото разделение между децата и възрастните, което ограничава напътствията от страна на родителите, учителите и настойниците. В същото време, тъй като децата и младите хора растат и стават възрастни, родители и активни членове на обществото, съществува потенциална и неизбежна възможност за тях да намалят цифровото разделение.

С оглед на това изграждането на доверие в Интернет трябва да бъде начело и в центъра на обществената политика. Правителствата и обществото трябва да работят с децата и младите хора, за да разберат техните перспективи и да предизвикат истински обществен дебат относно рисковете и възможностите. Подкрепата за децата и младите хора за управление на онлайн рисковете може да бъде ефикасна, но правителствата

[11] От 2016 г. насам МСД провежда консултации в рамките на COP с деца и възрастни заинтересовани страни по важни въпроси като кибертормоза, цифровата грамотност и дейностите на децата онлайн.
[12] МСД, Младежка консултация, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.
[13] UNICEF, "Global Kids Online Comparative Report (2019)."
[14] МСД, „Честване на 10 години онлайн защита на детето", ITU News, 6 февруари 2018 г., https://news.itu.int/celebrating-10-years-child-online-protection/.

трябва също така да гарантират, че са налице подходящи услуги за подкрепа за тези, които изпитват вреди онлайн, и че децата са наясно как да получат достъп до тези услуги.

Някои държави се стараят да отделят достатъчно ресурси за справяне с цифровата грамотност и безопасността на децата онлайн. Децата обаче съобщават, че родителите, учителите, технологичните компании и правителствата са важни участници в разработването на решения в подкрепа на тяхната онлайн безопасност. Държавите членки на Международния съюз по далекосъобщения, посочиха, че е налице значителна подкрепа за засиления обмен на знания и координираните усилия за гарантиране на безопасността на по-голям брой деца онлайн[9].

Децата и младите хора се ориентират към все по-сложна цифрова среда и възприемането на изкуствен интелект за машинно самообучение, анализ на големи информационни масиви, роботика, виртуална и добавена реалност, и Интернет на нещата трансформират медийните практики на децата. Това изисква изготвянето на политики и инвестиции за децата, родителите и общностите както за бъдещето толкова, колкото и днес.

2.1. Какво представлява защитата на децата онлайн?

Онлайн технологиите предоставят много възможности за децата и младите хора да общуват, да придобиват нови умения, да бъдат креативни и да допринасят за по-добро общество. Но те могат да доведат и до нови рискове, като например, свързани с неприкосновеността на личния живот, незаконното съдържание, тормоза, кибертормоза, злоупотребата с лични данни или сприятеляването с цел сексуална злоупотреба със сексуални цели и дори сексуалното насилие над деца.

Настоящите Насоки разработват цялостен подход за реагиране на всички потенциални заплахи и вреди, с които могат да се сблъскат децата и младите хора, когато придобиват цифрова грамотност. Те отчитат, че всички съответни заинтересовани страни имат роля в тяхната цифрова устойчивост, благосъстояние и защита, като същевременно се възползват от възможностите, които Интернет може да предложи.

Защитата на децата и младите хора е споделена отговорност и всички заинтересовани страни трябва да гарантират устойчиво бъдеще за всички. За да се случи това, създателите на политики, промишлеността, родителите, лицата, полагащи грижи, преподавателите и други заинтересовани страни, трябва да гарантират, че децата и младите хора могат да реализират своя потенциал — онлайн и офлайн.

Въпреки че не съществува универсално определение за защита на децата онлайн, то има за цел да възприеме цялостен подход за изграждане на безопасни, съобразени с възрастта, приобщаващи цифрови пространства за децата и младите хора, характеризиращи се с:

- реагиране, подкрепа и самопомощ срещу заплахата;
- предотвратяване на вреди;

- динамичен баланс между осигуряването на защита и предоставянето на възможност на децата да бъдат цифрови граждани;
- отстояване на правата и отговорностите както на децата, така и на обществото.

Освен това, поради бързия напредък в технологиите и обществото и безграничния характер на Интернет, защитата на децата онлайн трябва да бъде гъвкава и адаптивна, за да бъде ефикасна. Въпреки че настоящите Насоки дават представа за водещите рискове за децата и младите хора онлайн, включително вредно и незаконно съдържание, тормоз, кибертормоз, злоупотреба с лични данни или сприятеляване със сексуални цели и сексуално насилие, и експлоатация на деца, ще възникнат нови предизвикателства с развитието на технологични иновации, които обикновено се различават в отделните региони. Новите предизвикателства обаче най-добре ще бъдат преодолени чрез съвместна работа като глобална общност, тъй като трябва да се намерят нови решения на тези предизвикателства.

2.2 Децата в цифровия свят

Интернет промени начина, по който живеем. Той е изцяло интегриран в живота на децата и младите хора, което прави невъзможно разглеждането на цифровия и физическия свят поотделно. Една трета от всички потребители на Интернет днес са деца и млади хора, а УНИЦЕФ изчислява, че 71% от младите хора вече са онлайн.

Такава свързаност е изключително оправомощаваща/. Онлайн светът позволява на децата и младите хора да преодолеят недостатъците и увреждания и дава нови възможности за забавление, образование, участие и изграждане на взаимоотношения. Днес цифровите платформи се използват за различни дейности и често представляват мултимедийни преживявания.

Достъпът до технологии и запознаването с тях за използване и навигация се разглежда като критично важно за развитието на младите хора и се прави за първи път в ранна възраст. Създателите на политики трябва да разберат, че децата и младите хора често започват да използват платформи и услуги, преди да достигнат определената минимална възраст, и следователно образованието трябва да започне рано.

Децата и младите хора искат да участват в разговора и имат ценен опит като „цифрови по природа“, който може да бъде споделен. Създателите на политики и практиците трябва да се ангажират с децата и младите хора в текущ дебат относно онлайн средата, за да подкрепят техните права.

Достъп до Интернет

През 2019 г. повече от половината от световното население е използвало Интернет (53,6 %) с приблизително 4,1 милиарда потребители. На глобално ниво един на всеки

трима потребители на Интернет е дете под 18 години[15]. В някои страни с по-ниски доходи това се повишава до около едно към две, докато в страните с по-висок доход съотношението е около едно към пет. Според УНИЦЕФ в световен мащаб 71 % от младите хора вече са онлайн[16]. Ето защо децата и младите хора сега са значително и постоянно присъстващи в Интернет [17] . Интернет обслужва други социални, икономически или политически цели и се е превърнал в семеен или потребителски продукт или услуга, която е неразделна част от начина, по който семействата, децата и младите хора живеят живота си.

През 2017 г. в регионален план достъпът до Интернет на децата и младежите е силно свързан с нивото на доходите. Страните с ниски доходи обикновено имат по-малко деца, ползващи Интернет, отколкото страните с висок доход.

Децата и младите хора в повечето страни прекарват повече време онлайн през уикенда, отколкото в делничен ден, като юношите (15–17 годишни) прекарват най-дълго онлайн, средно между 2,5 и 5,3 часа, в зависимост от страната.

Използване на Интернет

Сред децата и младите хора най-популярното устройство за достъп до Интернет е мобилният телефон, следван от настолните компютри и лаптопи. Децата и младите хора прекарват средно около два часа на ден онлайн през седмицата и приблизително удвояват това всеки ден от уикенда. Някои се чувстват постоянно свързани. Но много други все още нямат достъп до Интернет у дома.

На практика повечето деца и младежи, които използват Интернет, имат достъп до него чрез повече от едно устройство: Децата и младежите, които се свързват поне седмично, понякога използват до три различни устройства, за да направят това. По-големите деца и децата в по-богатите страни обикновено използват повече устройства, а момчетата използват малко повече устройства от момичетата във всяка изследвана страна.

Най-популярното занимание – както за момичета, така и за момчета – е гледането на видеоклипове. Повече от три четвърти от децата и младежите, които използват Интернет, казват, че гледат видеоклипове онлайн поне седмично, самостоятелно или с други членове на семейството си. Много деца и млади хора могат да се считат за „активни социализатори“, използвайки няколко социални медийни платформи като Facebook, Twitter, TikTok или Instagram.

Децата и младите хора се занимават също с политика онлайн и гласът им се чува чрез блогове.

[15] Ливингстън, С., Кар, Дж., и Бърн, Дж. (2015) Един от три: Задачата за глобално управление на Интернет за справяне с правата на децата. Глобална комисия за управление на Интернет: Серия документи. Лондон: CIGI и Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights

[16] Комисията за широколентов достъп, „Безопасност на децата онлайн: Минимизиране на риска от насилие, злоупотреба и експлоатация онлайн (2019 г.)“, Комисия за широколентов достъп за устойчиво развитие, октомври 2019 г., 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report. pdf

[17] Ливингстън, Кар и Бърн, „Едно от три: управление на Интернет и правата на децата“.

Общото ниво на участие в онлайн игрите варира по държави приблизително в зависимост от достъпа на децата и младите хора до Интернет, докато 10—30 процента от децата и младите хора, които използват Интернет, участват в творчески онлайн дейности всяка седмица.

За образователни цели много деца и млади хора от всички възрасти използват Интернет за домашна работа или дори да наваксат отсъствие от часове или да търсят здравна информация онлайн всяка седмица. По-големите деца изглежда имат по-голям апетит за информация, отколкото по-малките деца.

2.3 Въздействието/ влиянието на технологиите върху цифровия опит на децата

Интернет и цифровите технологии могат да предоставят възможности и да представляват рискове за децата и младите хора. Например, когато децата използват социалните медии, те се възползват от много възможности за проучване, учене, общуване и развиване на ключови умения. Например, социалните мрежи се разглеждат от децата като платформи, които им позволяват да изследват личната идентичност в безопасна среда. За младите хора е важно да притежават съответните умения и да знаят как да се справят с проблемите, свързани с неприкосновеността на личния живот и репутацията.

„Знам, че всичко, което публикувате в Интернет, остава завинаги и може да повлияе на живота ви в бъдеще“, момче, на 14 години, Чили.

Въпреки това, след консултации, които показват, че повечето деца, използващи социални медии преди минималната възраст от тринадесет години[18], и услугите за проверка на възрастта като цяло са слаби или липсват, рисковете, пред които са изправени децата, могат да бъдат увеличени. И докато децата искат да придобият цифрови умения и да станат цифрови граждани, по-специално да се грижат за неприкосновеността на личния си живот, те са склонни да мислят за неприкосновеността на личния живот по отношение на своите приятели и познати — „Какво могат да видят приятелите ми?“ — и по-малко по отношение на непознати и трети страни. В съчетание с естественото любопитство на децата и като цяло по-ниския праг за риск, това може да ги направи уязвими на сприятеляване с цел сексуална злоупотреба, експлоатация, тормоз или други видове вредно съдържание или контакт.

Широко разпространената популярност на споделянето на изображения и видео чрез мобилни приложения, и по-специално използването от деца на платформи за стрийминг на живо, поражда допълнителни опасения, свързани с неприкосновеността на личния живот и риска. Някои деца произвеждат сексуални изображения на себе си, приятели , братя и сестри и ги споделят онлайн. За някои, особено по-големите деца, това може да се разглежда като естествено изследване на сексуалността и сексуалната идентичност, докато за други, особено по-малките деца, често има принуда от възрастен или друго дете. Независимо от случая, полученото съдържание в много държави е

[18]мрежа Contectados al Sur, “Hablatam”; УНИЦЕФ, „Глобален сравнителен доклад за деца онлайн (2019 г.)“

незаконно и може да изложи децата на риск от наказателно преследване, или може да бъде използвано за по-нататъшна експлоатация на детето.

По подобен начин онлайн игрите дават възможност на децата да упражняват основното си право на игра, както и да изграждат контакти, да прекарват време и да се срещат с нови приятели, както и да развиват важни умения. Преобладаващо, това може да бъде положително. Съществуват обаче все повече доказателства, които сочат, че ненаблюдаваните и без помощ от отговорен възрастен онлайн платформи за игри могат да създадат рискове за децата, от игрови разстройства, финансови рискове, събиране и монетизиране на лични данни на деца, до кибертормоз, изказвания, подбуждащи към омраза, насилие и излагане на неподходящо поведение или съдържание, както [19] и сприятеляване с цел сексуална злоупотреба с реални, компютърни или дори виртуални изображения и видеоматериали, изобразяващи и улесняващи сексуалното насилие и експлоатация на деца.

Освен това развитието на технологиите доведе до появата на Интернет на нещата, където все повече и повече устройства могат да се свързват, да комуникират и да влизат в мрежа по Интернет. Това включва играчки, бебешки монитори и устройства, задвижвани от изкуствен интелект, които могат да представляват рискове по отношение на неприкосновеността на личния живот и нежелания контакт.

2.4 Ключови заплахи за децата онлайн

Възрастните и децата са изложени на редица рискове и опасности онлайн. Въпреки това децата са много по-уязвимо население. Някои деца също са по-уязвими от други групи деца, например деца с увреждания[20] или деца в движение. Създателите на политики трябва да гарантират, че всички деца могат да се развиват и образоват в безопасна цифрова среда. Идеята, че децата са уязвими и следва да бъдат защитени от всички форми на експлоатация, е изложена в Конвенцията на ООН за правата на детето. Няколко области в цифровата среда предлагат големи възможности за децата, но в същото време могат да утежнят рисковете, които биха могли да навредят дълбоко на децата и да подкопаят тяхното благосъстояние. Съществуват опасения, както за възрастни, така и за деца, че например Интернет може да се използва за нарушаване на личния живот, разпространяване на дезинформация или по-лошо, за да се позволи достъп до порнография.

Тук е от решаващо значение да се прави разграничение между рисковете и вредите за децата. Не всяка дейност, която може да носи елементи на риск, е опасна и не всички рискове стават непременно вредни за децата, например секстинг, който е начин, по който младите хора могат да изследват сексуалността и взаимоотношенията, и който не е непременно вреден.

---

[19] УНИЦЕФ, „Глобален сравнителен доклад за децата онлайн (2019 г.)" (УНИЦЕФ, 2019 г.)

[20] Lundy et al., „ДВЕ КЛИКАНИЯ НАПРЕД И ЕДНО КЛИКАНЕ НАЗАД," Доклад за деца с увреждания в цифровата среда (Съвет на Европа, октомври 2019 г.), https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

Фигура 2: Класификация на онлайн заплахите за децата[21]

	съдържание детето като получател приемник /на масова продукция	**контакт** детето като участник (инициирана от възрастен дейност)	**поведение** детето като актьор (извършител/жертва)
агресивни	**насилствено/брутално съдържание**	**тормоз**	**тормоз враждебна дейност**
сексуални	**порнографско съдържание**	**сприятеляване, сексуално насилие при среща с непознати**	**сексуален тормоз, секстинг**
ценностни	**расистко/омразно, обидно съдържание**	**идеологически убеждения**	**потенциално вредно съдържание, генерирано от потребителите**
търговски	**реклама, продуктово позициониране**	**използване и злоупотреба с лични данни**	**хазартни игри, нарушаване на авторски права**

Източник: Деца от ЕС онлайн (Livingstone, Haddon, Görzig и Ólafsson (2011)

Появата на цифровата ера постави нови предизвикателства пред защитата на детето. Децата трябва да имат възможност да се ориентират безопасно в онлайн света и да се възползват от многобройните му награди.

Създателите на политики трябва да гарантират, че съответното законодателство, гаранции и инструменти са въведени, за да се даде възможност на децата да се развиват и учат безопасно. От решаващо значение е децата да разполагат с необходимите умения за идентифициране на заплахите и да разбират напълно последиците и нюансите на своето поведение онлайн.

Докато са онлайн, децата могат да се сблъскат с множество заплахи от организации, възрастни и техните връстници.

Съдържание и манипулация

- Излагането на неподходящо или дори престъпно съдържание може да доведе децата до крайности като самонараняване, разрушително и насилствено поведение. Излагането на такова съдържание може също така да доведе до радикализация или присъединяване към расистки или дискриминационни идеи. Установено е, че много деца не спазват възрастовите ограничения, поставени на уебсайтовете.

[21] Livingstone, S., Haddon, L., Görzig, A. и Ólafsson, K. (2011 г.). *Рискове и безопасност в Интернет: Гледната точка на европейските деца. Пълни констатации*. LSE, Лондон: EU Kids Online, http://eprints.lse.ac.uk/33731/.

- Излагането на неточна или непълна информация ограничава разбирането на децата за света около тях. Тенденцията за персонализиране на съдържанието въз основа на поведението на потребителите може да доведе до „филтърни мехурчета“, ‘filter bubbles’ което ограничава децата да развиват и достигат широк спектър от съдържание.
- Излагането на съдържание, което е алгоритмично филтрирано с намерението да се манипулира, може значително да повлияе на развитието, мненията, ценностите и навиците на детето. Изолирането на децата в „ехо камери„‘echo chambers’ или „филтърни мехурчета“ им пречи да получат достъп до голямо разнообразие от мнения и идеи.

Контакт с възрастни или връстници

Децата могат да се сблъскат с широк спектър от заплахи при контакт с техни връстници или възрастни.

- Онлайн тормозът може да се разпространи по-широко, с по-голяма скорост, отколкото офлайн. Той може да се случи по всяко време на деня или нощта, като по този начин нахлуе в предишните „безопасни пространства“ и може да бъде анонимен.
- Децата, които са жертви офлайн, вероятно ще бъдат жертви и онлайн. По този начин децата с увреждания са изложени на по-висок риск онлайн, тъй като проучванията показват, че е по-вероятно децата с увреждания да бъдат подложени на каквато и да е злоупотреба, и по-специално е по-вероятно да бъдат подложени на сексуална виктимизация. Виктимизацията може да включва тормоз, изключване и дискриминация въз основа на действителното или предполагаемо увреждане на детето или на аспекти, свързани с неговото увреждане, като например начина, по който то се държи или говори, или оборудването или услугите, които използва.
- Клевета и накърняване на репутацията: изображенията и видеоматериалите могат да бъдат променяни и споделяни с милиарди хора. Неуместни коментари могат да бъдат достъпни в продължение на десетилетия, видими безплатно за всеки.
- Децата могат да бъдат нападани, примамвани за среща и малтретирани чрез Интернет от нарушители или на местно равнище, или от другата страна на света, като често твърдят, че са някой, който не са. Това може да приеме няколко форми, включително радикализация или принуда да изпраща изрично сексуално съдържание за себе си.
- Да бъдат подложени на натиск, подведени или принудени да правят покупки със или без разрешението на платеца на сметката.
- Нежеланата реклама повдига въпроси, свързани със съгласието и продажбата на данни.

Поведение на детето, което може да доведе до последици

- Тормозът онлайн може да бъде особено разстройващ и увреждащ, тъй като може да се разпространи по-широко, с по-голяма степен на публичност, а съдържанието, разпространявано по електронен път, може да се появи отново по всяко време, което може да направи по-трудно за жертвата на тормоза да се справи с инцидента; може да съдържа вредни визуални изображения или болезнени думи; съдържанието е достъпно 24 часа в денонощието; тормозът чрез електронни средства може да се случи 24/7 така че да може да нахлуе в неприкосновеността на личния живот на жертвата дори в други „безопасни“ места, като например техния дом; и личната информация може да бъде манипулирана, визуалните изображения се променят и след това те се предават на другите. Освен това може да бъде извършен анонимно. Може да бъде разкриване на лична информация, водеща до риск от физическо увреждане, включително реални срещи с познати онлайн, с възможност за физическо и/или сексуално насилие.
- Нарушаване на техните собствени права или правата на други лица чрез плагиатство и качване на съдържание без разрешение, включително заснемане и качване на неподходящи снимки без разрешение.
- Нарушаване на авторските права на други лица, например чрез изтегляне на музика, филми или телевизионни програми, които трябва да бъдат платени, тъй като това може да бъде вредно за пострадалия от кражбата.
- Принудително и прекомерно използване на Интернет и/или онлайн игри в ущърб на социални дейности и/или дейности на открито, които са важни за здравето, изграждането на доверие, социалното развитие и общото благосъстояние.
- Опити да наранят или тормозят някой друг, включително да се преструват на някой друг, често и на друго дете.
- Все по-често срещано поведение от страна на тийнейджърите е „сексиране“ (споделяне на сексуализирани изображения или текст чрез мобилни телефони). Тези изображения и текст често се споделят между партньори в отношенията или с потенциални партньори, но понякога в крайна сметка се споделят и с много по-широка аудитория. Смята се, че е малко вероятно младите тийнейджъри да имат адекватно разбиране за последиците от това поведение и потенциалните рискове, до които те водят.

2.5 Основни вреди за децата онлайн

Предишният раздел се отнася до заплахите, с които децата могат да се сблъскат онлайн. В този раздел се подчертават вредите, които могат да възникнат от тези заплахи.

Вреди

Според проучвания на УНИЦЕФ относно използването на Интернет следните категории се считат за рискове и вреди:

— **Самозлоупотреба и самонараняване:**

• самоубийствено съдържание

• дискриминация

— **Експозиция на неподходящи материали:**

• излагане на екстремистко/насилствено/, брутално съдържание

• продуктово позициониране

• онлайн хазарт

— **Около 20 % от децата, изследвани по темата, заявяват, че през изминалата година са видели уебсайтове или онлайн дискусии за хора, които физически се наранят или увреждат.**

— **Радикализация:**

• идеологическо убеждаване

• изказвания, подбуждащи към омраза

— **Децата са по-склонни да съобщават, че са разстроени от изказвания, подбуждащи към омраза, или сексуално съдържание онлайн, че са били третирани по обиден начин онлайн или офлайн, или като се срещнат с някого лице в лице, което първо са опознали онлайн.**

— **Сексуално насилие и експлоатация:**

• самостоятелно генерирано съдържание

• сексуално сприятеляване

• материали, съдържащи сексуално насилие над деца (CSAM)

• трафик

• сексуална експлоатация на деца по време на пътувания и туризъм

Проучване от 2017 г. на деца в Дания, Унгария и Обединеното кралство установи, че 6 % от децата имат изрични снимки, които са споделяни без тяхно разрешение.

През 2019 г. Фондацията за наблюдение на Интернет (IWF) идентифицира над 132 000 уебстраници, за които е потвърдено, че съдържат изображения и видеоклипове на сексуално насилие над деца. Всяка уебстраница може да съдържа всичко от едно до хиляди изображения на тази злоупотреба.

Рисковете, свързани с насилието онлайн, като разпространението на голи снимки без съгласие и сексуалния кибертормоз, са белязани от неравномерна динамика по

отношение на пола, като момичетата обикновено са по-силно засегнати от полов натиск към сексуално поведение с последици, които са по-негативни и причиняват вреда.

— **Нарушаване и злоупотреба с лични данни:**

• хакерство

• измами и кражби

Много хора са запознати с измами и хакерство, но нахлуването в личния живот по отношение на онлайн дейностите на детето се разглежда като друго нарушение. Възрастните често проверяват младите хора, като контролират мобилните им телефони и проучват дейностите им онлайн, например докладите на деца в Бразилия показват, че както момчетата, така и момичетата от различни възрастови групи смятат, че родителите упражняват по-голям контрол върху използването на Интернет от страна на момичетата. Опитите да се обясни това често предполагат, че в някои случаи момичетата могат да бъдат по-уязвими поради обществените структури, в които живеят, по-специално по отношение на тяхната безопасност, в контекст, в който границата между онлайн и офлайн взаимодействие става все по-размита.

— **Кибертормоз, преследване и тормоз: Враждебна и насилствена дейност от връстници**

Чат стаите и сайтовете на социалните мрежи могат да отворят вратата за насилие и тормоз, когато анонимните потребители, включително младите хора, участват в агресивна или злонамерена комуникация. В седем държави в Европа — Белгия, Дания, Ирландия, Италия, Португалия, Румъния и Обединеното кралство — Livingstone, Mascheroni, Ólafsson и Haddon[22] установиха, че средно през 2010 г. 8 % от децата са били подложени на кибертормоз, докато 12 % от децата са били жертви на кибертормоз през 2014 г.

От съществено значение е да се отбележи, че уязвимите деца често са изложени на по-висок риск от кибертормоз.

На фокус: Засилване на неравенствата

През 2017 г. около 60 % от децата в региона на Африка не са били онлайн в сравнение със само 4 % в Европа. Интернет потребителите от мъжки пол превъзхождат жените потребители във всеки регион на света, а използването на Интернет от момичета често се наблюдава и ограничава. С разширяването на широколентовия достъп до несвързани части на света това неравенство ще се увеличи значително[23].

Децата, които разчитат на мобилни телефони, а не на компютри, могат да получат само второто най-добро онлайн преживяване. Децата, които говорят малцинствени

[22] Livingstone, S., Mascheroni, G., Ólafsson, K., and Haddon, L., (2014) *Детски онлайн рискове и възможности: сравнителни констатации от EU Kids Online и Net Children Go Mobile*. Лондон: London School of Economics and Political Science, www.eukidsonline.net и hYp://www.netchildrengomobile.eu/.

[23] Комисията за широколентов достъп, „Безопасност на децата онлайн: Минимизиране на риска от насилие, злоупотреба и експлоатация онлайн (2019 г.)“

езици, често не могат да намерят подходящо съдържание онлайн, а за децата от селските райони е по-вероятно да се сблъскат с кражба на пароли или пари.

Изследванията показват, че много подрастващи по света срещат значителни пречки пред участието си в Интернет. За много хора основните пречки продължават да бъдат предизвикателствата пред достъпа — слабата свързаност, твърде високите разходи за данни и устройства и липсата на подходящо оборудване.

С разширяването на широколентовия достъп на достъпни цени за развиващия се свят е необходимо спешно да се въведат мерки за свеждане до минимум на рисковете и заплахите за тези деца, като същевременно им се даде възможност да се възползват от всички предимства на цифровия свят.

На фокус: Материали за сексуално насилие над деца (CSAM)

Мащабът на проблема

Интернет преобрази мащаба и естеството на производството, разпространението и наличността на материали за сексуално насилие над деца (Child Sexual Abuse Material - CSAM). През 2018 г. технологичните компании, базирани в Съединените американски щати, съобщиха за над 45 милиона онлайн изображения и видеоматериали, за които се подозира, че показват сексуално насилие над деца от цял свят. Това е глобална индустрия и мащабът и тежестта на злоупотребите се увеличават въпреки усилията за нейното спиране.

Исторически погледнато, в един офлайн свят намирането на CSAM изисква нарушителите да поемат значителни рискове на висока цена, за да получат достъп до материалите. С Интернет нарушителите вече имат сравнително лесен достъп до този материал и се ангажират с все по-рисково поведение. Камерите са по-малки, все по-интегрирани във всеки аспект на живота ни, което прави процеса на производство на CSAM и придобиване на съдържание от безконтактни злоупотреби по-лесно, отколкото някога е било.

Невъзможно е да се определи точният размер или форма на това нелегално и незаконно начинание. Ясно е обаче, че броят на незаконните изображения, които понастоящем са в обращение, може да бъде отчетен в милиони. Почти всички деца, участващи в изображенията, са дублирали образа си. През 2018 г. IWF проследи колко често се появяват изображения на дете, за което е известно, че е било спасено през 2013 г. През трите месеца анализаторите от IWF проследяваха изображенията 347 пъти — 5 пъти всеки работен ден.

Настоящата картина

Всеки път, когато изображение на дете, което е малтретирано, се появи за първи път или отново онлайн или бъде изтеглено от извършител нарушител, това дете бива

подлагано на повторно малтретиране. Жертвите са принудени да живеят с дълголетието и разпространението на тези изображения до края на живота си.

Веднага след като бъде открит изобразяващ материал или хостинг на уеб страница със сексуално насилие над деца, е важно съдържанието да бъде премахнато или блокирано възможно най-бързо. Глобалният характер на Интернет затруднява това: нарушителите могат да произвеждат материали в една държава и да ги хостват в друга за потребителите. Почти невъзможно е националните разпореждания или известия да бъдат приведени в действие без задълбочено международно сътрудничество.

Темпът на иновациите в цифровия свят означава, че положението на нарушителите непрекъснато се променя. Основните заплахи, които се появиха наскоро, включват:

- Възходът на криптирането неволно позволява на нарушителите да оперират и споделят материали по скрити канали, което прави откриването и правоприлагането по-трудно.
- Форумите, посветени на сприятеляването с деца, се разрастват в защитени места на Интернет, нормализират и насърчават това поведение, като често изискват да се присъединява „ново съдържание“ .
- Бързото развитие на Интернет дава възможност на потребителите да отидат онлайн в области, където все още не са разработени/приложени всеобхватни защитни стратегии или съответната инфраструктура.
- Децата използват устройства без надзор на ранна възраст, а сексуалното поведение онлайн се нормализира. Броят на самостоятелно генерираните изображения на злоупотреби нараства всяка година.

На фокус: Самостоятелно генерирано съдържание

Децата и юношите могат да правят компрометиращи снимки или видеоклипове на себе си. Въпреки че това поведение само по себе си не е непременно незаконно и може да се осъществява като част от нормално, здравословно сексуално развитие, съществува риск такова съдържание да бъде разпространявано онлайн или офлайн, за да навреди на деца или да се използва като основа на услуги за изнудване. Въпреки че някои деца могат да бъдат притиснати или принудени да споделят сексуални изображения, други (по-специално подрастващите) могат доброволно да произвеждат сексуално съдържание. Това не означава, че те са съгласни или са отговорни за експлоатацията или злоупотребата и/или разпространението на тези изображения. Секстингът е дефиниран като „самосъздаване на сексуални изображения„ [24] или като „обмен на сексуални

[24] Карън Купър и др., „Юноши и самозатворени сексуални образи: преглед на литературата“, Компютри в човешкото поведение 55 (февруари 2016 г.): 706–16, https://doi.org/10.1016/j.chb. 2015.10.003 .

съобщения или изображения“ и „създаване, споделяне и препращане на сексуално внушаващи голи или почти голи изображения чрез мобилни телефони и/или Интернет“[25]

Секстингът е форма на самостоятелно генерирано сексуално изрично съдържание[26] и практиката е „изключително различна по отношение на контекста, смисъла и намерението“[27].

Докато секстингът е вероятно най-честата форма на самостоятелно генерирано изрично сексуално съдържание, включващо деца, и често се извършва от и сред даващите съгласие юноши, които извличат удоволствие от преживяването, има и много форми на нежелано сексиране. Това се отнася до неконсенсусните аспекти на дейността, като например споделяне или получаване на нежелани снимки, видеоматериали или съобщения с нежелано сексуално съдържание, например от известни или неизвестни лица, които се опитват да осъществят контакт, да окажат натиск върху или да се сприятелят с детето. Секстингът може да бъде и форма на сексуален тормоз, при който детето е подложено на натиск да изпрати снимка на приятел/приятелка/партньор, който след това я разпространява в партньорска мрежа без тяхно съгласие.

На фокус: Кибертормоз

Въпреки че тормозът като явление далеч предхожда Интернет, добавеният мащаб, обхват и непрекъснатост на тормоза, извършван онлайн, могат да изострят още повече това, което вече е обезпокояващо и често вредно за жертвите. Кибертормозът се определя като умишлена и повтаряща се вреда, причинена чрез използването на компютри, мобилни телефони и други електронни устройства. Той често се осъществява успоредно с офлайн тормоза, който се извършва в училище или другаде, може да има допълнителни расистки, религиозни или сексистки измерения и може да представлява продължение на вредите, причинени офлайн, като например чрез хакерство на акаунти, разпространяване на снимки и видеоклипове онлайн и денонощното естество на вредните послания и наличието на съдържание. Като цяло социален въпрос, а не с криминален характер, политиките за справяне с кибертормоза изискват цялостен подход, който да включва училищата, семействата и най-вече самите деца.

На фокус: Онлайн сприятеляване и изнудване

Предвид бързия напредък в технологиите и увеличения достъп до Интернет и цифрови комуникации, наблюдаван през последните години, неизбежно последва повишен риск от онлайн престъпни деяния, насочени срещу деца. Сред тези нововъзникващи форми на сексуална експлоатация на деца онлайн са онлайн

[25] Джесика Рингроуз и др., „Качествено изследване на деца, млади хора и „секстинг“: доклад, изготвен за NSPCC“ (Лондон, Обединеното кралство: Национално дружество за превенция на жестокостта към деца, 2012 г.) http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x .

[26] UNODC, “Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children” (Vienna: UN, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.[3] UNODC, Проучване на въздействието на новите информационни технологии върху злоупотребата и експлоатацията на деца, стр. 22.

[27] Cooper et al., “Adolescents and Self-Taken Sexual Images.”*

сприятеляването с цел сексуална злоупотреба с деца и изнудването на деца. Онлайн сприятеляването с цел сексуална злоупотреба най-общо се отнася до процеса на сприятеляване и оказване на влияние върху дете (на възраст под 18 години) чрез Интернет или други цифрови технологии, за да се улесни контактът или неконтактното сексуално взаимодействие с това дете. Чрез процеса на сприятеляване извършителят се опитва да спечели доверието от страна на детето, за да запази тайна и да избегне разкриването и наказанието[28]. Важно е да се признае, че има и случаи на злоупотреба между връстници.

Интерпол съобщава, че Интернет улеснява сприятеляването с цел сексуална злоупотреба, тъй като има голям брой леснодостъпни потенциални цели и дава възможност на нарушителите да се представят по привлекателен за детето начин. Онлайн извършителите на сексуални престъпления срещу деца използват манипулация, принуда и съблазняване към по-малки задръжки и примамват децата да се занимават със сексуална активност. Нарушителят предприема умишлен процес на идентифициране на уязвима потенциална жертва, събиране на информация относно подкрепата на семейството на детето и използва натиск или срам/страх за сексуално насилие над дете. Нарушителите могат да използват порнография за възрастни и материали, съдържащи малтретиране или експлоатация на деца, за да постигнат потенциалните си цели, като представят сексуалната активност на децата като естествена и нормална. Интернет промени начина, по който хората си взаимодействат, и предефинира понятието „приятел“. Нарушителят може да установи приятелство с дете онлайн много лесно и бързо, което налага преоценка на традиционните образователни послания за „опасност от непознат“.

Онлайн сприятеляването с цел сексуална злоупотреба беше официално признато през 2007 г. в международен правен инструмент от **Конвенцията на Съвета на Европа за закрила на децата срещу сексуална експлоатация и сексуално насилие** (Конвенция Лансароте). Член 23 инкриминира „склоняването на деца за сексуални цели“ което изисква да има умишлено предложение за среща с детето с цел извършване на сексуално престъпление, последвано от „материални действия, водещи до такава среща“. В много случаи на сприятеляване с деца с цел сексуална злоупотреба с децата се злоупотребява и се експлоатират онлайн — „срещата“, визирана от Конвенцията от Лансароте, и много съществуващи национални закони е изцяло виртуална — но въпреки това е еднакво вредна за детето като физическата среща. От решаващо значение е криминализирането на сприятеляването с цел сексуална злоупотреба да обхваща „случаите, в които сексуалното насилие не е резултат от лична среща, а се извършва онлайн“[29].

---

[28] Международен център за изчезнали и експлоатирани деца, "Онлайн сприятеляване с деца за сексуални цели: Model Legislation & Global Review, 1st Edition (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

[29] Комитет Лансароте, Комитет на страните по Конвенцията на Съвета на Европа за защита на децата срещу сексуална експлоатация и сексуално насилие, склоняване към *деца за сексуални цели чрез информационни и комуникационни технологии (сприятеляване с цел сексуална злоупотреба), становище относно член 23 от Конвенцията от Лансароте и обяснителната бележка към нея*, юни. 17, 2015 г., *https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html* (последно посетен на 6 ноември 2019 г.).

Сексуалното изнудване [30] може да се случи като характеристика на онлайн сприятеляване с цел сексуална злоупотреба или като самостоятелно престъпление. Докато изнудването може да се случи без процеса на онлайн сприятеляване, в някои случаи онлайн сприятеляването може да доведе до изнудване[31]. Сексуалното изнудване може да се случи в контекста на онлайн сприятеляване, тъй като нарушителят манипулира и оказва влияние върху детето по време на процеса на сприятеляване с цел сексуална злоупотреба чрез заплахи, сплашване и принуда да изпращат сексуални изображения на себе си (самосъздадено съдържание)[32]. Ако жертвата не предостави поисканите сексуални услуги, допълнителни интимни изображения, пари или други облаги, неговите изображения могат да бъдат публикувани онлайн с цел да се предизвика унижение или дистрес или да се принуди детето да генерира допълнителен сексуален материал[33].

Сексуалното изнудване се нарича „виртуално сексуално насилие“ поради подобни емоционални и психологически ефекти върху жертвите[34]. В някои случаи малтретирането е толкова травмиращо, че жертвите са се опитали да се самонаранят или да се самоубият като средство за бягство от тормоза.

Европол отбеляза, че събирането на информация за оценка на обхвата на изнудването, което засяга децата, е предизвикателство и е недостатъчно докладвано[35]. Освен това липсата на обща терминология и определения за онлайн сприятеляването с цел сексуална злоупотреба и изнудване са пречки пред събирането на точни данни и разбиране за истинския обхват на проблематиката в световен мащаб.

2.6 Деца с уязвимости

Децата и младите хора могат да бъдат уязвими по различни причини. Изследванията, проведени през 2019 г., показват, че „цифровият живот на уязвимите деца рядко получава същото нюансирано и чувствително внимание, което „реалният живот“ често привлича. Освен това в доклада се казва, че „в най-добрия случай те [деца и млади хора] получават същите общи онлайн съвети за безопасност като всички други деца и млади хора, като същевременно е необходима специализирана намеса“. Три

[30] Национален център за изчезнали и експлоатирани деца (NCMEC), *Sextortion, http://www.missingkids.com/theissues/onlineexploitation/sextortion* http://www.missingkids.com/theissues/onlineexploitation/sextortion (последно посетен на 6 ноември 2019 г.).

[31] Терминологични насоки за защита на децата от сексуална експлоатация и сексуално насилие, Междуведомствена работна група по сексуална експлоатация на деца, Люксембург, 28 януари 2016 г., D.4iii, 27—28, *на адрес* http://luxembourgguidelines.org/english-version.

[32] Терминологични насоки за защита на децата от сексуална експлоатация и сексуално насилие, Междуведомствена работна група по сексуална експлоатация на деца, Люксембург, 28 януари 2016 г., D.4iii, 27—28, *на адрес* http://luxembourgguidelines.org/english-version.

[33] Терминологични насоки за защита на децата от сексуална експлоатация и сексуално насилие, Междуведомствена работна група по сексуална експлоатация на деца, Люксембург, 28 януари 2016 г., D.4iii, 27—28, *на адрес* http://luxembourgguidelines.org/english-version.

[34] Benjamin Wittes et al., "Sextortion: Киберсигурност, тийнейджъри и дистанционно сексуално нападение" (Brookings Institution, 11 май 2016 г.), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

[35] Европол, "Онлайн сексуалната принуда и изнудването като форма на престъпност, засягаща деца: Перспектива в областта на правоприлагането" (Европейски център за борба с киберпрестъпността, май 2017 г.), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

примера за специфични уязвимости са: деца мигранти, деца с разстройства от аутистичния спектър и деца с увреждания, но разбира се, има и много други.

Деца мигранти

Децата и младите хора от мигрантски произход често идват в една държава (или вече живеят там) с особен набор от социално-културни преживявания и очаквания. Докато технологията обикновено се счита за посредник при свързването и участието, онлайн рисковете и възможностите могат да се различават значително в различните контексти. Освен това емпиричните констатации и изследвания показват жизненоважната функция на цифровите медии като цяло:

- Това е важно за ориентацията (при пътуване до нова държава).
- Тя е централна функция за присвояване и запознаване с обществото/културата на приемащата държава.
- Социалните медии могат да играят ключова роля за поддържането на контакт със семейството и връстниците, както и за достъпа до обща информация.

Наред с многото положителни аспекти цифровите медии могат също така да доведат до предизвикателства за мигрантите, включително:

- Инфраструктура — важно е да се помисли за безопасни пространства онлайн, така че децата мигранти и младите хора да могат да се възползват от неприкосновеността на личния живот и безопасността.
- Ресурси — мигрантите харчат по-голямата част от парите си за предплатени телефонни карти.
- Интеграция — наред с достъпа до технологии децата мигранти и младите хора също трябва да получат добро цифрово образование.

Деца с нарушения на аутистичния спектър (ASD)

Спектърът на аутизма обобщава две основни области в процеса на диагностика на поведението на DSM-5:

- ограничено и повтарящо се поведение („необходимост от еднаквост“);
- трудности със социалното и комуникативното поведение;
- чести съвместни прояви с интелектуални увреждания, езикови проблеми и други подобни.

Технологиите и Интернет предлагат безкрайни възможности за децата и младите хора, когато учат, общуват и играят. Наред с тези ползи обаче съществуват много рискове, по отношение на които децата и младите хора с ASD могат да бъдат по-уязвими:

- Интернет може да предостави на децата и младите хора с аутизъм възможности за социализиране и специални интереси, които може да нямат офлайн.
- Социалните предизвикателства, като например трудното разбиране на намеренията на другите, могат да направят тази група уязвима за „приятели“ с лоши намерения.

- Онлайн предизвикателствата често са свързани с основните характеристики на аутизма: конкретни, специфични Насоки биха могли да подобрят онлайн преживяванията на отделните лица, но основните предизвикателства остават.

Деца с увреждания

Децата с увреждания са изправени пред рискове онлайн по много от същите начини като децата без увреждания, но те могат също така да бъдат изправени пред специфични рискове, свързани с техните увреждания. Децата с увреждания често са изправени пред изключване, стигматизация/заклеймяване и пречки (физически, икономически, обществени и поведенчески) за участието в техните общности. Тези преживявания могат да допринесат за това дете с увреждане да търси социални взаимодействия и приятелства в онлайн пространствата, което може да бъде положително, да изгради самочувствие и да създаде мрежи за подкрепа. Те обаче могат също така да ги изложат на по-голям риск от случаи на сприятеляване с цел сексуална злоупотреба, онлайн склоняване и/или сексуален тормоз — изследванията показват, че децата, изпитващи затруднения офлайн, и тези, които са засегнати от психосоциални затруднения, са изложени на повишен риск от подобни инциденти[36].

Като цяло децата, които са жертви офлайн, вероятно ще бъдат жертви и онлайн. По този начин децата с увреждания са изложени на по-висок риск онлайн, но те имат по-голяма нужда да бъдат онлайн. Изследванията показват, че е по-вероятно децата с увреждания да бъдат подложени на каквато и да е злоупотреба[37], като по-специално е по-вероятно да изпитат сексуална виктимизация[38]. Виктимизацията може да включва тормоз, изключване и дискриминация въз основа на действителното или предполагаемо увреждане на детето или на аспекти, свързани с неговото увреждане, като например начина, по който то се държи или говори, оборудването или услугите, които използва.

Извършителите на сприятеляване с цел сексуална злоупотреба, онлайн склоняване и/или сексуален тормоз спрямо деца с увреждания могат да включват не само извършителите на престъпления, които се насочват към деца, но и тези, които са насочени към деца с увреждания. Такива нарушители могат да включват поклонници ‘devotees’ — лица без увреждания, които са сексуално привлечени от хора с увреждания (най-често ампутирани и лица, използващи помощни средства за мобилност), някои от които дори се преструват, че са с увреждания[39]. Действията на такива хора могат да включват изтеглянето на снимки и видеоматериали на деца с увреждания (които са безвредни по своя характер) и/или споделянето им чрез специализирани форуми, или профили в социалните медии. Инструментите за докладване във форумите и социалните медии често нямат целенасочен или подходящ начин за справяне с такива действия.

---

[36] Андрю Шрок и др., „Склоняване, тормоз и проблемно съдържание“, Berkman Center for Internet & Society, Harvard University, декември 2008 г., 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

[37] УНИЦЕФ, „Доклад за състоянието на децата в света: Деца с увреждания“, 2013 г., https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

[38] Катрин Мюлер-Джонсън, Мануел П. Айснер и Ингрид Обсут, „Сексуална виктимизация на младежи с физическо увреждане: Изследване на нивата на разпространение, рисковете и защитните фактори“, Journal of Interpersonal Violence 29, бр. 17 (ноември 2014 г.): 3180–3206, https://doi.org/10.1177/0886260514534529.

[39] Richard L Bruno, “Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder,” *Sexual and Disability* 15, no. 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

Съществуват опасения, че „споделянето“ (родители, които споделят информация и снимки на своите деца онлайн) може да наруши неприкосновеността на личния живот на детето, да доведе до тормоз, да предизвика неудобство или да има отрицателни последици на по-късен етап от живота[40]. Родителите на деца с увреждания могат да споделят такава информация в търсене на подкрепа или съвети, като поставят децата с увреждания в по-висок риск от неблагоприятни последици.

Някои деца с увреждания могат да се сблъскат с трудности при използването или дори изключването от онлайн среда поради недостъпен дизайн (напр. приложения, които не позволяват увеличаване на размера на текста), отказ на поисканите улеснения (напр. софтуер за четене на екран или адаптивни компютърни контроли) или необходимостта от подходяща подкрепа (напр. наставничество за това как да се използва оборудването, подкрепа за навигация в социалните взаимодействия[41]).

По отношение на риска по договора или подписването на общите условия, децата с увреждания са изложени на по-висок риск да приемат правни условия, които понякога дори възрастните не могат да разберат.

2.7 Възприятията на децата за онлайн рисковете

Излагане на насилие в световен мащаб, достъп до неподходящо съдържание, стоки и услуги; опасения относно прекомерната употреба; въпросите, свързани със защитата на данните и неприкосновеността на личния живот, са рисковете, изтъкнати от децата[42].

Подрастващите съобщават за редица опасения по отношение на ангажираността си с цифровите технологии. Сред тях са широко обсъжданите опасения относно безопасността онлайн, като страховете от взаимодействие с непознати лица онлайн, достъп до неподходящо съдържание или излагане на зловреден софтуер или вируси, докато други са свързани с надеждността на техния достъп до технологии; намеса на родителите в техния „частен“ живот онлайн; и уменията им за цифрова грамотност[43].

Изследванията на ЕС за децата онлайн показват, че порнографията и насилственото съдържание са най-важните проблеми на децата онлайн в Европа. Като цяло момчетата изглеждат по-загрижени от насилието, докато момичетата са по-загрижени за рисковете, свързани с контактите[44]. Загрижеността относно рисковете е по-

[40] UNICEF, “Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy,” Innocenti Discussion Paper 2017-03 (UNICEF, Office of Research-Innocenti), accessed January 16, 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

[41] За насоки относно тези права вж. Конвенцията за правата на хората с увреждания, член 9 относно достъпността и член 21 относно свободата на изразяване на мнение и свободата на мнение и достъпа до информация.

[42] Amanda Third et al., “Children’s Rights in the Digital Age” (Melbourne: oung and Well Cooperative Research Centre, September 2014), http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

[43] Amanda Third et al., “Young and Online: Children’s Perspectives on Life in the Digital Age,” The State of the World’s Children 2017 Companion Report (Sydney: Western Sydney University, 2017). В доклада се обобщават мненията на 490 деца на възраст 10—18 години от 26 различни държави,които говорят 24 официални езика.

[44] Livingstone, S. (2014) *EU Kids Online: Констатации, методи, препоръки*. LSE, Лондон: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.

голяма сред децата от държавите с висока степен на използване на Интернет и висок риск.

В Латинска Америка консултациите с деца показаха, че загубата на лична неприкосновеност, насилие и тормоз са основните тревоги[45]. Децата съобщават, че се свързват с хора, които не познават — това е особено случаят, когато играят игри онлайн. В такива ситуации изглежда, че основната стратегия не е да се ангажира и/или блокира лицето. Момичетата са изправени пред тормоз в социалните медии от ранна възраст. Те успяват сами да се ориентират в тези форми на насилие, като блокират потребителите и променят настройките за неприкосновеност на личния живот. Тормозът идва от потребители, които понякога не говорят испански, но успяват да им изпратят изображения, да поискат приятелство и да коментират публикациите им. Някои момчета също съобщават, че са получили такива искания и заявки.

В много части на света децата добре разбират някои от рисковете, пред които са изправени онлайн[46]. Изследванията показват, че по-голямата част от децата са в състояние да разграничат кибертормоза от шегите или закачките и подигравките онлайн, като разбират, че кибертормоза има публично измерение и е предназначен да навреди[47].

[45] Contectados al Sur network, "Hablatam."
[46] От 2016 г. насам МСД провежда консултации в рамките на СОР с деца и възрастни заинтересовани страни по важни въпроси като кибертормоза, цифровата грамотност и дейностите на децата онлайн.
[47] UNICEF, "Global Kids Online Comparative Report (2019)."

3. Подготовка за национална стратегия за защита на децата онлайн

При разработването на национална стратегия за защита на децата онлайн за насърчаване на онлайн безопасността на децата и младите хора, националните правителства и институциите, определящи политиките, трябва да определят най-добрите практики и да се ангажират с ключови заинтересовани страни. В следващите раздели се подчертават типичните участници и заинтересовани страни заедно с описание на тяхната потенциална роля и отговорности по отношение на защитата на децата онлайн.

3.1 Участници и заинтересовани страни

Създателите на политики могат да определят подходящи лица, групи и организации, представляващи всеки от тези участници и заинтересовани страни в рамките на тяхната юрисдикция. Оценяването на всяка една от техните настоящи, планирани и потенциални дейности е важно при всяка национална координация и организиране на стратегиите за защита на децата онлайн.

Деца и младежи

По целия свят децата и младите хора показаха, че могат да се адаптират към новите технологии и да ги използват с голяма лекота. Интернет става все по-важен в училищата и като арена, където децата могат да работят, играят и общуват.

Според последния доклад на Алианса ChildFund само 18, 1 % от интервюираните деца смятат, че управляващите действат, за да ги защитят. Важно е създателите на политики да се ангажират с децата в това отношение, като признават правото им на изслушване (член 12 от Конвенцията за правата на детето).

За да могат да защитават децата, създателите на политики следва да стандартизират определението за дете във всички правни документи. Дете трябва да бъде определено като всеки на възраст под 18 години. Това е в съответствие с член 1 от Конвенцията на ООН за правата на детето (КООНПД), който гласи, че „дете означава всяко човешко същество на възраст под 18 години“. На компаниите не следва да се разрешава да третират като пълнолетни лица, които са на възраст под 18 години, но правно са достатъчно възрастни, за да дадат съгласието си за обработване на данни. Това тясно определение не е оправдано от никакви доказателства за основните етапи на развитието на децата. То подкопава правата и застрашава безопасността на децата.

Въпреки че много деца могат да изглеждат уверени в използването на технологиите, много от тях не се чувстват в безопасност[48] онлайн и имат няколко притеснения[49] по отношение на Интернет.

Липсата на опит на децата и младите хора от широкия свят може да ги направи уязвими от редица рискове. Те имат право да очакват помощ и защита. Важно е също така да се помни, че не всички деца и млади хора ще възприемат Интернет или новите технологии по един и същ начин. Някои деца със специални нужди, причинени от физически или други увреждания, могат да бъдат особено уязвими в онлайн среда и ще се нуждаят от допълнителна подкрепа.

Проучванията многократно показват, че това, което възрастните мислят, че децата и младите хора правят онлайн и какво всъщност се случва, може да бъде много различно. Половината от всички анкетирани деца заявиха, че в страната си възрастните не слушат мнението им по въпроси, които са от значение за тях[50]. Поради тази причина е важно да се гарантира, независимо от договореностите, които се предприемат на национално равнище за разработване на политика в тази област, че са намерени подходящи механизми, позволяващи да се чуят гласовете на всички деца и млади хора, и че се взема предвид техният конкретен опит от използването на технологията.

Родители, настойници и възпитатели

Родителите, настойниците и възпитателите прекарват най-много време с деца. Те следва да бъдат образовани по цифрова грамотност, за да разбират онлайн средата и да могат да защитават децата и да ги учат как да се защитават.

Образователните институции носят особена отговорност да научат децата как да останат по-безопасни онлайн, независимо дали използват Интернет в училище, у дома или навсякъде другаде, а създателите на политики следва да включат в националните учебни програми цифровата грамотност от много ранна възраст (от 3 до 18 години). Това би позволило на децата да се защитават, да познават правата си и следователно да използват Интернет като средство за познание[51].

На създателите на политики се напомня, че родителите и настойниците почти винаги ще бъдат първата, последната и най-добрата линия на защита и подкрепа за собствените си деца. Но когато става въпрос за Интернет, може да се почувстват малко изгубени. Отново училищата могат да действат като важен канал за достигане до родителите и настойниците, за да осъзнаят както рисковете, така и многобройните положителни възможности, които предлагат новите технологии. Въпреки това,

[48] ChildFund Alliance, „НАСИЛИЕТО СРЕЩУ ДЕЦА, КАТО ОБЯСНЕНО ОТ ДЕЦА“, Save Voices Big Dreams, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee61c.pdf

[49] Съвет на Европа, „Това е нашият свят: възгледите на децата за това как да защитят правата си в дигиталния свят“, Доклад за консултации с деца (Съвет на Европа, Отдел за правата на децата, октомври 2017 г.), https://rm.coe.int/ it-s-our-world-children-s-views-on-how-to-protect-right-in-the-/1680765dff .

[50] ChildFund Alliance, “Violence against children as explained by children.”

[51] UNICEF, “Policy Guide on Children and Digital Connectivity” (Policy Lab, Data, Research and Policy, United Nations Children’s Fund, June 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

училищата не трябва да бъдат единственият използван път за достигане до родителите и настойниците. Важно е да се използват много различни канали, за да се увеличи максимално възможността за достигане до възможно най-голям брой родители и настойници. Тук промишлеността играе важна роля в подпомагането на своите потребители или клиенти. Родителите и настойниците могат да изберат да управляват онлайн дейността и достъпа на детето си, да разговарят с детето за правилното поведение и използване на технологиите, да разберат какво прави детето онлайн, така че семейният разговор да интегрира онлайн и офлайн преживяванията в едно цяло.

Родителите и настойниците също трябва да бъдат добър пример за децата си за това как да използват устройствата си и да се държат по подходящ начин в Интернет.

На създателите на политики следва да се напомни, че с родителите и лицата, полагащи грижи, следва да се провеждат консултации, за да се получи тяхното мнение, опит и разбиране за защитата на децата им онлайн.

И накрая, създателите на политики заедно с други публични институции могат да разработят кампании за повишаване на обществената осведоменост, включително за родителите, лицата, полагащи грижи, и възпитателите. Обществените библиотеки, здравните центрове, дори търговските центрове и други големи центрове за търговия на дребно могат да предоставят достъпни места за представяне на информация за електронната безопасност и цифровите умения. При изпълнението на тази задача правителствата следва да гарантират, че предоставяните съвети са неутрални, без какъвто и да било частен интерес и обхващат широк кръг от въпроси в рамките на цифровото пространство.

Промишленост

Промишлеността е една от основните заинтересовани страни в екосистемата, тъй като секторът притежава технологичните знания, които създателите на политики трябва да разгледат и разберат, за да разработят правната рамка. По този начин от съществено значение е създателите на политики да ангажират промишлеността в процеса на изготвяне на законите за онлайн защита на децата.

Също така е важно да се насърчи промишлеността да включи в бизнеса си подход за безопасност още при разработването на нови технологии. Ясно е, че компаниите, които разработват или предоставят нови технологични продукти и услуги, следва да помогнат на своите потребители да разберат как работят и как да ги използват безопасно и по подходящ начин.

Промишлеността също така носи голяма отговорност да спомогне за повишаване на осведомеността относно онлайн програмите и програмите за безопасност, по-специално сред децата и техните родители или настойници, но също и сред широката общественост. По този начин заинтересованите страни от промишлеността ще научат повече за други опасения на заинтересованите страни и за рисковете и вредите, на които са изложени крайните потребители. С тези познания промишлеността би могла да

коригира съществуващите продукти и услуги и да идентифицира опасностите в развитието.

Неотдавнашният напредък в областта на изкуствения интелект проправя пътя за промишлеността да изгради много по-солидни механизми за взаимозависимост и взаимоограничаване, за да идентифицира потребителя и да осигури на децата благоприятна среда за положително онлайн поведение. Този напредък би могъл обаче да създаде и нови рискове за децата.

В някои страни Интернет се управлява от рамка за саморегулиране или съвместно регулиране. Някои държави обаче обмислят или са въвели правни и регулаторни рамки, включително задължения за компаниите да откриват, блокират и/или отстраняват вреди срещу деца от платформи или услуги, както и да предоставят ясни маршрути за докладване и достъп до подкрепа.

Научноизследователската общност и неправителствените организации

В рамките на университетите и научноизследователската общност е много вероятно да има редица учени, които имат професионален интерес и много подробни познания за социалното и техническото въздействие на Интернет. Те са много ценен ресурс за подпомагане на националните правителства и създателите на политики да разработят стратегии, които се основават на твърди факти и добри доказателства. Те могат също така да действат като интелектуална противотежест на бизнес интереси, които понякога могат да бъдат твърде краткосрочни и търговски.

По подобен начин, в рамките на общността на неправителствените организации (НПО) съществува набор от експертни познания и информация, които могат да бъдат безценен ресурс за достигане до деца, родители, лица, полагащи грижи и възпитатели, или за предоставяне на услуги на деца, родители и възпитатели, за да се подпомогне популяризирането на програмата за онлайн безопасност и в по-общ план да се защити обществения интерес.

Правоприлагане

Тъжен факт е, че колкото и прекрасна да е технологията, тя привлича вниманието и на престъпни и антисоциални елементи. Интернет значително увеличи разпространението на материали за сексуално насилие над деца/CSAM и други онлайн вреди. Сексуалните хищници са използвали Интернет, за да направят първоначален контакт с деца, като ги примамват в много вредни форми на контакт, онлайн и офлайн. Различни форми на тормоз могат да навредят много на живота на децата и Интернет предостави нов начин това да се случи.

Поради тези причини е от съществено значение правоохранителните органи да бъдат изцяло ангажирани с всяка цялостна стратегия, която да спомогне за повишаване на безопасността на Интернет за децата и младите хора. Служителите на правоприлагащите органи трябва да бъдат подходящо обучени да провеждат разследвания на свързани с Интернет престъпления срещу деца и млади хора. Те се

нуждаят от подходящо ниво на технически познания и достъп до средства от криминалистиката, за да могат да извличат и интерпретират данни, получени от компютри или Интернет, в най-кратък срок.

Освен това е много важно правоприлагането да установи ясни механизми, които да позволяват на децата и младите хора или на всеки член на обществеността да докладват за всякакви инциденти или опасения, които биха могли да имат във връзка с безопасността на децата или младите хора онлайн. Много държави например са създали горещи линии за улесняване на докладването на CSAM и съществуват подобни специални механизми за улесняване на докладването на други видове проблеми, например тормоз. Създателите на политики следва да работят с Международната асоциация на горещите линии в Интернет (INHOPE), като им оказват подкрепа при оценяването и обработването на докладите на CSAM и се възползват от помощта на INHOPE за организации по света при създаването на гореща линия, където няма такава. Създателите на политики следва да гарантират наличието на отворени канали за комуникация между правоприлагащите органи и другите заинтересовани страни. Правоприлагането е основният източник за изземването на CSAM в рамките на националните граници. Следва да се въведе процес за разглеждане на този материал, за да се установи дали местните жертви могат да бъдат идентифицирани. Когато това не е възможно, материалите следва да бъдат предадени на Интерпол за включване в базата данни ICSE. Тъй като това е глобална заплаха, създателите на политики трябва да гарантират международното сътрудничество между правоприлагащите органи по света. Това би намалило времето на официалните процеси и би позволило на агентите да реагират по-бързо.

Социални услуги

Когато деца или млади хора са били увредени или малтретирани онлайн, например чрез публикуване на неподходяща или незаконна снимка, има вероятност те да се нуждаят от специализирана и дългосрочна подкрепа или консултации. Възможно е също така да се наложи да се обобщят услугите и възстановителните практики за извършителите на престъпления, особено за младите правонарушители, които също може да са станали жертва на онлайн или офлайн злоупотреба. Специалистите, работещи в рамките на социалните служби, ще трябва да бъдат подходящо обучени, за да могат да предоставят такъв вид подкрепа. Подкрепата следва да се предоставя чрез онлайн и офлайн канали.

Здравни услуги

Здравната услуга, необходима след всеки случай на насилие срещу дете, следва да бъде обхваната от основния план за здравеопазване на национално равнище. Лечебните заведения следва задължително да докладват за злоупотреби. Специалистите в областта на здравеопазването следва да бъдат подходящо оборудвани и информирани, за да могат да подкрепят децата в това отношение. Здравните услуги следва да се

разширят, така че да включват подкрепа за психичното здраве и благосъстояние на децата.

Държавни институции

Политиката за онлайн защита на децата ще попада в юрисдикцията на редица правителствени институции и е важно всички те да бъдат ангажирани с всяка успешна национална стратегия и план за действие. Те могат да включват:

- Вътрешни работи
- Здравеопазване
- Образование
- Правосъдие
- Цифрова/информация
- Регулатори

Регулаторните органи са в най-добра позиция да допринасят за ролята на контрольора и одитора в сътрудничество с държавните институции. Това може да включва медийните регулатори и регулаторните органи за защита на данните.

Оператори на широколентови, мобилни и безжични мрежи

Операторите могат да откриват, блокират и докладват за незаконно съдържание в рамките на своята мрежа и да предоставят съобразени със семейството инструменти, услуги и конфигурации за използване от родителите при избора как да управляват достъпа на децата си. Важно е доставчиците да гарантират в еднаква степен зачитането на гражданските свободи и неприкосновеността на личния живот.

Права на детето

Независимите институции за защита на човешките права за децата могат да играят решаваща роля за осигуряването на защита на децата онлайн. Въпреки че техните мандати са различни, тези институции често имат функции за:

- наблюдение на въздействието на правото, политиката и практиката върху защитата на правата на детето;
- насърчаване на прилагането на международните стандарти в областта на правата на човека на национално равнище;
- разследване на нарушения на правата на децата;
- предоставяне на експертен опит в областта на правата на децата в съдилищата;

- гарантиране, че мненията на децата се изслушват по въпроси, свързани с техните права на човека, включително разработването на съответното законодателство и политика;
- насърчаване на общественото разбиране и осведоменост за правата на децата; и
- предприемане на инициативи за образование и обучение в областта на правата на човека.

Важно е да се включат преки консултации с деца, както е тяхното право съгласно член 12 от Конвенцията на ООН за правата на детето. Консултативните, разследващите, повишаването на осведомеността и образователните функции на независимите институции за защита на правата на човека за децата са от значение за предотвратяването и реагирането на вредите, които децата могат да изпитат онлайн. Ето защо тези институции следва да бъдат в основата на разработването на всеобхватен, основан на правата подход за укрепване на правните, регулаторните и политическите рамки, уреждащи защитата на децата онлайн, включително пряка консултация с деца, както и тяхното право съгласно член 12 от Конвенцията на ООН за правата на детето.

В последно време имаше и примери за юрисдикции, които въвеждат или обмислят въвеждането на държавни агенции със специален мандат за подкрепа на правата на детето онлайн, включително защитата от насилие или вреда. Когато съществуват такива агенции, те следва също така да бъдат тясно свързани с усилията за засилване на реакцията по отношение на защитата на децата онлайн на национално равнище.

3.2 Съществуващи отговори за защита на децата онлайн

Разработени са няколко инициативи, за да се действа на национално и международно равнище, предвид нарастващото значение на ИКТ в живота на децата по света и присъщите рискове за най-малките в нашите общества.

Национални модели

На национално равнище следва да се подчертае, че няколко законодателни акта обхващат важни аспекти на всеобхватната рамка за защита на децата онлайн. Те включват, но не се ограничават до:

- Директива за аудиовизуалните медийни услуги (AVMSD) (преразгледана през 2018 г., ЕС)
- Общ регламент относно защитата на данните (ОРЗД) (2018 г., ЕС)

Налице са новаторски промени в регулаторната и институционална реакция на държавите членки на заплахите за безопасността и благосъстоянието на децата онлайн. Няма единен начин да се реагира на CSAM, кибертормоза и други вреди, с които децата се сблъскват онлайн, но е забележително, че през последните няколко години са били изпробвани нови подходи:

Кодекс за подходящ за възрастта дизайн (2019 г., Обединено кралство)

В началото на 2019 г. Службата на информационните комисари публикува предложения за своя „подходящ за възрастта дизайнерски кодекс“ за по-нататъшна защита на децата онлайн. Предложеният кодекс е съсредоточен върху висшия интерес на детето, както е посочено в Конвенцията на ООН за правата на детето, и излага няколко очаквания за промишлеността. Те включват строги мерки за проверка на възрастта, услуги за определяне на местоположението, които по подразбиране трябва да бъдат изключени за деца, за промишлеността да събира и съхранява само минималното количество лични данни на децата, за продукти, които да бъдат безопасни още при проектирането, и за обяснения, които са подходящи и достъпни за възрастта.

Закон за вредните цифрови комуникации (преразгледан през 2017 г., Нова Зеландия)

Законодателството от 2015 г. превърна злоупотребата в кибернетичното пространство в конкретно престъпление и се съсредоточи върху широк кръг вреди — от кибертормоза до порно с цел отмъщение. То има за цел да възпре, предотврати и намали вредната цифрова комуникация, като направи нелегално публикуването на цифрова комуникация с намерението да причини сериозни емоционални затруднения на някой друг, и определи поредица от 10 комуникационни принципа. Тя дава право на потребителите да подават жалби до независима организация, ако тези принципи са нарушени, или да поискат съдебни разпореждания срещу автора или домакина/ host на съобщението, ако проблемът не бъде решен.

Комисар по електронната безопасност /eSafety (2015 г., Австралия)

Комисарят по електронната безопасност е първата в света правителствена агенция, посветена специално на безопасността онлайн. Създадена през 2015 г., eSafety има законодателна роля да ръководи, координира, образова и съветва по въпросите на онлайн безопасността, за да гарантира, че всички австралийци имат безопасни, положителни и предоставящи права преживявания онлайн. eSafety администрира схеми за разследване, които се фокусират върху редица вреди, включително сериозни : кибертормоз на деца, злоупотреба с изображения и забранено съдържание. Тя има правомощието да разследва и да предприема действия за разглеждане на жалби или доклади, свързани с тези видове вреди, включително, в някои случаи, правомощието да отправя уведомления до физически лица и до онлайн услуги за отстраняване на материали. Наред с разследващите си правомощия, eSafety възприема цялостен общностен подход, който се основава на социални, културни и технологични инициативи и интервенции. Нейната превенция, защита и проактивни усилия осигуряват всеобхватен подход към безопасността онлайн.

Международни модели

На международно и транснационално равнище бяха отправени препоръки и стандарти от различни заинтересовани страни. Настоящите Насоки се основават на работата на следните усилия:

Насоки относно прилагането на Факултативния протокол към Конвенцията за правата на детето относно търговията с деца, детската проституция и детската порнография.

Насоки на Съвета на Европа за зачитане, защита и изпълнение на правата на детето в цифровата среда[52].

Насоките са адресирани към всички държави —членки на Съвета на Европа, с цел подпомагане на държавите членки и други заинтересовани страни в усилията им да приемат всеобхватен, стратегически подход за максимално увеличаване на пълния набор от права на децата в цифровата среда. Сред многото обхванати теми са защитата на личните данни, предоставянето на съобразено с нуждите на детето съдържание, адаптирано към развиващите се способности, линиите за помощ и горещите линии, уязвимостта и устойчивостта, както и ролята и отговорностите на промишлените предприятия. Освен това в Насоките държавите се призовават да се ангажират с децата, включително в процесите на вземане на решения, за да се гарантира, че националните политики отговарят адекватно на промените в цифровата среда. Понастоящем Насоките са достъпни на 19 езика. Те ще бъдат придружени от съобразена с интересите на децата версия на документа, както и от Наръчник за създателите на политики, който ще предостави конкретни мерки за прилагане на Насоките.

Съвет на Европа — Конвенция Лансароте

Конвенцията на Съвета на Европа за закрила на децата срещу сексуална експлоатация и сексуално насилие (Конвенция Лансароте) изисква от държавите да предложат цялостен отговор на сексуалното насилие срещу деца чрез подхода „4ps“: Prevention, Protection, Prosecution and Promotion /Предотвратяване, Защита, Наказателно преследване и Насърчаване на националното и международното сътрудничество. Действието на Конвенцията във връзка с цифровата среда беше изяснено от Комитета на страните по Конвенцията за закрила на децата срещу сексуална експлоатация и сексуално насилие („Комитетът Лансароте“) чрез приемането на редица документи. Това са: становище относно сексуалните или явните изображения и/или видеоматериали, генерирани, споделени и получени от деца (6 юни 2019 г.); тълкувателно становище относно приложимостта на Конвенцията Лансароте към сексуални престъпления срещу деца, улеснени чрез използването на ИКТ (12 май 2017 г.); декларация относно Интернет адресите на материали или изображения, съдържащи сексуално насилие над деца, или на други престъпления, установени в съответствие с Конвенцията Лансароте (16 юни 2016 г.) и становище относно член 23 от Конвенцията Лансароте – склоняване на деца за сексуални цели чрез информационни и комуникационни технологии (сприятеляване с деца с цел сексуална злоупотреба). Комитетът Лансароте извършва мониторинг на прилагането на Конвенцията: вторият тематичен кръг от мониторинг на Комитета е съсредоточен върху защитата на децата от сексуална експлоатация и сексуално насилие, улеснени от ИКТ: през 2020 г. е

[52] Съвет на Европа (2020 г.), The Digital Environment,https://www.coe.int/en/web/children/the-digital-environment. Насоките на Съвета на Европа за зачитане, защита и изпълнение на правата на детето в цифровата среда са първият такъв набор от стандарти, приет от междуправителствен орган (CM/Rec, 2018 г.).

публикуван доклад относно мониторинга. Към 2019 г. има 46 държави — страни по Конвенцията, включително Тунис — първата държава, която не е членка на ЕС. Мониторинговият доклад ще се публикува през 2020 година.

Допълнителни насоки на Съвета на Европа

Допълнителни стандарти и инструменти на Съвета на Европа допринасят за колективните достижения на правото на ЕС/ acquis за всеобхватна рамка, насочена към всички заинтересовани страни. Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство съдържа задължения за страните да криминализират редица престъпления, свързани с материали, съдържащи сексуално насилие над деца: понастоящем тя е ратифицирана от 64 държави — страни по конвенцията. Съветът на Европа се съсредоточава, наред с другото, върху предоставянето на възможности на децата и хората около тях да се ориентират безопасно в цифровата сфера. Това се насърчава чрез образователни инструменти, включително изцяло преразгледан Наръчник за грамотност в Интернет (2017 г.), Наръчник за образование по цифрово гражданство (2019 г.) и наръчници, насочени към родителите (родител в ерата на цифровите технологии — Родителски насоки за онлайн защита на децата от сексуална експлоатация и сексуално насилие (2017 г.); Цифровото гражданство и вашето дете — Какво трябва да знае и прави всеки родител (2019 г.). И накрая, Съветът на Европа предприе консултативни изследвания с деца във връзка с техните права в цифровата среда — това е нашият свят: Мнението на децата за това как да защитят правата си в цифровата среда (2017 г.) и проведе някои от първите консултативни изследвания, насочени към опита на децата с увреждания в цифровата среда — две кликвания напред и едно кликване назад: Доклад относно децата с увреждания в цифровата среда (2019 г.).

Детски онлайн доклад за безопасност

Безопасност на децата онлайн: Свеждане до минимум на риска от насилие, злоупотреба и експлоатация онлайн + Всеобща декларация за безопасност на децата онлайн[53].

Препоръки на ОИСР относно защитата на децата онлайн (2012/Преглед 2019—2020 г.)

Други национални и транснационални инициативи следва да бъдат допълнително подчертани като подкрепа за международното сътрудничество, както и за националните усилия за създаване на стратегии за онлайн защита на децата. Това са например:

Международната база данни за изображения на сексуална експлоатация на деца

Управлявана от Интерпол, Международната база данни за изображения на сексуална експлоатация на деца (ICSE DB) е мощен инструмент за разузнаване и разследване, който позволява на специализираните следователи да споделят данни с колеги от цял свят. На разположение чрез защитената глобална комуникационна система на Интерпол (известна като I-247), ICSE DB използва усъвършенстван софтуер за сравняване на изображения, за да установи връзки между жертви, насилници и места.

[53] Broadband Commission for Sustainable Development (2019), The State of Broadband 2019: Broadband as a Foundation for Sustainable Development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

ICSE DB дава възможност на сертифицирани потребители в държавите членки да имат достъп до базата данни в реално време — да разпитват съществуващите стопански субекти, да качват нови данни, да сортират материали, да намаляват риска от конфликти, да извършват анализ и да общуват с други експерти по света в отговор на запитвания, свързани с разследвания на сексуална експлоатация на деца.

Световният алианс WePROTECT

Световният алианс WePROTECT (WPGA) е глобално движение, което обединява влиянието, експертния опит и ресурсите, необходими за трансформиране на начина, по който онлайн сексуалната експлоатация на деца (OSCE) се третира в световен мащаб. Това е партньорство между правителства, световни технологични компании и организации на гражданското общество. Характерът му с участието на множество заинтересовани страни (multi-stakeholder) е уникален в тази област. Визията на WePROTECT Global Alliance е да се идентифицират и защитят повече жертви, да се задържат повече извършители и да се сложи край на сексуалната експлоатация на деца онлайн.

Световният алианс WeProtect се състои от редица компоненти, по-специално модел на национален отговор и глобален стратегически отговор. Допълнителна информация може да бъде намерена в Приложение 3.

Индексът за онлайн безопасност на децата за 2020 г.

DQ Institute 2020 Child Online Safety Index (COSI) е първата в света аналитична платформа в реално време, която помага на нациите да наблюдават по-добре статуса на онлайн безопасността на децата си.

COSI се основава на шест стълба, които формират рамката на COSI. Стълбове едно и две — киберриск и дисциплинирано цифрово използване — са свързани с разумното използване на цифровите технологии. Стълбове три и четири, „Цифрова компетентност“ и „Ориентиране и образование“, са свързани с овластяването. Последните два стълба са свързани с инфраструктурата, това са стълбовете на социалната инфраструктура и свързаността.

3.3 Примери за отговори на онлайн вреди

В Приложение 4 има редица примери за отговори/реагиране на онлайн вреди. Тези примери обхващат образователни отговори, законодателни актове и идентифициране на онлайн вредите.

3.4 Ползи от националните стратегии за защита на децата онлайн

Хармонизиране на законодателствата

Приемането от всички държави на подходящо законодателство срещу злоупотребата с ИКТ за престъпни или други цели е от основно значение за постигането на глобална киберсигурност. Тъй като заплахите могат да възникнат навсякъде по света, предизвикателствата по своята същност са международни по обхват и изискват международно сътрудничество, помощ при разследването и общи материалноправни и процедурни разпоредби. Поради това е важно държавите да хармонизират своите правни

рамки за борба с киберпрестъпността, защита на децата онлайн и улесняване на международното сътрудничество[54].

Разработването на подходящо национално законодателство, свързаната с нея правна рамка в областта на киберпрестъпността и в рамките на този подход хармонизирането на международно равнище е ключова стъпка към успеха на всяка национална стратегия за защита на децата онлайн. Това изисква преди всичко необходимите материалноправни наказателноправни разпоредби за инкриминиране на действия като компютърни измами, незаконен достъп, намеса в данните, нарушения на авторските права и CSAM, като същевременно се внимава децата да не бъдат неправомерно инкриминирани. Фактът, че в Наказателния кодекс съществуват разпоредби, приложими към подобни деяния, извършени в реалния свят, не означава, че те могат да се прилагат и за деяния, извършени по Интернет. Поради това задълбоченият анализ на действащото национално законодателство е от съществено значение за установяването на евентуални пропуски. Следващата стъпка ще бъде да се набележат и определят законодателният език и справочните материали, които могат да помогнат на държавите при установяването на хармонизирани закони и процедурни правила в областта на киберпрестъпността. Такива практически инструменти могат да бъдат използвани от държавите за разработването на правна рамка в областта на киберсигурността и свързаните с нея закони. Международният съюз за далекосъобщения работи с държавите членки и съответните заинтересовани страни в тази насока и допринася значително за напредъка в хармонизирането на законодателството в областта на киберпрестъпността в световен мащаб.

Като се има предвид бързият темп на технологичните иновации, саморегулирането и съвместното регулиране бяха предложени като потенциални решения на остаряването на съществуващото регулиране и на продължителния законодателен процес. Въпреки това, за да бъдат ефективни, регулаторните органи/създателите на политики трябва ясно да дефинират определени онлайн цели и предизвикателства в областта на защитата на детето, да въведат ясен процес на преглед и методика за оценка на ефикасността на саморегулирането и съвместното регулиране, а в случай че саморегулирането и съвместното регулиране не успеят да отговорят на установените предизвикателства — да инициират официален законодателен процес за справяне с тези предизвикателства. Освен това успешните мерки за саморегулиране биха могли постепенно да бъдат приети във формален закон в рамките на законодателния процес, за да се превърнат в правен предпазен механизъм и да предотвратят отмяната или прекратяването на присъединяването към определени инициативи за саморегулиране.

Координация

Вероятно е, сред различните участници и заинтересовани страни, вече да има редица съществуващи действия с цел защита на децата онлайн, но те са извършени изолирано. Разбирането им е важно за оценяването на съществуващите усилия в

[54] Комисия за широколентов достъп за устойчиво развитие (2019 г.)

разработването на националната стратегия за защита на децата онлайн. Стратегията ще координира и насочва усилията чрез организирането както на съществуващи, така и на нови дейности.

4. Препоръки за рамкиране и изпълнение

Правителствата трябва да обърнат внимание на всички прояви на насилие срещу деца в цифровата среда. Въпреки това мерките, предприети за защита на децата в цифровата среда, не следва да ограничават неоснователно упражняването на други права, като правото на свобода на изразяване на мнение, правото на достъп до информация или правото на свобода на сдружаване. Вместо да се ограничават естественото любопитство и усещането за иновации на децата поради страх да не се сблъскат с рискове онлайн, от решаващо значение е да се използва находчивостта на децата и да се повишава тяхната устойчивост, като същевременно се проучва потенциалът на цифровата среда.

В много случаи актове на насилие срещу деца се извършват от други деца. В такива ситуации правителствата следва, доколкото е възможно, да прилагат възстановителни подходи за отстраняване на нанесените вреди, като същевременно предотвратяват инкриминирането на децата. Правителствата следва да насърчават използването на ИКТ за предотвратяване и справяне с насилието, като например разработването на технологии и ресурси за достъп на децата до информация, блокиране на вредни материали и докладване на случаи на насилие, когато те възникнат[55].

За да се справят с глобалната ситуация по отношение на безопасността на децата онлайн, правителствата трябва да улеснят комуникацията между съответните субекти и открито да си сътрудничат, за да премахнат вредите за децата онлайн.

4.1 Рамкови препоръки

4.1.1 Правна рамка

Правителствата следва да преразгледат и, когато е необходимо, да актуализират своята правна рамка, за да подкрепят пълното упражняване на правата на детето в цифровата среда. Една всеобхватна правна рамка следва да обхваща превантивните мерки; забрана на всички форми на насилие срещу деца в цифровата среда; предоставяне на ефективни средства за правна защита, възстановяване и реинтеграция за справяне с нарушенията на правата на децата; организиране на съобразени с интересите на децата консултации, механизми за докладване и подаване на жалби и механизми за отчетност за борба с безнаказаността[56].

[55] Специален представител на генералния секретар по въпросите на насилието срещу деца, *годишен доклад на специалния представител на генералния секретар относно насилието срещу деца пред Съвета по правата на човека,* A/HRC/31/20 (януари 2016 г.), точки 103 и 104.

[56] Специален представител на генералния секретар по въпросите на насилието срещу деца, *освобождаването на потенциала на децата и свеждането до минимум на рисковете: ИКТ, Интернет и насилието срещу деца,* 2014 г. (Ню Йорк: ООН), стр. 55.

Когато е възможно, законодателството следва да бъде технологично неутрално, така че неговата приложимост да не бъде подкопана от бъдещото технологично развитие[57].

Ефективното прилагане на законодателството изисква правителствата да въведат допълнителни мерки, включително инициативи за повишаване на осведомеността и социална мобилизация, образователни усилия и кампании, както и изграждане на капацитет на специалистите, работещи с и за деца.

При разработването на подходящо законодателство е важно също така да се има предвид, че децата не са хомогенна група. Може да са необходими различни отговори за деца от различни възрастови групи, както и за деца, които имат специфични нужди или които са изложени на повишен риск от увреждане във или чрез цифровата среда.

Правителствата следва да създадат ясна и предвидима правна и регулаторна среда, която да подпомага предприятията и други трети страни да изпълняват задълженията си за защита на правата на децата по време на своята дейност в страната и в чужбина[58].

Следните аспекти ще бъдат от полза за създателите на политики при прегледа на обхвата на всяка правна рамка и осигуряване на следното:

- сприятеляване с цел сексуална злоупотреба или други форми на дистанционно съблазняване, изнудване или принуда на деца за неподходящ сексуален контакт или сексуална активност;
- гарантиране на притежаването, производството и разпространението на CSAM, независимо от намерението за разпространение;
- тормоз, злоупотреба или изказвания, подбуждащи към омраза онлайн;
- онлайн терористични материали;
- киберсигурността;
- отчитане, че това, което е незаконно офлайн, е също толкова незаконно онлайн.

4.1.2 Политически и институционални рамки

Гарантирането на упражняването на правата на децата в цифровата среда изисква правителствата да постигнат баланс между максималното увеличаване на ползите от използването на ИКТ от децата и свеждането до минимум на рисковете, свързани с тях. Това може да бъде постигнато чрез включване на мерки за защита на децата онлайн в националните планове за широколентов достъп [59] и чрез разработване на отделна многостранна/multifaceted стратегия за защита на децата онлайн. Тази програма следва

[57] Специален представител на генералния секретар по въпросите на насилието срещу деца, *освобождаването на потенциала на децата и свеждането до минимум на рисковете: ИКТ, Интернет и насилието срещу деца,* 2014 г. (Ню Йорк: ООН), стр. 64.
[58] Комитет на ООН по правата на детето, *Общ коментар № 16*, параграф 53.
[59] Състоянието на широколентовия достъп през 2019 г., Препоръка 5.6, стр. 78. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

да бъде напълно интегрирана с всички съществуващи рамки на политиката, свързани с правата на децата или защитата на детето, и освен това следва да допълва националните политики за защита на детето, като предлага специфична рамка за всички рискове и потенциални вреди за децата, насочена към създаване на безопасна, приобщаваща и предоставяща възможности цифрова среда[60].

Правителствата следва да въведат национална координационна рамка с ясен мандат и достатъчно правомощия за координиране на всички дейности, свързани с правата на децата и цифровите медии и ИКТ на междусекторно, национално, регионално и местно равнище. Правителствата следва да включват обвързани със срокове цели и прозрачен процес за оценка и наблюдение на напредъка, и да гарантират, че необходимите човешки, технически и финансови ресурси са на разположение за ефективното функциониране на тази рамка[61].

Правителствата следва да създадат многостранна платформа, която да направлява разработването, изпълнението и наблюдението на националната програма в областта на цифровите технологии за децата. Тази платформа следва да обединява представители на най-важните конституенти, включително: деца и младежи; сдружения на родители/настойници/полагащи грижи; съответните органи на управление; секторите на образованието, правосъдието, здравеопазването и социалните грижи; националните институции за правата на човека и съответните регулаторни органи; гражданското общество; промишлеността; академичните среди; и съответните професионални сдружения.

4.1.3 Регулаторна рамка

Правителствата носят отговорност за нарушения на правата на децата, причинени или подпомогнати от стопански предприятия когато не са предприели необходимите, подходящи и разумни мерки за предотвратяване и отстраняване на такива нарушения или са сътрудничили, или толерирали по друг начин нарушенията[62].

Ръководните принципи за бизнеса и човешките права предвиждат, че корпорациите следва да предоставят коригиращи механизми и такива за обжалване, които са законни, достъпни, предвидими, справедливи, съвместими с правата, прозрачни, основани на диалог и ангажираност, както и източник на непрекъснато обучение. Механизмите за подаване на жалби, установени от стопанските предприятия, могат да предоставят гъвкави и своевременни алтернативни решения в най-добрия интерес на детето за опасенията, изразени във връзка с поведението на компанията, да бъдат разрешени чрез тях. Във всички случаи следва да има достъп до правосъдие или

[60] За примерни разпоредби относно закрилата на децата за националните широколентови планове вж. глава 10 от Доклада за безопасността на децата онлайн. For model provisions on child protection for national broadband plans see chapter 10 of the Child Online Safety Report.

[61] Специален представител на генералния секретар по въпросите на насилието срещу деца, *годишен доклад на специалния представител на генералния секретар относно насилието срещу деца (декември 2014 г.*) A/HRC/28/55 и освобождаване на потенциала на *децата и свеждане до минимум на рисковете: ИКТ, Интернет и насилието срещу деца,* 2014 г. (Ню Йорк: Организация на обединените нации), параграф 88.

[62] Комитет на ООН по правата на детето, *Общ коментар № 16*, параграф 28.

съдебен контрол на административните средства за защита и други процедури[63]. Следва да се обърне внимание на механизми, които създават безопасни, съобразени с възрастта услуги за децата, за да могат потребителите да докладват своите опасения.

Независимо от наличието на вътрешни механизми за подаване на жалби, правителствата следва да създадат механизми за наблюдение за разследване и правна защита на нарушенията на правата на децата, с цел да се подобри отчетността на ИКТ и други съответни компании, както и да се засили отговорността на регулаторните агенции за разработването на стандарти, свързани с правата на децата и ИКТ[64]. Това е особено важно, тъй като другите средства за правна защита, с които разполагат неблагоприятно засегнатите от корпоративните искове, като например гражданските производства и други средства за съдебна защита, често са тромави и скъпи[65].

Комитетът на ООН по правата на детето подчерта потенциалната роля на националните институции за правата на човека в тази област, като очерта как те биха могли да получат, разследват и посредничат при жалби за нарушения от страна на промишлени субекти; провеждане на публични разследвания на широкомащабни злоупотреби; и предприемане на законодателни прегледи, за да се гарантира спазването на Конвенцията за правата на детето. Комитетът посочи, че при необходимост „държавите следва да разширят законодателния мандат на националните институции за защита на правата на човека, за да се вземат предвид правата на децата и стопанската дейност“. Особено важно е всеки механизъм за подаване на жалби да бъде чувствителен към децата, да гарантира неприкосновеността на личния живот и защитата на жертвите и да предприема мониторинг, последващи действия и дейности за проверка на децата жертви.

Пример за област, в която национална институция по правата на човека или друг регулаторен орган биха могли да предоставят ефективни правни средства за защита на децата, е в случаите на кибертормоз. Вътрешните механизми за корекции и подаване на жалби понякога се оказват неефективни в такива случаи, тъй като, въпреки че съдържанието е обезпокоително и вредно, то често не се разглежда от националното законодателство и няма ясна основа за търсене на премахването му от хоста на съдържание. Предоставянето на правомощия на публичен орган да получава жалби във връзка със случаи на кибертормоз и да се застъпва пред приемниците на съдържание за премахване на съответния материал би било важна гаранция за децата[66]. Тя би имала предимствата на бързото реагиране, което е от решаващо значение в контекста на кибертормоза, както и на ясна правна основа за справяне с премахването на материали за кибертормоза.

[63] Доклад на специалния представител на генералния секретар по въпроса за правата на човека и транснационалните корпорации и други стопански предприятия, A/HRC/17/31 (2011), точка 71.
[64] Комитет на ООН по правата на детето, *Доклад от Деня на общото обсъждане през 2014 г.*, параграф 96.
[65] Доклад на специалния докладчик относно насърчаването и защитата на правото на свобода на мнение и изразяване, A/HRC/32/38 (2016), точка 71.
[66] Bertrand de Crombrugghe, “Report of the Human Rights Council on Its Thirty-First Session” (UN Human Rights Council, 2016).

При формулирането на подхода си към регулирането на цифровата среда правителствата трябва да се запознаят с въздействието на това регулиране върху упражняването на всички права на човека, включително свободата на изразяване[67].

Правителствата следва да задължат бизнеса да извършва надлежна проверка за спазване на правата на детето. Това ще гарантира, че стопанските предприятия идентифицират, предотвратяват и смекчават/ограничават въздействието си върху правата на децата, включително във всички свои делови взаимоотношения и в рамките на глобалните операции[68].

Освен това правителствата следва да обмислят допълнителни мерки, като например гарантиране, че промишлените субекти, чиито дейности могат да окажат въздействие върху правата на децата в цифровата среда, трябва да спазват най-високите стандарти по отношение на предотвратяването и реагирането на потенциални нарушения на правата, за да отговарят на условията за финансиране или договори.

4.2 Препоръки за изпълнение

Правителствата следва да осигурят достъп до ефективни средства за правна защита за децата жертви на нарушения на правата им, включително помощ за търсене на бързо и подходящо обезщетение за претърпените вреди, чрез компенсация, когато е целесъобразно. Правителствата следва също така да предоставят подходяща подкрепа и помощ за децата жертви на нарушения, свързани с цифровите медии и ИКТ, включително всеобхватни услуги, за да се гарантира пълното възстановяване и реинтеграция на детето и да се предотврати повторното виктимизиране на децата жертви[69].

Безопасните и леснодостъпни чувствителни за децата механизми за консултиране, докладване и подаване на жалби, като например телефонни линии за помощ, следва да бъдат установени със закон и да са част от националната система за защита на детето. Важно е да се гарантира, че тези услуги са свързани с всички регулаторни услуги, за да се спомогне за рационализиране на взаимодействието на детето с институционалните органи във време, когато то може да изпитва затруднения. Линиите за помощ са особено ценни по отношение на изключително чувствителни въпроси, като например сексуалното насилие, които децата трудно могат да обсъдят с връстници, родители, полагащи грижи лица или учители. Линиите за помощ също играят решаваща роля за насочването на децата към услуги като правни услуги, безопасни домове, правоприлагане или рехабилитация[70].

Освен това правителствата трябва да разбират и проследяват поведението на нарушителите, за да увеличат процента на разкритията на извършителите на

[67] Доклад на специалния докладчик относно насърчаването и защитата на правото на свобода на мнение и изразяване, A/HRC/32/38 (2016 г.), параграф 45.
[68] Комитет на ООН по правата на детето, *Общ коментар № 16*, параграф 62.
[69] Комитет на ООН по правата на детето, *Доклад от Деня на общото обсъждане през 2014 г.*, параграф 106.
[70] Специален представител на генералния секретар по въпросите на насилието срещу деца, освобождаването на *потенциала на децата и свеждането до минимум на рисковете*, стр. 51 и стр. 65.

злоупотреби и да намалят риска от повторно извършване на престъпления от осъдени насилници, да създават линии за помощ/горещи линии, предлагащи безплатни и анонимни телефонни или чат-базирани консултации и подкрепа за хора, които изпитват чувства или мисли за сексуален интерес към деца — потенциални нарушители. Оказването на помощ на нарушителите да променят поведението си свежда до минимум риска от повторно извършване на престъпление.

Законоустановените механизми за разглеждане на жалби също представляват съществена част от рамката за ефективни правни средства за защита.

Регулаторните органи следва да извършват независими измервания и проучвания, за да оценят как платформите докладват и разглеждат въпроси, свързани със защитата на детето. Съществува технология за независимо наблюдение на платформите от регулаторните органи. Доставчиците от промишления сектор следва да бъдат подкрепяни да публикуват доклади за прозрачност.

Заедно с международната общност и промишлеността правителствата следва да разработят универсален набор от показатели, които заинтересованите страни могат да използват за измерване на всички съответни аспекти на безопасността на децата онлайн.

4.2.1 Сексуална експлоатация

Конкретни съображения за създателите на политики, когато разглеждат заплахите за децата от вреди, по-специално материали, съдържащи сексуално насилие над деца, самостоятелно създадено съдържание, сприятеляване с цел сексуална злоупотреба и изнудване, и други онлайн рискове, могат да включват:

- Стъпки за прекъсване или намаляване на трафика в CSAM, например чрез създаване на национална гореща линия или портал за докладване на IWF чрез въвеждане на мерки, които ще блокират достъпа до онлайн съдържание, за което е известно, че съдържа или рекламира наличността на CSAM.
- Гарантиране, че са въведени национални процеси, за да е сигурно, че всички открити в дадена държава CSAM се насочват към централизиран национален ресурс, който има законодателни правомощия да насочва компаниите към премахване на съдържание.
- Стратегии за справяне с търсенето на CSAM, по-специално сред лицата, които имат присъди за такива престъпления. Важно е да се повиши осведомеността за факта, че това не е престъпление без жертви: с деца се злоупотребява, за да се произведат материалите, които се разглеждат, а чрез умишлено гледане или изтегляне на CSAM се допринася пряко за малтретирането на изобразеното дете и също така насърчава малтретирането на повече деца с цел създаване на повече снимки.
- Повишаване на осведомеността за факта, че децата никога не могат да дадат съгласието си за сексуално насилие, било то за производството на CSAM или по друг начин. Насърчаване на хората, които използват CSAM, да потърсят помощ, като в същото време ги осведомяват, че ще бъдат подведени под наказателна отговорност за незаконната дейност, в която са ангажирани/ангажирали.

- Други стратегии за справяне с търсенето на CSAM. Например някои държави поддържат регистър на осъдените извършители на сексуални престъпления. Съдилищата са издали съдебни заповеди, с които се забранява на такива нарушители да използват Интернет изцяло или да използват части от Интернет, посещавани от деца и младежи. Проблемът с тези заповеди досега е бил в изпълнението. В някои държави обаче се обмисля включването на списъка на известните извършители на сексуални престъпления в блок списък, който ще попречи на лицата в него да посещават или да се присъединяват към определени уебсайтове, например уебсайтове, за които е известно, че са посещавани от голям брой деца и младежи. Разбира се, ако извършителят се присъедини към уебсайт, като използва различно име или фалшиво влизане, ефикасността на тези мерки може да бъде значително намалена, но чрез инкриминиране на това поведение може да бъде установено допълнително възпиращо действие.
- Предоставяне на подходяща дългосрочна подкрепа за жертвите. Когато деца или млади хора са били жертви онлайн, където например в Интернет се е появил незаконен техен образ, те естествено ще се чувстват много загрижени за това кой може да го е видял и какво въздействие ще има това върху тях. Това би могло да накара детето или младия човек да се чувства уязвим на тормоз или на по-нататъшна сексуална експлоатация и малтретиране. В този контекст ще бъде важно да има на разположение услуги за професионална помощ в подкрепа на децата и младите хора, които се намират при тези обстоятелства. Може да се наложи такава подкрепа да се предоставя в дългосрочен план.
- Гарантиране, че е създаден и широко насърчаван механизъм за предоставяне на лесноразбираеми и бързи средства за докладване на незаконно съдържание или незаконно или тревожно онлайн поведение, например система, подобна на тази, създадена от виртуалната глобална работна група и INHOPE. Следва да се насърчава използването на системата на Интерпол i24/7.
- Гарантиране, че достатъчен брой служители на правоприлагащите органи са подходящо обучени в разследването на Интернет и компютърните престъпления и имат достъп до подходящи структури за криминалистика, за да им се даде възможност да извличат и тълкуват съответните цифрови данни.
- Инвестиране в обучение за правоприлагащите, прокурорските и съдебните органи относно методите, използвани от престъпниците онлайн за извършване на тези престъпления. Ще бъдат необходими инвестиции и за придобиването и поддържането на съоръженията, необходими за получаване и тълкуване на доказателства в областта на криминалистиката от цифрови устройства. Освен това ще бъде важно да се установи двустранно и многостранно сътрудничество и обмен на информация със съответните правоприлагащи органи и разследващи органи в други държави.

4.2.2 Образование

Образовайте децата по отношение на цифровата грамотност като част от стратегия, за да се гарантира, че те могат да се възползват от технологиите, без да бъдат нанасяни вреди. Това ще позволи на децата да развият умения за критично мислене, които ще им помогнат да идентифицират и разберат добрите и лошите страни на своето поведение в цифровото пространство. Въпреки че е важно да се илюстрират на децата вредите, които могат да възникнат онлайн, това ще бъде ефективно само ако бъде включено в по-широка програма за цифрова грамотност, която следва да бъде съобразена с възрастта и да се съсредоточи върху уменията и компетентностите. Важно е да се включат концепции за социално и емоционално обучение в онлайн образованието по безопасност, тъй като те ще помогнат на учениците да разбират и управляват емоциите, за да имат здравословни и уважителни отношения, както онлайн, така и офлайн.

Децата следва да разполагат с подходящи инструменти и знанието за справяне с Интернет е един от най-добрите начини за тяхната безопасност. Въвеждането на цифрова грамотност в учебните програми е един от начините. Друга възможност е да се създадат образователни ресурси извън учебната програма.

Работещите с деца следва да притежават подходящи знания и умения, за да могат уверено да подкрепят децата както при реагирането, така и при решаването на проблеми, свързани със защитата на децата онлайн, както и да предоставят на децата необходимите цифрови умения, за да могат успешно да се възползват от технологиите.

4.2.3 Промишленост

Участниците на национално и международно равнище следва да работят за повишаване на осведомеността по въпросите, свързани с безопасността на децата онлайн, и да помагат на всички възрастни, отговорни за благосъстоянието на детето, включително родителите и лицата, полагащи грижи, училищата, младежките организации и общности, да развият знанията и уменията, от които се нуждаят, за да опазят децата. Промишлеността следва да възприеме по-безопасен още при проектирането подход към своите продукти, услуги и платформи, като отчита безопасността като основна цел.

- Да предоставят подходящи за възрастта инструменти, съобразени със семейството, за да помогнат на своите потребители да управляват по-добре защитата на семействата си онлайн.
- Да предоставят подходящи механизми за докладване, за да могат техните потребители да докладват за проблеми и опасения. Потребителите следва да очакват своевременни отговори на тези доклади с информация за предприетите действия и, ако е приложимо, къде потребителите могат да получат допълнителна подкрепа.
- Да се осигурява проактивно докладване за малтретиране на деца с цел откриване и справяне с всякакъв вид малтретиране (класифицирано като престъпна

дейност) срещу деца. Тази практика показа, че ако всички заинтересовани страни допринасят за откриването, блокирането и докладването, можем да помислим за по-чист и по-безопасен Интернет за всички. Промишлеността следва да обмисли използването на всички съответни инструменти, за да предотврати използването на техните платформи, като например IWF Services.

От жизненоважно значение е всички съответни участници в екосистемата да бъдат запознати с онлайн рисковете и вредите, за да не могат децата да бъдат изложени на ненужни рискове.

Разработвайте общи показатели за безопасността на децата онлайн, за да се измерят всички съответни аспекти на проблема. Общите стандарти и показатели са единственият начин за проследяване на напредъка в държавите и за определяне на успеха на проектите и дейностите, изпълнявани за премахване на всяко насилие срещу деца и признаване на силата на екосистемата за безопасност на децата онлайн.

5. Разработване на национална стратегия за защита на децата онлайн

5.1 Национален контролен списък

За да формулират национална стратегия, съсредоточена върху безопасността на децата онлайн, създателите на политики трябва да обмислят набор от стратегии. В таблица 1 са посочени основните области, които трябва да бъдат разгледани.

Таблица 1: Ключови области за разглеждане

	#	Ключови области за разглеждане	Допълнителни подробности
Правна рамка	1	Преглед на съществуващата правна рамка, за да се определи, че са налице всички необходими законови правомощия, за да се даде възможност на правоприлагащите органи и на други съответни институции да защитават лицата на възраст под 18 години онлайн на всички платформи, използващи Интернет.	Като цяло ще бъде необходимо да има набор от закони, които ясно да показват, че всяко престъпление, което може да бъде извършено срещу дете в реалния свят, може, *mutatis mutandis*, да бъде извършено и в Интернет или в друга електронна мрежа. Може също така да е необходимо да се разработят нови закони или да се адаптират съществуващите закони, за да се забранят определени видове поведение, които могат да се извършват само в Интернет, например дистанционното примамване на деца да извършват или гледат сексуални действия, или да се сприятеляват с деца, за да се срещат в реалния свят със сексуална цел. В допълнение към тези цели по принцип ще бъде необходимо да има правна рамка, която
	2	Да се установи, *mutatis mutandis*, че всяко действие срещу дете, което е незаконно в реалния свят, е незаконно онлайн и че правилата за защита на данните онлайн и неприкосновеността на личния живот на децата също са адекватни.	

			забранява злоупотребата с компютри за престъпни цели, забранява хакерството или друго злонамерено или несъзнателно използване на компютърен код и установява, че Интернет е място, в което могат да бъдат извършени престъпления.
Регулаторна рамка	3	Обмисляне на разработването на регулаторна политика. Това може да включва разработване на политика за саморегулиране или съвместно регулиране, както и пълна регулаторна рамка. Моделът за саморегулиране или съвместно регулиране може да включва формулирането и публикуването на кодекси за добри практики или основни онлайн очаквания за безопасност, както по отношение на оказването на помощ за ангажиране, координиране или организиране и поддържане на участието на всички съответни заинтересовани страни, така и по отношение на ускоряването на разработването и прилагането на подходящи отговори на технологичните промени.	Някои държави са създали модел за саморегулиране или съвместно регулиране във връзка с разработването на политика в тази област и чрез такива модели например са публикували кодекси за добри практики, които да насочват Интернет индустрията по отношение на мерките, които могат да работят най-добре, когато става въпрос за осигуряване на безопасността на децата и младите хора онлайн. Например в рамките на Европейския съюз, където са публикувани кодекси за целия ЕС както за сайтове за социални мрежи, така и за мобилни телефонни мрежи във връзка с предоставянето на съдържание и услуги на деца и млади хора чрез техните мрежи. Саморегулирането и съвместното регулиране могат да бъдат по-гъвкави по отношение на увеличаването на скоростта, с която могат да се формулират и приложат подходящи отговори на технологичните промени.

		Един регулаторен модел може да определи очакванията и задълженията на заинтересованите страни и да се впише в правен контекст. Могат да бъдат взети предвид и санкции за нарушения на политиката.	Неотдавна няколко държави разработиха и/или въведоха регулаторна рамка. В тези примери регулаторната рамка произтича от собствени или съвместни регулаторни модели и определя изискванията и очакванията на заинтересованите страни, по-специално на доставчиците от отрасъла, за по-добра защита на техните потребители.
Докладване на незаконно съдържание	4	Да гарантира, че е създаден и широко насърчаван механизъм за предоставяне на лесноразбираеми средства за докладване на разнообразието от незаконно съдържание, намиращо се в Интернет. Например национална гореща линия, която дава възможност да се реагира бързо и незаконните материали да бъдат отстранени или да станат недостъпни. Промишлеността следва да разполага с механизми за идентифициране, блокиране и премахване на малтретирането на деца онлайн, като се ползват всички услуги, които са от значение за техните организации.	Механизмите за докладване на злоупотреба с онлайн услуга или за съобщаване на неприемливо или незаконно поведение онлайн, например на национална гореща линия, следва да бъдат широко рекламирани и популяризирани както в Интернет, така и в други медии. Ако няма национална гореща линия, IWF предлага решението на порталите за докладване. Връзките за докладване на механизми за злоупотреба следва да се показват на видно място в съответните части на всеки уебсайт, който позволява да се появи генерирано от потребителите съдържание. Следва също така да е възможно хората, които се чувстват застрашени по някакъв начин, или хората, които са станали свидетели на тревожна дейност в Интернет, да могат да докладват за това възможно най-бързо на съответните правоприлагащи органи, които

			трябва да бъдат обучени и готови да реагират. Виртуалната глобална работна група е правоприлагащ орган, който предоставя 24/7 механизъм за получаване на доклади за незаконно поведение или съдържание от лица в САЩ, Канада, Австралия и Италия, като други страни се очаква да се присъединят скоро. Вж. www.virtualglobaltaskforce.com. Вж. също INHOPE.
Докладване на опасения на потребителите	5	Промишлеността следва да предоставя на потребителите възможност да докладват за опасения и проблеми на своите потребители и да реагират по съответния начин.	Доставчиците следва да бъдат задължени да предоставят и ясно да указват на своите потребители възможността да докладват за проблеми и опасения в рамките на своите услуги. Те трябва да са подходящи за деца и леснодостъпни.
Участници и заинтересовани страни	6	Ангажиране на всички съответни заинтересовани страни, които имат интерес към защитата на децата онлайн, и по-специално: • Държавни агенции • Правоприлагане • Организации за социални услуги • Доставчици на Интернет услуги (ДИУ) и други доставчици на електронни услуги (ЕПУ) • Доставчици на мобилни телефонни мрежи	Няколко национални правителства сметнаха за полезно да обединят всички основни заинтересовани страни и участници, за да се съсредоточат върху разработването и осъществяването на национална инициатива за превръщането на Интернет в по-безопасно място за децата и младите хора и повишаването на осведомеността по въпросите и начините за справяне с тях по много практичен начин. В рамките на тази стратегия ще бъде важно да се оцени, че много от тях са универсално и

		• Обществени доставчици на Wi-Fi • Други съответни високотехнологични компании • Организации на преподавателите • Родителски организации • Деца и младежи • Защита на детето и други съответни НПО • Академична и научноизследователска общност • Собственици на Интернет кафенета и други доставчици на публичен достъп, например библиотеки, телецентрове, PC Bangs [71] и онлайн игрални центрове и т.н.	постоянно свързани с Интернет чрез различни устройства. Необходимо е да участват операторите на широколентови, мобилни и безжични мрежи. Освен това в много страни мрежата от обществени библиотеки, телецентрове и Интернет кафенета може да бъде важен източник на достъп до Интернет, особено за децата и младите хора.
Изследвания	7	Да се предприеме проучване на спектъра от национални участници и заинтересовани страни, за да се определят техните мнения, опит, тревоги и възможности по отношение на защитата на децата онлайн и да се оцени степента на всяка отговорност, заедно със съществуващите или планираните дейности за защита на децата онлайн.	

[71] „PC Bang“ е термин, който обикновено се използва в Република Корея и в някои други страни, за да опише голяма стая, където LAN улеснява широкомащабната игра онлайн или между играчите в стаята.

Образование цифрова грамотност и компетентност	8	Разработване на характеристики за цифрова грамотност като част от всяка национална училищна програма, която е подходяща и приложима за всички деца.	Училищата и образователната система като цяло ще представляват основата на компонента за образование и цифрова грамотност на националната стратегия за защита на децата онлайн. Всяка национална училищна програма следва да включва аспекти, свързани със защитата на децата онлайн, и да има за цел да предостави на децата от всички възрасти подходящи за възрастта умения как успешно да използват технологиите, както и да са чувствителни към заплахите и вредите, за да бъдат успешно избегнати. Тя следва да признава и възнаграждава положителното и конструктивно онлайн поведение. В рамките на всяка образователна и осведомителна кампания ще бъде важно да се постигне правилният тон. Съобщенията, основани на страх, следва да се избягват и да се отдава дължимото внимание на многото положителни и забавни характеристики на новата технология. Интернет има голям потенциал като средство за даване на възможност на децата и младите хора да откриват нови светове. Преподаването на положителни и отговорни форми на онлайн поведение е основна цел на образователните програми и програмите за повишаване на осведомеността.

			Тези, които работят с деца, особено учителите, следва да бъдат подходящо обучени и подготвени, за да могат успешно да образоват и да предоставят на децата тези умения. Те следва да разбират онлайн заплахите и вредите, както и да имат способността уверено да разпознават признаците на малтретиране и вреда и да реагират и докладват за тези опасения, за да защитят децата си.
Образователни ресурси	9	Възползване от знанията и опита на всички заинтересовани страни и разработване на послания и материали за безопасност в Интернет, които отразяват местните културни норми и закони, и гарантиране, че те се разпространяват ефективно и се представят по подходящ начин на всички ключови целеви аудитории. Да се обмисли възможността за включване на помощта на средствата за масово осведомяване за популяризиране на посланията за повишаване на осведомеността. Разработване на материали, които подчертават положителните и овластяващи аспекти на Интернет за децата и младите хора и избягват	При производството на образователни материали е важно да се има предвид, че много хора, които са нови в технологията, няма да се чувстват комфортно да я използват. Поради тази причина е важно да се гарантира, че материалите за безопасност се предоставят в писмена форма или се произвеждат с помощта на други носители, с които новодошлите ще се чувстват по-добре запознати, например с видео Много от големите Интернет компании произвеждат уебсайтове, които съдържат много информация за онлайн проблеми за деца и млади хора. Въпреки това, много често тези материали са достъпни само на английски език или на много тесен диапазон от езици. Поради това е много важно материалите да се произвеждат на местно равнище, да отразяват местните

		посланията, основани на страх. Насърчаване на положителни и отговорни форми на онлайн поведение. Да се обмисли разработването на ресурси, които да помогнат на родителите да оценят онлайн безопасността на собствените си деца и да се научат как да сведат до минимум рисковете и да увеличат максимално потенциала на собственото си семейство чрез целенасочено образование.	закони, както и местните културни норми. Това ще бъде от съществено значение за всяка кампания за безопасност в Интернет или за всякакви материали за обучение, които са разработени.
Защита децата	10	Да гарантира, че са въведени универсални и систематични механизми за защита на детето, които задължават всички, които работят с деца (социални грижи, здравеопазване, училища и т.н.), да идентифицират, реагират и докладват за случаи на малтретиране и вреда, които настъпват онлайн.	Следва да бъде въведена универсална система за защита на детето, която да се прилага за всички лица, работещи с деца, която да ги задължава да докладват за малтретиране или увреждане на деца, за да се даде възможност за разследване и разрешаване на ситуациите.
Национална осведоменост	11	Организиране на национални кампании за повишаване на осведомеността, за да се създаде възможност за всеобщо изтъкване на проблемите, свързани със защитата на децата онлайн. Може да е полезно да се използват глобални	Родителите, настойниците и специалистите, като например учителите, имат решаваща роля за това децата и младите хора да останат в по-безопасна онлайн среда. Следва да се разработят подкрепящи програми, които да спомогнат за повишаване на осведомеността по въпросите и

		кампании като Деня за по-безопасен Интернет, за да се организират и национални кампании.	да се осигурат стратегии за справяне с тях. Следва също така да се обмисли включването на помощта на средствата за масово осведомяване за популяризиране на посланията и кампаниите за повишаване на информираността. Възможности като Деня за по-безопасен Интернет ще бъдат полезни за стимулиране и насърчаване на национален диалог относно защитата на децата онлайн. Много държави успешно изградиха национални кампании за повишаване на осведомеността, основани на Деня за по-безопасен Интернет, и включиха пълния набор от участници и заинтересовани страни в разширяването на универсалните съобщения в медиите и социалните медии.
Инструменти, услуги и настройки	12	Обмислете ролята на настройките на устройствата, техническите инструменти (като програми за филтриране) и приложенията и настройките за защита на децата, които могат да помогнат. Насърчаване на потребителите да поемат отговорност за своите устройства, като извършват актуализации на операционната система, както и използването на	Има няколко услуги на разположение, които могат да помогнат за екраниране на нежелани материали или блокиране на нежелани контакти. Някои от тези програми за безопасност и филтриране на деца могат да бъдат по същество безплатни, защото са част от компютърна операционна система или се предоставят като част от пакет, достъпен от Интернет доставчик или ESP. Производителите на някои конзоли за игри също предоставят подобни инструменти, ако устройството

		подходящ софтуер и приложения за сигурност.	е включено в Интернет. Тези програми не са безупречни, но могат да осигурят желана подкрепа, особено в семейства с по-малки деца. По-голямата част от устройствата са снабдени с настройки, които помагат за защита на децата и също така насърчават здравословна и балансирана употреба. Това обхваща и механизми, които позволяват на родителите да управляват устройствата на децата си, като разпределят времето, приложенията и услугите, които могат да използват и управляват покупките. Наскоро бяха разработени материали и настройки, за да се даде възможност на потребителите и родителите по-добре да разбират и управляват времето и достъпа до екрана. Тези технически инструменти следва да се използват като част от по-широк арсенал. Участието на родителите и/или настойниците е от решаващо значение. Тъй като децата започват да стават малко помалко възрастни, те ще искат повече неприкосновеност на личния живот и също така ще почувстват силно желание да започнат да проучват сами. Освен това, когато съществува връзка на фактуриране между продавача и клиента, процесите на проверка на възрастта могат да играят много ценна роля за

			подпомагане на продавачите на стоки и услуги, които са ограничени по възраст, или на издателите на материали, предназначени само за публика на или над определена възраст, да достигнат до тези конкретни аудитории. Когато не съществува връзка с фактурирането, използването на технология за проверка на възрастта може да бъде проблематично или в много държави това може да е невъзможно поради липсата на надеждни източници на данни.

5.2 Примерни въпроси

С определянето на националните заинтересовани страни и участници, сред тях могат да бъдат разпространени следните въпроси, на които те да бъдат приканени да допълнят и отговорят. Техните отговори ще спомогнат за определяне на обхвата на политиката, силните страни и областите, върху които трябва да се съсредоточи вниманието в националния контролен списък.

- До каква степен безопасността онлайн и правата на децата са ваша отговорност?
- Как безопасността онлайн и правата на децата са интегрирани във вашите съществуващи политики и процеси?
- До каква степен безопасността онлайн е обхваната от съществуващото законодателство?
- Какви са вашите онлайн приоритети за безопасност?
- Какви дейности имате, за да подкрепите безопасността онлайн?
- Как работите с други агенции и организации за подобряване/напредък на безопасността онлайн?
- Могат ли деца/родители да ви докладват за опасения или проблеми с безопасността онлайн?
- Какви са трите ви ключови предизвикателства в онлайн света?
- Какви са трите ви ключови възможности в онлайн света?

Също така би било полезно да се предприемат изследвания и разбиране на възприятията и опита на децата, както и на техните родители по отношение на защитата на децата онлайн.

6. Справочен материал

Безопасност на децата онлайн: Основни документи и публикации

2020

- ECPAT International, Сексуална експлоатация на деца в Близкия изток и Северна Африка, 2020
- DQ InstMCДte, 2020 г. Доклад за безопасността на децата онлайн, 2020 г.
- EU Kids Online, EU Kids Online 2020: Резултати от проучването от 19 държави, 2020 г.

2019

- Фондация за наблюдение на Интернет (IWF), Годишен доклад, 2019 г.
- Световен алианс WePROTECT, Global Threat Assessment, 2019
- Широколентова комисия/МСД, Детска онлайн безопасност. Универсална декларация, 2019 г.
- Широколентова комисия/МСД, Детска безопасност онлайн: Свеждане до минимум на риска от насилие, злоупотреба и експлоатация онлайн, 2019 г.
- Global Kids Online, Израстване в свързан свят, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery in the Internet, in Proceedings of the 2019 World Wide Web Conference, 13—17, 2019, Сан Франциско, САЩ, 2019 г.
- Министерство на вътрешните работи на Обединеното кралство, Бяла книга за онлайн вредите (само за Обединеното кралство), 2019 г.
- PA Consulting, Заплетена мрежа: Rethinking the approach to online CSEA (Преосмисляне на подхода към онлайн CSEA), 2019 г.
- Служба на комисаря по информацията на Обединеното кралство, Консултация относно Кодекса за поведение за подпомагане на защитата на децата онлайн (само за Обединеното кралство), 2019 г.
- Глобален фонд за прекратяване на насилието срещу деца, нарушаване на вредите: доказателства за разбиране на сексуалната експлоатация и малтретирането на деца онлайн, 2019 г.
- Глобално партньорство за прекратяване на насилието над деца, безопасно да научите покана за действие, Младежки манифест, 2019 г.
- ЮНЕСКО, Зад цифрите: „Прекратяване на насилието и тормозав училищата“, 2019 г. (включва данни за обидно поведение онлайн и кибертормоз)
- Права на човека на ООН, Права на децата във връзка с цифровата среда 2019 г.
- Австралийски комисар по електронната безопасност, Преглед на безопасността чрез дизайн, 2019 г.
- УНИЦЕФ, Защо предприятията трябва да инвестират в цифровата безопасност на децата, 2019 г.
- Държавен департамент на САЩ, Доклад за трафика на хора, 2019 г.

2018

- Световен алианс WePROTECT, Global Threat Assessment, 2018
- Детско достойнство в цифровия свят, Доклад на техническата работна група, Съвет на Европа, 2018 г., Препоръка CM/Rec(2018)7 на Комитета на министрите до държавите членки относно насоки за зачитане, защита и изпълнение на правата на детето в цифровата среда, 2018 г.
- Глобален фонд за прекратяване на насилието над деца, Две години помощни решения: резултати от инвестициите на Фонда, 2018 г.
- Световен алианс WePROTECT, Country examples of Model of National Response capacity and implementation (Посочени по държави примери за модел на капацитет за национални ответни действия и изпълнение), 2018 г.
- Интерпол и ECPAT International, Към глобален показател за неидентифицираните жертви в материали за сексуална експлоатация на деца, 2018 г.
- Европол, Оценка на заплахата от организираната престъпност в Интернет (IOCTA), 2018 г.
- NetClean, Доклад за сексуалното насилие над деца, 2018 г.
- Международен център за изчезнали и експлоатирани деца (ICMEC), материал за сексуално насилие над деца: Модел Legislation & Global Review, 9th Edition, 2018
- Международен център за изчезнали и експлоатирани деца (ICMEC), Проучвания в областта на защитата на детето: Сексуално изнудване и неконсенсуална порнография, 2018
- Международна асоциация на горещите линии в Интернет, доклад INHOPE, 2018 г.
- Фондация за наблюдение на Интернет (IWF), Годишен доклад, 2018 г.
- Thorn, Производство и активна търговия на изображения на сексуална експлоатация на деца, 2018
- МСД, Глобален индекс за киберсигурност, 2018 г.
- Експертен център на CSA, Интервенции за извършители на сексуална експлоатация на деца онлайн — преглед на обхвата и анализ на пропуските, 2018 г.
- NatCen, Поведение и характеристики на извършителите на подпомаганата онлайн CSEA — бърза оценка на доказателствата, 2018 г.
- УНИЦЕФ, Ръководство за политиката относно децата и цифровата свързаност, 2018 г.

2017

- Националният център за изчезнали и амп; Експлоатирани деца (NCMEC), онлайн примамването на деца: задълбочен анализ на CyberTipline Reports, 2017 г.
- Фондация 5Права, Цифрово детство, основни етапи на развитието в цифрова среда, 2017 г.
- Childnet, доклад наD eShame, 2017 г.
- Канадски център за защита на детето, Проучване на оцелелите, 2017 г.
- Фондация за наблюдение на Интернет (IWF), Годишен доклад, 2017 г.

- International Centre for Missing & Exploited Children (ICMEC), Годишен доклад, 2017 г.
- Международен център за изчезнали и експлоатирани деца (ICMEC), Онлайн сприятеляване с деца за сексуални цели: Моделно законодателство и Глобален преглед, 2017 г.
- Thorn, Sextortion онлайн проучване с 2,097 жертви на sextortion възраст от 13 до 25, 2017
- УНИЦЕФ, Децата в дигиталния свят, 2017 г.
- Western Sydney University, Young and Online: Детски перспективи за живота в дигиталната ера, 2017 г.
- ECPAT International, Сексуална експлоатация на деца в Югоизточна Азия, 2017

2016

- УНИЦЕФ, "Рискове и възможности: израстване онлайн, 2016 г.
- УНИЦЕФ, Защита на децата в ерата на цифровите технологии: Национални отговори на онлайн CSEA в АСЕАН, 2016 г.
- Център за правосъдие и превенция на престъпността, защита на децата онлайн в региона на Близкия изток и Северна Африка, 2016 г.
- ECPAT International, Междуведомствена работна група по въпросите на сексуалната експлоатация на деца, Терминологични насоки за защита на децата от сексуална експлоатация и сексуално насилие (Насоки от Люксембург), 2016 г.

2015

- Световен алианс WePROTECT, Предотвратяване и борба със сексуалната експлоатация и злоупотребите с деца (CSEA): Модел на национален отговор, 2015 г.
- NCMEC, A Global Landscape of Hotlines Combating CSAM (Глобален пейзаж на горещите линии за борба с CSAM), 2015 г.
- МСД и УНИЦЕФ, Насоки за промишлеността относно защитата на децата онлайн, 2015 г.

Свързани с правата на човека в цифровия свят

- Съвет на Европа, Насоки за зачитане, защита и изпълнение на правата на детето в цифровата среда, 2018 г.
- ЮНЕСКО, Индикатори за универсалност в Интернет, 2019 г.
- Класация на цифровите права (RDR), 2019 г. Индекс на корпоративната отчетност на RDR, 2019 г.
- Комисия по въпросите на широколентовия достъп за устойчиво развитие, Състоянието на широколентовия достъп, 2019 г.
- МСД, Измерване на цифровото развитие, 2019 г.
- МСД, Измерване на информационното общество, 2018 г.

- УНИЦЕФ, Набор от инструменти за детска и цифрова маркетингова индустрия, 2018 г.
- Комисия за широколентов достъп за устойчиво развитие, Цифрово здравеопазване, 2017 г.
- Комисия по въпросите на широколентовия достъп за устойчиво развитие, цифрови умения за живот и работа, 2017 г.
- Комисия по въпросите на широколентовия достъп за устойчиво развитие, цифрово разделение между половете, 2017 г.
- УНИЦЕФ, неприкосновеност на личния живот, защита на личната информация и репутация, 2017 г.
- УНИЦЕФ, Свобода на изразяване на мнение, сдружаване, достъп до информация и участие, 2017 г.
- УНИЦЕФ, Достъп до Интернет и цифрова грамотност, 2017 г.
- Конвенцията на ООН за правата на детето, Насоки за ефективна защита на децата от сексуална експлоатация, 2019 г.

За допълнителни ресурси, моля, вижте списъка с допълнителни ресурси на адрес:

www.itu-cop-guidelines.com

Приложение 1: Терминология

Определенията по-долу се основават главно на съществуващите термини, разработени в Конвенцията за правата на детето от 1989 г., както и на междуведомствената работна група по сексуалната експлоатация на деца в Терминологичните насоки за защита на децата от сексуална експлоатация и сексуално насилие от 2016 г.[72] (Люксембургски насоки) от Конвенцията на Съвета на Европа: Защита на децата срещу сексуална експлоатация и сексуално насилие, 2012 г.,[73] както и от Доклада Global Kids Online, 2019 г.[74].

Подрастващи

Подрастващите са хора на възраст 10—19 години. Важно е да се отбележи, че *подрастващите* не са обвързващ термин съгласно международното право, и тези на възраст под 18 години се считат за деца, а 19-годишните се считат за възрастни, освен ако по националното право не е друго[75].

Изкуствен интелект (ИИ)

В най-широк смисъл терминът се отнася неопределено до системи, които са чиста научна фантастика (т.нар. „силни“ ИИ със самосъзнателна форма)/ "strong" AIs with a self-aware form) и системи, които вече функционират и са способни да изпълняват много сложни задачи (лицево или гласово разпознаване, управление на превозно средство — тези системи са описани като „слаби“ или „умерени“ ИИ)[76].

Системи с ИИ

Системата с ИИ е машинно базирана система, която може, за определен набор от определени от човека цели, да прави прогнози, препоръки или решения, влияещи върху реална или виртуална среда, и е проектирана да работи с различни равнища на автономност[77].

Най-добрият интерес на детето

Описва всички елементи, необходими за вземане на решение в конкретна ситуация за конкретно дете или група деца[78].

Дете

---

[72] „Люксембург Терминологични насоки за защита на децата от сексуална експлоатация и сексуално насилие“, 2016 г., 114, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf.

[73] Съвет на Европа, Conseil de l’Europe и Съвет на Европа, Защита на децата срещу сексуална експлоатация и сексуално насилие: Конвенция на Съвета на Европа (Страсбург: Съвет на Европа, 2012 г.), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

[74] Globalkidsonline.net, „Done Right, Internet Use Canrease Learning and Skills“, ноември 2019 г., http://globalkidsonline.net/synthesis-report-2019/.

[75] УНИЦЕФ и Международния съюз по далекосъобщения, Насоки за промишлеността относно закрилата на децата онлайн (itu.int/cop, 2015 г.), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

[76] Съвет на Европа, „What„s AI?“, coe.int, Artificial Intelligence (Изкуствен интелект), посетен на 16 януари 2020 г., https://www.coe.int/en/web/artificial-intelligence/what-is-ai.

[77] ОИСР, „Препоръка на Съвета относно изкуствения интелект“ (ОИСР, 2019 г.), https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

[78] СВКПЧ, „Конвенция за правата на детето“, посетен на 16 януари 2020 г., https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

В съответствие с член 1 от Конвенцията за правата на детето, дете е всяко лице на възраст под 18 години, освен ако не е навършило пълнолетие по-рано съгласно националното законодателство[79].

Сексуална експлоатация и малтретиране на деца (CSEA)

Описва всички форми на сексуална експлоатация и сексуално насилие (КПД, 1989 г., член 34), напр. "а) подтикване или принуда на дете да участва в незаконна сексуална дейност; б) експлоататорно използване на деца за проституция или други незаконни сексуални практики; в) експлоататорно използване на деца в порнографски представления и материали, както и „сексуален контакт“, който обикновено включва употреба на сила върху лице без съгласие“. Сексуалната експлоатация и малтретирането на деца все повече се извършват чрез Интернет или в някаква връзка с онлайн средата[80]

Материали, съдържащи сексуално (експлоатация и) насилие над деца (CSAM)

Бързото развитие на ИКТ създаде нови форми на сексуална експлоатация и малтретиране на деца онлайн, които могат да се осъществяват на практика и не е необходимо да включват физическа среща лице в лице с детето[81] Въпреки че много юрисдикции все още обозначават изображения и видеоматериали със сексуално насилие над деца като „детска порнография“ или „неприлични изображения на деца“, тези Насоки ще наричат субектите заедно като материали, съдържащи сексуално насилие над деца (оттук нататък, CSAM). Това е в съответствие с Насоките на Комисията по широколентовия достъп и модела за национален отговор WePROTECT на Световния алианс[82]. Този термин описва по-точно съдържанието. Порнографията се отнася до легитимна, комерсиализирана промишленост, а в Насоките на Люксембург се посочва използването на термина:

„*може (неволно или не) да допринесе за намаляване на тежестта, омаловажаване или дори легитимиране на това, което в действителност е сексуално насилие и/или сексуална експлоатация на деца [...], терминът „детска порнография“ рискува да намекне, че действията се извършват със съгласието на детето и представляват законен сексуален материал*“[83]

Терминът CSAM се отнася до материали, представляващи действия, които са сексуално насилие и/или експлоатация на дете. Това включва, но не се ограничава до материали, в които се записва сексуалното насилие над деца от страна на възрастни; изображения на деца, включени в сексуално изрично поведение; половите органи на

[79] СВКПЧ; УНИЦЕФ и Международния съюз по далекосъобщения, *Насоки за промишлеността относно закрилата на децата онлайн*.
[80] “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.”
[81] “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse”; UNICEF, “Global Kids Online Comparative Report (2019).”
[82] Световен алианс WePROTECT, "Предотвратяване и борба със сексуалната експлоатация и укриване на деца (CSEA): Образец на национален отговор, 2016 г., https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf; Широколентова комисия, "Безопасност на децата онлайн: Свеждане до минимум на риска от насилие, злоупотреба и експлоатация онлайн (2019 г.).
[83] Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.”

децата, когато изображенията се произвеждат или използват предимно за сексуални цели.

Деца и младежи

Описва всяко лице на възраст под 18 години, при което децата, посочени също като по-малки деца в Насоките, обхващат всички лица на възраст под 15 години, а младите хора — от 15 до 18-годишна възраст.

Свързани играчки

Свързаните играчки се свързват с Интернет, като използват технологии като Wi-Fi и Bluetooth, и обикновено работят заедно със съпътстващи приложения, за да позволят интерактивна игра за деца. Според Juniper Research през 2015 г. пазарът на свързани играчки е достигнал 2,8 милиарда щатски долара и нараства до 11 милиарда щатски долара до 2020 г. Тези играчки събират и съхраняват лична информация от деца, включително имена, геолокация, адреси, снимки, аудио и видеозаписи[84].

Кибертормоз, наричан още онлайн тормоз

Международното право не определя кибертормоза. За целите на настоящия документ кибертормозът се описва като умишлен агресивен акт, извършван многократно от група или от физическо лице, което използва цифрови технологии и е насочено срещу жертва, която не може лесно да се защити[85]. Той обикновено включва „използване на цифрови технологии и Интернет за публикуване на обидна информация за някого, целенасочено споделяне на лична информация, снимки или видеоматериали по обиден начин, изпращане на заплашителни или обидни съобщения (по електронна поща, съобщения в реално време, чат, текстове), разпространяване на слухове и невярна информация за жертвата или целенасоченото й изключване от онлайн комуникациите“.[86] Той може да включва преки (като чат или текстови съобщения), полупублични (като например публикуване на тормозно съобщение в списък с електронна поща) или публични съобщения (като създаване на уебсайт, посветен на подиграването на жертвата).

Киберомраза, дискриминация и насилствен екстремизъм

„Киберомразата, дискриминацията и насилственият екстремизъм са различна форма на кибернасилие, тъй като са насочени към колективна идентичност, а не към отделни лица [...], които често се отнасят до раса, сексуална ориентация, религия, националност или имиграционен статут, пол и политика“[87]

Цифрово гражданство

---

[84] Джеръми Грийнбърг, "Опасни игри: Свързани играчки, COPPA и лоша сигурност," Georgetown Law Technology Review, 4 декември 2017 г., https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

[85] Anna Costanza Baldry, Anna Sorrentino и David P. Farrington, „Cyberbullying and Cybervictimisation against Parental Supervision, Monitoring and Control of Adolescents' Online activities„(„Кибертормоз и кибервиктимизация срещу родителски надзор, мониторинг и контрол на онлайн дейностите на подрастващите“, Преглед на услугите за деца и младежи 96 (януари 2019 г.): 302—7, https://doi.org/10.1016/j.childyouth.2018.11.058.

[86] UNICEF, "Global Kids Online Comparative Report (2019)"; "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

[87] UNICEF, "Global Kids Online Comparative Report (2019)."

Цифровото гражданство се отнася до способността за позитивно, критично и компетентно участие в цифровата среда, като се използват уменията за ефективна комуникация и творчество, за практикуване на форми на социално участие, които зачитат правата на човека и достойнството чрез отговорно използване на технологиите[88].

Цифрова грамотност

Цифровата грамотност означава да притежавате уменията, от които се нуждаете, за да живеете, да учите и да работите в общество, в което комуникацията и достъпът до информация все повече се осъществяват чрез цифрови технологии като Интернет платформи, социални медии и мобилни устройства[89]. Тя включва ясна комуникация, технически умения и критично мислене.

Цифрова устойчивост

Този термин описва способността на детето емоционално да се справи с вредите онлайн. Цифровата устойчивост включва наличието на емоционални ресурси, необходими, за да се разбере кога детето е изложено на риск онлайн, да знае какво да направи, за да потърси помощ, да се учи от опита и да се възстанови, когато нещата се объркат[90].

Преподаватели

Преподавател е човек, който систематично работи за подобряване на разбирането на друго лице за даден предмет. Ролята на преподавателите обхваща както тези, които преподават в класните стаи, така и по-неофициалните преподаватели, които например използват платформи и услуги на сайтове за социални мрежи, за да предоставят онлайн информация за безопасността или да провеждат курсове, базирани в общността или училището, за да дадат възможност на децата и младите хора да останат в безопасност онлайн. Работата на преподавателите ще варира в зависимост от контекста, в който работят, и от възрастовата група на децата и младите хора (или възрастните), които се стремят да образоват.

Сприятеляване с цел сексуална злоупотреба/онлайн сприятеляване с цел сексуална злоупотреба

Сприятеляването с цел сексуална злоупотреба/сприятеляването онлайн, както е определено в Насоките от Люксембург, се отнася до процеса на установяване на връзка с дете лично или чрез използването на Интернет или други цифрови технологии за улесняване на сексуалния контакт онлайн с това лице, убеждавайки детето да има сексуална връзка[91] Процес, предназначен да примами децата към сексуално поведение или разговори с или без тяхното знание, или процес, който включва комуникация и социализация между извършителя и детето, за да го направи по-уязвимо на сексуално

[88] Съвет на Европа, „Цифрово гражданство и образование за цифрово гражданство“, Образование за цифрово гражданство, посетен на 16 януари 2020 г., https://www.coe.int/en/web/digital-citizenship-education/home.
[89] Western Sydney University-Claire Urbach, „What is Digital Literacy?„(„Какво е цифровата грамотност?“), посетен на 16 януари 2020 г., https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.
[90] Д-р Андрю К. Пшибилски, и др., "Споделена отговорност. Building Children's Online Resilience Report" (ParentZone, University of Oxford and Virgin Media, 2014 г.), https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.
[91] "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

насилие. Понятието „сприятеляване с цел сексуална злоупотреба“ не е определено в международното право; някои юрисдикции, включително Канада, използват термина „примамване, съблазняване“.

Информационни и комуникационни технологии (ИКТ)

Информационните и комуникационните технологии описват всички информационни технологии, които акцентират върху аспекта на комуникацията. Това включва всички услуги и устройства за свързване към Интернет, като например компютри, лаптопи, таблети, смартфони, конзоли за игри, телевизори и часовници[92]. Освен това се включват услуги като радиото, както и широколентовия достъп, мрежовия хардуер и спътниковите системи.

Интернет и свързаните с него технологии

Сега е възможно да се свържете с Интернет с помощта на различни устройства, например смартфони, таблети, конзоли за игри, телевизори и лаптопи, както и по-традиционни компютри. Следователно, освен когато контекстът не подсказва друго, всяко позоваване на Интернет следва да се разбира като обхващащо всички тези различни методи. За да се обхване богатата и комплексна картина на Интернет, „Интернет и свързаните с него технологии“, „ИКТ и онлайн индустриите“ и „Интернет базираните услуги“ се използват взаимозаменяемо.

Уведомяване и премахване на съдържание

Операторите и доставчиците на услуги понякога биват уведомявани за подозрително съдържание онлайн от клиенти, членове на обществеността, правоприлагащи организации или организации на горещи линии. Процедурите за уведомяване и премахване се отнасят до процесите на компаниите за бързо премахване (сваляне) на незаконно съдържание (незаконното съдържание се определя в съответствие с юрисдикцията), веднага след като те бъдат уведомени („уведомление“) за присъствието му в техните услуги.

Онлайн игри

„Онлайн игри“ се определя като игра на всякакъв вид единична или мултиплейърна търговска цифрова игра чрез всяко свързано с Интернет устройство, включително специални конзоли, настолни компютри, лаптопи, таблети и мобилни телефони. „Екосистемата на онлайн игрите“ включва гледане на други видеоигри чрез електронни спортове, стрийминг или платформи за споделяне на видеоклипове, които обикновено предоставят възможности на зрителите да коментират или да взаимодействат с играчите и другите членове на аудиторията[93].

Инструменти за родителски контрол

Софтуер, който позволява на потребителите, обикновено родител, да контролират някои или всички функции на компютър или друго устройство, което може

[92] УНИЦЕФ и Международния съюз по далекосъобщения, *Насоки за промишлеността относно закрилата на децата онлайн.*

[93] УНИЦЕФ, "Права на децата и онлайн игри: Възможности и амп; предизвикателства пред децата и индустрията," DISCUSSION PAPER SERIES: Правата на децата и бизнесът в един цифров свят, 2019 г., https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

да се свърже с Интернет. Обикновено такива програми могат да ограничат достъпа до определени видове или класове уебсайтове, или онлайн услуги. Някои също така предоставят възможност за управление на времето, т.е. устройството може да бъде настроено да има достъп до Интернет само между определени часове. По-усъвършенстваните версии могат да записват всички текстове, изпратени или получени от устройството. Програмите обикновено са защитени с парола[94].

Родители, предоставящи грижи, настойници

Няколко Интернет сайта се отнасят до родителите по общ начин (като например „страница за родители“ и до „родителски контрол“) Поради това може да е полезно да се определят хората, които в идеалния случай следва да дадат възможност на децата да увеличат максимално наличните онлайн възможности, да гарантират, че децата и младите хора използват Интернет сайтове безопасно и отговорно и да дадат съгласието си за достъп до конкретни Интернет сайтове. В настоящия документ терминът „родители“ се отнася за всяко лице (с изключение на преподавателите/възпитателите), което носи правна отговорност за дете. Родителската отговорност варира в отделните държави, както и законните родителски права.

Лична информация

Терминът описва индивидуално идентифицираща информация за дадено лице, която се събира онлайн. Това включва пълното име, данните за контакт като домашен адрес и адрес на електронна поща, телефонни номера, пръстови отпечатъци или материали за разпознаване на лица, застрахователни номера или всеки друг фактор, който позволява физически или онлайн контакт или локализация на дадено лице. В този контекст той се отнася и до всяка информация за детето и неговото обкръжение, която се събира онлайн от доставчиците на услуги онлайн, включително свързани играчки и Интернет на нещата, както и всяка друга свързана технология.

Неприкосновеност на личния живот

Неприкосновеността на личния живот често се измерва по отношение на споделянето на лична информация онлайн, наличието на публичен профил в социалните медии, споделянето на информация с хората, които те познават онлайн, използването на настройки за неприкосновеност на личния живот, споделянето на пароли с приятели, загрижеността относно неприкосновеността на личния живот[95].

Секстинг

Секстингът обикновено се определя като изпращане, получаване или обмен на самостоятелно произведено сексуално съдържание, включително изображения, съобщения или видеоклипове чрез мобилни телефони и/или Интернет[96]. Създаването, разпространението и притежаването на сексуални изображения на деца е незаконно в повечето държави. Ако се разкрият сексуални изображения на деца, възрастните не трябва да ги виждат. Споделянето на сексуални изображения от възрастен с дете винаги

---

[94] УНИЦЕФ и Международния съюз по далекосъобщения, *Насоки за промишлеността относно закрилата на децата онлайн.*

[95] „Детски закон за защита на личните данни онлайн“, Пъб. L. № 15 U.S.C. 6501—6505 (1998 г.), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

[96] “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.”

е престъпно деяние и между децата може да възникне вреда и може да са необходими съобщаване и действия за премахване на споделени изображения.

Сексуално изнудване на деца

Sextortion описва или сексуално изнудване (наричано също „онлайн сексуална принуда и изнудване„)[97] „изнудване на лице с помощта на собствени изображения на това лице за сексуални услуги, пари или други облаги от него под заплаха от споделяне на материала без съгласието на изобразеното лице (напр. публикуване на изображения в социалните медии)“[98].

Интернет на нещата (IoT)

Интернет на нещата представлява следващата стъпка към цифровизацията на обществото и икономиката, където обектите и хората са взаимосвързани чрез комуникационни мрежи и докладват за техния статус и/или заобикалящата ги среда[99].

URL АДРЕС

Съкращението означава „уникален локатор на ресурси“, адресът на Интернет страница[100].

Виртуална реалност

Виртуалната реалност е използването на компютърни технологии за създаване на ефекта на интерактивен триизмерен свят, в който обектите имат усещане за пространствено присъствие[101].

Wi-Fi

Wi-Fi (Wireless Fidelity) е групата от технически стандарти, които позволяват предаване на данни по безжични мрежи[102]

[97] Europol, “Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective” (European Cybercrime Centre, May 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

[98] “Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.”

[99] Ntantko, The Internet of Things (Интернет на нещата), 1 октомври 2013 г., цифров единен пазар — Европейска комисия, https://ec.europa.eu/digital-single-market/en/internet-of-things.

[100] УНИЦЕФ и Международния съюз по далекосъобщения, *Насоки за промишлеността относно закрилата на децата онлайн.*

[101] НАСА, „Виртуална реалност“, nas.nasa.gov, посетен на 16 януари 2020 г., https://www.nas.nasa.gov/Software/VWT/vr.html.

[102] Children’s Online Privacy Protection Act.

Приложение 2: Контактни престъпления срещу деца и младежи

Децата и младите хора могат да бъдат изложени на редица нежелани или неподходящи контакти в Интернет, които могат да имат тежки последици за тях. Някои от тези контакти може да са сексуални по природа.

Проучванията показват, че 22 % са били тормозени[103] или преследвани онлайн; 24 % са получили нежелани сексуални коментари;[104] 8 % са се срещали с хора в реалния живот, които преди това са познавали само онлайн[105]. Въпреки че процентите варират по държави и региони, тези цифри показват, че рисковете са реални[106]. Едно проучване в Интернет в Съединените американски щати[107] установи, че 32 % от тийнейджърите онлайн са се свързали с напълно непознат, от които 23 % казват, че са се чувствали уплашени и неудобно по време на контакта; а 4 % са получили агресивно сексуално настояване.

Сексуалните „хищници“ използват Интернет, за да се свързват с деца и млади хора за сексуални цели, като често използват техника, известна като „сприятеляване с цел сексуална злоупотреба“, чрез която те печелят доверието на детето, като привличат интересите му. Те често въвеждат сексуални теми, снимки и изричен език, за да десенсибилизират, повишават сексуалната осведоменост и омекотяват волята на младите си жертви. Подаръците, парите и дори билетите за транспорт се използват, за да убедят и примамят детето или младия човек на място, където „хищникът“ може да го експлоатира сексуално. Тези срещи могат дори да бъдат записани или заснети на видео. Децата и младите хора често нямат емоционална зрялост и самочувствие, което ги прави податливи на манипулация и сплашване. Те се колебаят да кажат на възрастните за своите срещи от страх, от срам или от загуба на достъп до Интернет. В някои случаи те са застрашени от „хищниците“ и им се казва да пазят връзката в тайна. Сексуалните „хищници“ също се учат един от друг чрез Интернет форуми и чат стаи.

[103] U-доклад (2019 г.), http://www.ureport.in/v2/.
[104] Проект dEShame (2017 г.), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.
[105] Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships, https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/
[106] Livingstone, S., Haddon, L., Görzig, A. и Ólafsson, K. (2011 г.). *Рискове и безопасност в Интернет: Гледната точка на европейските деца. Пълни констатации*. LSE, Лондон: EU Kids Online, http://eprints.lse.ac.uk/33731/.
[107] Amanda Lenhart et al., “The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive Online Media.,” *Pew Internet and American Life Project*, 2007, 44, https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Приложение 3: Световният алианс WeProtect

Моделът за национален отговор WePROTECT

Стратегията за Световния алианс WePROTECT подкрепя държавите да разработят координирани отговори с участието на множество заинтересовани страни за справяне със сексуалната експлоатация на деца онлайн, ръководени от нейния модел за национален отговор (MNR). Моделът за национален отговор на WPGA действа като план за действие на национално равнище. Той предоставя рамка, която държавите да използват за справяне със сексуалната експлоатация на деца онлайн (OCSE). Моделът има за цел да помогне на дадена държава да:

- направи оценка на настоящия отговор на OCSE и да установи пропуските;
- се даде приоритет на националните усилия за запълване на пропуските;
- се засили международното разбирателство и сътрудничество.

Моделът няма за цел да предписва дейности, нито да определя единен подход. Целта му е да опише способностите, необходими за ефективна защита на детето и да подкрепи държавите да развият или подобрят съществуващите си способности. В него са изброени и редица фактори, които, ако са налице и ефективни, ще ускорят и подобрят резултатите. MNR включва двадесет и една възможности, разделени в шест раздела: политиката и управлението, наказателното правосъдие, жертвите, обществото, промишлеността и медиите и комуникациите. Работната група счита, че действията и в шестте области ще доведат до цялостен национален отговор на тези престъпления.

Моделът ще даде възможност на дадена държава — независимо от отправната си точка — да установи евентуални пропуски в способностите и да започне планиране за запълване на тези пропуски. Въпреки че държавите ще разработят свои собствени индивидуални подходи, като го направят в контекста на общоприета рамка и разбиране на способностите, се надяваме, че комуникацията и сътрудничеството между заинтересованите страни както на национално, така и на международно равнище могат да бъдат допълнително засилени.

Глобалният стратегически отговор WePROTECT

Глобалният стратегически отговор WePROTECT Global Alliance (GSR) е координиран подход за борба със сексуалната експлоатация на деца онлайн, който включва по-голяма глобална представа, международна хармонизация на националните подходи и глобални решения в допълнение към действията, ръководени от държавите. GSR е по същество допълнение към модела на национален отговор (MNR); въпреки че MNR е съсредоточен върху способностите, необходими за справяне с OCSE на национално равнище, GSR е съсредоточен върху приоритетните области за международно сътрудничество и изграждане на капацитет. GSR включва шест тематични области с необходими и очаквани резултати за всяка от тях, както и партньори, които следва да работят заедно, за да ги постигнат.

Политика и законодателство

Развитието както на политическата воля за действие, така и на законодателството за ефективно хармонизиране на подхода към престъпленията ще доведе до подновяване на ангажимента на високо равнище на национално и международно ниво за борба със сексуалната експлоатация на децата онлайн.

Наказателно правосъдие

Обменът на информация, включително споделен достъп до международни бази данни чрез официални рамки за обмен на данни, съчетани със специални, обучени служители и прокурори с опит в областта на сексуалната експлоатация на деца онлайн, е най-добрият начин за идентифициране, преследване и задържане на извършителите на престъпления, включително чрез успешни съвместни разследвания и присъди.

Въздействие върху жертвите и услуги

Ефективната и навременна подкрепа за жертвите, включително защитата на тяхната самоличност и предоставянето на глас, спомагат да се гарантира, че жертвите имат достъп до подкрепата, от която се нуждаят, когато се нуждаят от нея.

Технология

Използването на технически решения, включително изкуствен интелект, за откриване, блокиране и предотвратяване на вредни материали, стрийминг на живо и онлайн сприятеляване с цел сексуална злоупотреба, които трябва да включват широко и последователно възприемане от технологичния сектор, ще позволи на тези платформи да избегнат използването им като инструмент за сексуална експлоатация на деца онлайн.

Общество

Съществуват редица възможности, които работят заедно в рамките на обществото като цяло, за да дадат възможност на децата да се защитят от сексуалната експлоатация онлайн, независимо къде живеят. Като се гарантира, че развитието на цифровата култура е по-безопасно още при проектирането (т.е. има вградени елементи за безопасност) и че съществува етичен и последователен подход към медийното отразяване, излагането на незаконно съдържание онлайн ще бъде ограничено. Междувременно образованието и достигането до децата и родителите, лицата, полагащи грижи, и специалистите, както и целенасочените интервенции за нарушителите, всички трябва да работят за предотвратяване или ограничаване на възникването на сексуална експлоатация на деца онлайн.

Изследвания и оценки

И накрая, оценките на заплахите (като например оценката на глобалната заплаха за 2019 г.), изследвания на извършителите и работата за разбиране на дългосрочните травми на жертвите ще дадат на правителството, правоприлагащите органи, гражданското общество, академичните среди и промишлеността ясно разбиране за заплахите.

Приложение 4: Примери за отговори на онлайн вреди

Примерите, включени тук, са събрани от авторите и сътрудниците при изготвянето на Насоките на МСД за създателите на политики.

Образоване на децата срещу онлайн вреди

BBC Own IT App - приложение за благосъстояние, насочено към деца на възраст 8 - 13 години, получаващи първия си смартфон. Съчетавайки най-съвременните технологии за машинно самообучение за проследяване на активността на децата на техния смартфон със способността на децата сами да докладват емоционалното си състояние, то използва тази информация, за да осигури персонализирано съдържание и интервенции, за да помогне на децата да останат щастливи и здрави онлайн.

С участието на специално поръчано съдържание от BBC, приложението предоставя полезни материали и ресурси, за да помогне на младите хора да се възползват максимално от времето си онлайн и да изградят здравословни онлайн поведения и навици, помагайки на младите хора и родителите да водят по-конструктивни разговори за преживяванията си онлайн. Приложението не събира никакви лични данни или съдържание, генерирани от потребителя, тъй като цялото машинно самообучение се осъществява в рамките на приложението/в рамките на устройството на потребителя.

Проект Evolve - Напълно обезпечена с ресурси образователна рамка за компетентностите в областта на цифровите технологии, идентифицираща цифровите умения за всяка възраст на детето, за да помогне на родителите и учителите да разберат компетенциите, които техните деца трябва да притежават, заедно с ресурси и дейности, които ще им осигурят конкретните умения.

360 градуса безопасно - онлайн инструмент за самооценка за училищата при разглеждането и оценяването на цялото им онлайн осигуряване на безопасност, предоставящо насоки и подкрепа за спазване на определени стандарти.

DQ Institute — Данни бяха събрани от 145 426 деца и юноши в 30 страни от 2017—2019 г. като част от #DQEveryChild, глобално движение за цифрово гражданство, подкрепяно от института DQ, което започна в Сингапур с подкрепата на Singtel и бързо се разшири в сътрудничество със Световния икономически форум, за да включи над 100 партньорски организации. Това движение имаше за цел да даде възможност на децата с всеобхватни умения за цифрово гражданство от началото на техния цифров живот, като използват онлайн програмата за образование и оценка DQ World. Данните от това движение бяха използвани за създаване на Индекса за безопасност на децата онлайн за 2020 г. (COSI). Рамката за COSI оценява и класира безопасността на децата онлайн в 30 държави въз основа на 24 области, групирани в шест стълба, които засягат безопасността на децата онлайн.

DQ Pro Family Readiness Package и DQ World предоставят възможности на родителите да оценят цифровата готовност на детето си и чрез образователни материали да подобрят цифровите компетентности като цифрово гражданство, управление на

времето на екрана, управление на кибертормоза, управление на киберсигурността, цифрова емпатия, управление на цифровия отпечатък, критично мислене и управление на неприкосновеността на личния живот.

Австралия eSafety Toolkit за училища е набор от ресурси, предназначени да подкрепят училищата да се създаде по-безопасна онлайн среда. Наборът от инструменти отразява многостранен подход към онлайн образованието по безопасност и е категоризиран в четири елемента, с ресурси, които:

- да подготви училищата за оценка на готовността им да се справят с въпросите на онлайн безопасността и да предоставят предложения за подобряване на настоящите си практики;
- ангажиране на цялата училищна общност и участие в създаването на безопасна онлайн среда;
- образоване чрез изтъкване на най-добрите практики в областта на онлайн образованието по безопасност и подпомагане на училищата да развиват онлайн способностите за безопасност на училищната общност;
- да реагира ефективно на инциденти, като същевременно подпомага безопасността и благосъстоянието.

Службата за електронни съобщения на Полша-UKE I Click Sensible образователна кампания образова децата и родителите за това как да бъдат по-защитени онлайн и как да разпознават и управляват риска.

ChildFund Виетнам създаде инициативата Swipe Safe. Тази програма образова децата относно потенциалните рискове онлайн, като кибер измами, тормоз или сексуално насилие, и представя съвети относно методите за безопасност.

Доклад на Комисията по въпросите на широколентовия достъп относно *технологиите, широколентовия достъп и образованието: напредък по програмата „Образование за всички*“, 2013 г.

Детски опит онлайн: Изграждане на глобално разбиране и действие, УНИЦЕФ, 2019 г. Global Kids Online изследване включва богата информация за добри практики и отговори на онлайн вреди.

Примери за ангажиране на промишлеността

Австралийският комисар по електронната безопасност изгражда силни партньорства и работи с промишлеността, за да даде възможност на всички австралийци да имат по-безопасен и по-положителен опит онлайн. Пример за това е работата на eSafety в областта на безопасността още при проектирането. Като част от инициативата eSafety се проведе подробен процес на консултации с промишлеността, търговските органи и организациите, отговарящи за защитата на потребителите, както и с родителите, лицата, полагащи грижи и младите хора. Инициативата „Безопасност при

проектирането“ има за цел да насърчи и подпомогне индустрията да гарантира, че безопасността на потребителите е включена в проектирането, разработването и внедряването на онлайн услуги и платформи. eSafety също така администрира три схеми за докладване и подаване на жалби: схемата за кибертормоз, схемите за злоупотреба с изображения и схемата за онлайн съдържание. eSafety може официално да насочи определени доставчици на онлайн услуги да премахват съдържание от своите услуги. Въпреки че схемите до голяма степен функционират като кооперативен модел между правителството и промишлеността, правомощията, с които разполага eSafety, за да принуди отстраняването на материали, осигурява критична предпазна мрежа и кара промишлеността да бъде проактивна в борбата с онлайн вредите.

Дружеството Telia поема отговорност да разбере и управлява отрицателните въздействия на свързаността и да бъде напълно прозрачна и отчетна на равнището на Управителния съвет. Те също така се грижат за децата и младите хора, защото признават, че са активни потребители на техните услуги.

Службата за електронни съобщения на Полша-UKE включва гражданското общество и децата в техните застъпнически кампании, за да ги накара да осъзнаят какво подписват онлайн.

Фондацията за наблюдение на Интернет е партньорска организация, която обединява индустрията, правителството, правоприлагащите органи и НПО за премахване на сексуалното насилие над деца. През 2020 г. IWF имаше 152 членове в платформите и инфраструктурните услуги и предлага на членовете набор от услуги за предотвратяване на разпространението на престъпни изображения на техните платформи.

Обхват на законодателството

Да изрази политическа воля за даване на приоритет на СОР чрез подписване на Всеобщата декларация за безопасност на децата онлайн (Комисията за широколентов достъп).

Регулация

„Извън сенките“: показателят за противодействие на сексуалното насилие и сексуална експлоатация на деца (2019 г.) от Economist Intelligence Unit (2019 г.) е единственият референтен инструмент, който анализира реакцията на държавите на сексуалното насилие и сексуалната експлоатация на деца, включително в цифровото пространство и реакцията на сектора на ИКТ спрямо него.

Идентифициране на малтретирането на деца онлайн

По-долу са представени примери за добри практики при идентифицирането на малтретирането на деца онлайн.

INHOPE: Мрежата INHOPE е създадена през 1999 г. за борба с онлайн CSAM в отговор на споделена визия за Интернет, която не съдържа материали, съдържащи сексуално насилие над деца. През последните 20 години INHOPE се разраства, за да се бори успешно с растежа, географското разпространение и сериозността на онлайн CSAM. Днес горещите линии INHOPE работят на място във всеки континент, получават доклади и бързо премахват CSAM от Интернет и обменят данни с правоприлагащите органи.

Microsoft PhotoDNA създава хешове*на изображения и ги сравнява с база данни с хешове, които вече са идентифицирани и потвърдени като CSAM. Ако намери съвпадение, изображението се блокира. Този инструмент обаче не използва технология за разпознаване на лица, нито може да идентифицира лице или обект в изображението. Но с изобретяването на PhotoDNA за видео, нещата са поели в друга посока.

PhotoDNA за видео разгражда видеото на ключови кадри и по същество създава хешове за тези снимки на екрани. По същия начин, по който PhotoDNA може да съответства на изображение, което е било променено, за да се избегне откриването, PhotoDNA за видео може да намери съдържание, свързано със сексуална експлоатация на деца, публикувано във видео, което в противен случай може да изглежда безвредно.

Microsoft пусна нов инструмент за идентифициране на деца „хищници“, които се сприятеляват с деца за малтретиране в онлайн чатове. **Проект Artemis,** разработен в сътрудничество с The Meet Group, Roblox, Kik и Thorn, се основава на патентованата технология на Microsoft и ще бъде свободно достъпен чрез Thorn за компании за онлайн услуги, които предлагат чат функция. Проект Artemis е технологичен инструмент, който помага за вдигане на червени флагове на администраторите, когато е необходима някаква модерация в чат стаите. Тази техника за откриване на сприятеляване с цел сексуална злоупотреба ще може да открива, адресира и съобщава за „хищници“, опитващи се да примамят деца за сексуални цели.

Торн е разработил възпиращи реклами, насочени към тези, които търсят материали, съдържащи сексуално насилие над деца, които са били обслужвани милиони пъти в четири търсачки за период от три години. Освен това рекламите са видели 3 % кликване от хора, търсещи помощ след търсене на експлоататив материал.

Thorn's Safer, инструмент, който може да бъде внедрен директно на платформа на частна компания за идентифициране, премахване и докладване на CSAM.

Thorn Spotlight, софтуер, който дава на правоприлагащите органи във всички 50 щата в Съединените американски щати и в Канада способността да се ускори идентифицирането на жертвите и да се намали времето за разследване с повече от 60 %.

* Хеширането е просто предаване на някои данни през формула, което произвежда резултат, наречен хеш. Този хеш обикновено е низ от знаци и хешовете, генерирани от формула, винаги са с еднаква дължина, независимо от това колко данни подавате в него Бел.АД

Geebo, секретен сайт, който се ангажира да държи сексуалната експлоатация извън своята платформа, никога не е имал случай, свързан със сексуална експлоатация на деца. Те успяват да направят това отчасти поради своя процес на предварителна проверка.

Google AI Classifier може да се използва за откриване на материали, съдържащи сексуално насилие над деца, в мрежи, услуги и на платформи. Този инструмент е достъпен безплатно чрез API за безопасност на съдържанието на Google, който е набор от инструменти, който увеличава капацитета за преглед на съдържанието по начин, който изисква по-малко хора да бъдат изложени на него. Този инструмент ще помогне на експертите да преглеждат материалите в още по-голям мащаб и да са в крак с нарушителите, като насочват изображения, които преди това не са били маркирани като незаконни материали. Споделянето на тази технология ще ускори идентифицирането на изображенията.

През 2015 г. Google разшири работата си по хешовете, като въведе първата по рода си технология за снемане на пръстови отпечатъци и съчетаване на видеоматериали в YouTube, които сканират и идентифицират качени видеоклипове, които съдържат известни материали, включващи сексуално насилие над деца.

По време на Хакатона за безопасност на децата през 2019 г. Facebook обяви две технологии с отворен код, които откриват идентични и почти идентични снимки и видеоклипове. Тези два алгоритъма са достъпни в GitHub, което позволява на системите за споделяне на хеш да разговарят помежду си, което прави системите много по-мощни.

Горещата линия на IWF продължава да бъде бдителна, като не само следи хилядите съобщения от граждани, които може да са се натъкнали на изображения на сексуално насилие над деца онлайн, но също така изпълнява уникална проактивна роля в търсенето на това незаконно съдържание в Интернет. Като се даде възможност на горещите линии да използват информацията и ресурсите си, повече съдържание може да бъде идентифицирано и премахнато. Нещо повече, IWF непрекъснато работи с Google, Microsoft, Facebook и други компании в рамките на членството си, непрекъснато да разгръщат техническите граници. IWF предлага решението на портала за докладване, което позволява на потребителите на Интернет в държави и нации без горещи линии да докладват изображения и видеоматериали с предполагаеми сексуално насилие над деца директно на IWF чрез специално създадена онлайн страница на портала.

IWF в сътрудничество с благотворителната фондация „Мари Колинс“ в подкрепа на жертвите има за цел да създаде нова кампания, в която младите мъже да бъдат призовани да съобщават за всички самогенерирани сексуални изображения или видеоматериали на деца под 18 години, на които могат да се натъкнат, докато сърфират онлайн.

Интерпол създаде международна база данни с изображения и видеоматериали за сексуална експлоатация на деца (ICSE), която е инструмент за разузнаване и разследване, позволяващ на специализирани следователи от повече от 50 държави да обменят данни за случаи на сексуално насилие над деца. Чрез анализиране на цифровото, визуално и аудио съдържание на снимки и видеоматериали експертите по

идентифициране на жертвите могат да извличат улики, да идентифицират всяко припокриване в случаите и да обединят усилията си за откриване на жертвите на сексуално насилие над деца. Понастоящем базата данни на Интерпол за сексуална експлоатация на деца съдържа повече от 1,5 милиона изображения и видеоматериали и е помогнала за идентифицирането на 19 400 жертви по света.

NetClean ProActive е софтуер, базиран на съвпадение на подписи и други алгоритми за откриване, който автоматично открива изображения на сексуално насилие над деца и видеоклипове в корпоративни среди.

Griffeye Brain използва изкуствен интелект, за да сканира некласифицирано преди това съдържание, да го сравни с атрибутите на известното съдържание на CSAM и да постави подозрителни елементи за преглед от агент.

Rainn създаде и управлява Националната гореща линия за сексуално нападение в партньорство с повече от 1 000 местни доставчици на услуги за докладване на сексуално насилие в цялата страна и управлява горещата линия на DoD Safe за Министерството на отбраната. Рейн също така провежда програми за предотвратяване на сексуалното насилие, за подпомагане на оцелелите и за гарантиране, че извършителите ще бъдат изправени пред съда.

Safehorizon е организация за подпомагане на жертвите с нестопанска цел, която от 1978 г. е изправена пред жертви на насилие и злоупотреба в Ню Йорк. Safehorizon предлага услуги по гореща линия на жертвите на насилие.

Проект Arachnid е иновативен инструмент, управляван от канадския център за борба с нарастващото разпространение на материали, съдържащи сексуално насилие над деца (CSAM) в Интернет.

With the support of: