



Съфинансирано от  
Европейския съюз

# ДИГИТАЛИЗАЦИЯТА НА ТРАФИКА НА ХОРА: НОВОВЪЗНИКВАЩИ РИСКОВЕ, ИНСТИТУЦИОНАЛНИ ОТГОВОРИ И ПОЛИТИЧЕСКИ ПРЕДИЗВИКАТЕЛСТВА

*Антоанета Василева*



*София, 2026*



## 1. Въведение

Трафикът на хора днес е широко признат като една от най-сериозните и доходоносни форми на организирана престъпност, нареждаща се до трафика на наркотици и оръжие, с приблизителни годишни печалби, достигащи около 31 милиарда евро. В продължение на години редица държави отричаха съществуването на съвременни форми на робство или подценяваха техните последици. Днес обаче повече от 180 държави в света признават трафика на хора като системен проблем и са приели законодателни мерки, насочени към неговото криминализиране и предотвратяване.

Въпреки тези усилия, трафикът на хора с различни форми на експлоатация продължава да се развива и процъфтява - сексуална експлоатация, трудова експлоатация, принудително извършване на престъпления, отнемане на органи и др. Престъплението влияе върху миграционните процеси, поражда нови предизвикателства пред сигурността в Европейския съюз и води до сериозни икономически и социални последици за жертвите. Еволюиращият характер на това престъпление все повече поставя под въпрос ефективността на традиционните подходи, тъй като трафикът се осъществява през граници, икономически сектори и правни режими, като често използва пропуски в законодателните и институционалните рамки.

Бързото развитие и широкото разпространение на информационните и комуникационните технологии — и конкретно интернет — въведоха ново измерение в трафика на хора. Дигиталните технологии оказват влияние върху всички етапи на престъплението — от набиране и експлоатация до контрол, превенция и противодействие. Макар интернет да осигурява бърза, достъпна и дори евтина комуникация независимо от географското местоположение, през последните петнадесет години Мрежата демонстрира и значителен потенциал да улеснява престъпна дейност по безпрецедентен начин.



Днес трафикантите разполагат с високоефективни, често анонимни и в голяма степен нерегулирани дигитални инструменти, които позволяват целенасочено набиране, експлоатация и контрол върху жертвите в широк мащаб. Онлайн средата предоставя безпрецедентни възможности, които бързо бяха използвани от извършителите. Организираните престъпни групи, както и отделни извършители, все по-често използват дигитални платформи за набиране, рекламиране и експлоатация на жени и деца. По сходен начин агенции за работа, брачни посреднически услуги и модни агенции често се използват като средство за привличане на потенциални жертви на съвременни форми на експлоатация.

Чат стаи, специализирани уебсайтове, криптирани комуникационни канали и в някои случаи т.нар. тъмна мрежа (Dark Web)<sup>1</sup> се използват за идентифициране и набиране на жертви, като значително увеличават излагането на деца и млади хора на риск от експлоатация и усилват съществуващите уязвимости. Дигиталната среда не само разширява мащаба на потенциалната виктимизация, но и създава нови форми на уязвимост, свързани с онлайн поведение, видимост и модели на взаимодействие. Тези процеси не само променят профила на трафикантите и жертвите, но и трансформират начина на действие на мрежите на трафикантите, като едновременно с това усложняват разкриването и разследването на престъплението, и защитата на жертвите.

В отговор на тези процеси международните и европейските правни и политически рамки постепенно започнаха да отчитат ролята на технологиите в улесняването на трафика на хора. Въпреки това, продължава да съществува значителна разлика между законодателството, политиките и оперативната реалност. Институционалните практики, разследващите инструменти и системите за подкрепа на жертвите често изостават спрямо форми на експлоатация, които са децентрализирани, транснационални и се осъществяват чрез диги-



тални технологии. В резултат на това трафикът на хора, улеснен чрез технологии, често остава недоразпознат, недостатъчно разследван и неадекватно обхванат от съществуващите механизми за закрила.

Настоящата статия разглежда как дигитализацията променя трафика на хора като трансформира на профила на трафикантите и жертвите, изменя начините на извършване на престъплението и поставя на нови предизвикателства пред институциите и политиките, като същевременно създава нови аспекти и задълбочава вече съществуващата уязвимост на хората към експлоатация в дигитална среда. На основата на качествен анализ, базиран на експертен опит, наблюдение на политики и институционална практика, статията откроява ключови предизвикателства при разкриването, идентифицирането и защитата на жертвите в случаи на трафик, улеснен чрез технологии. Тя също така разглежда нововъзникващи глобални тенденции и добри практики, и формулира препоръки за политики, насочени към изграждане на координирани, постоянно адаптиращи се и ориентирани към жертвите подходи в условията на все по-дигитализирана среда.



## 2. Концептуална и правна рамка

Трафикът на хора се дефинира в международното право като процес, включващ набиране, транспортиране, прехвърляне, укриване или приемане на лица, чрез заплахата, сила, принуда, измама или злоупотреба с власт, с цел експлоатация. Макар основните елементи да остават непроменени, контекстът, в който се осъществява трафикът на хора, се е променил съществено с навлизането на дигиталните технологии във всички етапи на престъплението.

Нарастващото използване на съвременните технологии при трафика на хора следва да се разглежда в по-широкия контекст на дигитализацията, която надхвърля простото прилагане на технически инструменти. Дигитализацията представлява системна интеграция на дигитални технологии в социалните, икономическите и институционалните процеси, която променя начина, по който се осъществяват взаимодействията, организират се услугите и се координират дейности дори през географските граници. Тя обхваща не само интернет и дигиталните комуникационни средства, но и нарастващата употреба на онлайн платформи, системи, базирани на данни, автоматизирани процеси и дигитална инфраструктура в ежедневието. В този смисъл дигитализацията отразява по-дълбоки структурни трансформации, засягащи властовите и йерархичните отношения, достъпа до информация и организацията на труда и пазарите, с пряко отражение върху начина, по който трафикантите действат, как жертвите биват набирани, контролирани и експлоатирани, както и как правоприлагащите органи откриват, разследват и реагират на престъпления, свързани с трафик на хора.

В контекста на трафика на хора дигитализацията не следва да се разбира като възникване на нов вид престъпление, а като хоризонтален фактор, който променя начина, по който се извършват съществуващите престъпни дейности. Онлайн платформи, социални мрежи, приложения за съобщения и дигитални платежни системи



все по-често посредничат при набиране, комуникация, контрол и експлоатация. В резултат на това трафикът на хора става по-малко видим, все по-децентрализиран и по-труден за разкриване чрез традиционните оперативни и институционални механизми.

Международните и европейските правни рамки постепенно започнаха да отчитат ролята на технологиите в улесняването на престъпления, свързани с трафик на хора. Инструменти като Конвенцията на Съвета на Европа за борба с трафика на хора и съответните директиви на Европейския съюз предоставят всеобхватна дефиниция на трафика и установяват задължения, свързани с превенцията, защитата на жертвите и наказателното преследване. По-новите политически документи и стратегии все по-често разглеждат онлайн набирането, дигиталното посредничество и необходимостта от засилено сътрудничество с технологичния сектор.

На европейско ниво правната и политическата рамка, свързана с онлайн вредите за деца и отговорността на платформите, също се разви значително, което допринася за подобряване на противодействието на експлоатацията, свързана с трафик на хора. Инструменти като Конвенцията на Съвета на Европа за защита на децата от сексуална експлоатация и сексуално насилие (Конвенция Ланзароте)<sup>2</sup>, наред със законодателството на ЕС относно материали със сексуално насилие над деца (CSAM), установяват задължения, свързани с превенция, откриване и защита на жертвите в дигитална среда. Приетият през 2022 г. Регламент за цифровите услуги (Digital Services Act) въвежда хоризонтални правила относно отговорността на платформите, оценката на риска и модерирването на съдържание, включително по отношение на системни рискове за основните права. Паралелно с това предложението за регламент за предотвратяване и борба със сексуалното насилие над деца (COM(2022) 209 final) отразява текущите усилия за засилване на механизмите за откриване и докладване на онлайн сексуална експлоатация. Макар тези рамки да не са насочени изрично към трафика на хора, те все по-силно



оформят регулаторната среда, в която се развива експлоатацията, улеснена чрез технологии, особено в случаи, свързани с деца и злоупотреби, осъществявани чрез платформи.

Въпреки това, независимо от нарастващото признаване на ролята на дигиталните технологии в улесняването на дейности, свързани с трафик на хора, съществуващите рамки до голяма степен остават технологично неутрални в своя оперативен дизайн. Правните дефиниции се фокусират върху действията, средствата и целите, но предоставят ограничени насоки относно това как тези елементи се проявяват в дигитална среда. В резултат на това трафикът на хора, улеснен чрез технологии, често остава недоразпознат или неправилно класифициран в рамките на установените правни категории, особено когато експлоатацията се осъществява чрез платформи, комуникация, позволяваща анонимност, или чрез дигитални услуги, функциониращи в различни юрисдикции.

От концептуална гледна точка, трафикът на хора, улеснен чрез технологии, се пресича с по-широки категории киберпрестъпност, като същевременно запазва своята специфика, свързана с принуда, експлоатация и продължителен контрол върху жертвите. За разлика от самостоятелните киберпрестъпления, трафикът на хора включва устойчиви взаимоотношения между извършители и жертви, които все по-често се поддържат чрез дигитални средства. Това размиване на границите усложнява класификацията, разследването и събирането на данни и допринася за неравномерни реакции в различните юрисдикции.

От гледна точка на политиките, основното предизвикателство не е липсата на правни инструменти, а разрывът между формалното признаване и практическото прилагане. Макар правните и стратегическите рамки да отчитат дигиталните рискове, институционалният капацитет, разследващите инструменти и механизмите за подкрепа на жертвите често изостават спрямо реалностите на онлайн



експлоатацията. Ефективното противодействие на трафика на хора, улеснен чрез технологии, изисква не само спазване на правните изисквания, но и адаптивни интерпретации, оперативни насоки и засилена координация между органите на наказателното правосъдие, социалните услуги и дигиталните платформи, както и по-добро разпознаване на пресечните точки между трафика на хора и други форми на киберпрестъпност, които все по-често се преплитат в дигиталната среда.



### 3. Методология и аналитичен подход

Настоящата статия прилага качествен, експертно-базиран аналитичен подход за изследване на въздействието на дигитализацията върху трафика на хора. Макар да не представлява първично емпирично изследване, анализът се основава на съчетание от наблюдение на политики, преглед на налични качествени и количествени данни, институционално взаимодействие и дългогодишна професионална практика в областта на борбата с трафика на хора, закрилата на децата, дигиталната и онлайн безопасност. Този подход позволява задълбочено разглеждане на нововъзникващи тенденции, оперативни предизвикателства и институционални реакции, включително динамики и модели, които често остават недостатъчно отразени или изцяло незабелязани в количествените данни.

Анализът се основава на преглед на международни и европейски правни и политически инструменти, стратегически документи и тематични доклади, свързани с трафика на хора, онлайн експлоатацията и управлението на платформите. Особено внимание е отделено на инструментите и насоките, разработени в рамките на Съвета на Европа и Европейския съюз, както и на развиващите се регулаторни инициативи, свързани с цифровите услуги и защитата на децата онлайн.

Освен това, статията се основава на изводи, произтичащи от пряко взаимодействие с национални органи, правоохранителни структури, представители на съдебната власт, услуги за подкрепа на жертви и организации на гражданското общество, ангажирани с превенцията на трафика, идентифицирането и защитата на жертвите. Тези изводи отразяват практически предизвикателства при разкриването, разследването и наказателното преследване на трафик, улеснен чрез технологии, както и при предоставянето на помощ на жертви, чиято експлоатация се осъществява или е подпомагана чрез дигитални средства.



Аналитичният подход е тематичен и ориентиран към проблемите, като се фокусира върху това как дигитализацията променя профилите на трафикантите и жертвите, трансформира начина на извършване на престъплението, създава и задълбочава уязвимости към експлоатация и влияе върху институционалния капацитет на различните етапи от противодействието на трафика на хора. Макар анализът да е предимно качествен и илюстративен, той цели да идентифицира модели, хоризонтални взаимовръзки и системни предизвикателства, които имат значение в различни юрисдикции, а не да оценява отделни случаи.

Накрая, статията отчита ограниченията, присъщи на експертно-базирания качествен анализ. Изводите не претендират за изчерпателност или статистическа представителност, а имат за цел да допринесат към текущите политики и професионалния дебат чрез открояване на ключови пропуски, нововъзникващи рискове и добри практики в противодействието на трафика на хора, улеснен чрез технологии.



## 4. Дигитализация на трафика на хора: предизвикателства в практиката

Дигитализацията фундаментално промени начина, по който трафикът на хора се организира, извършва и поддържа в практиката. При различните форми на експлоатация дигиталните технологии все по-често посредничат във взаимодействието между трафикантите, жертвите и трети лица, като оказват влияние върху стратегиите за набиране, механизмите за контрол и генерирането на печалби. Тези промени не заменят традиционните форми на трафик, а съществуват паралелно с тях и ги усилват, създавайки хибридни модели на експлоатация, които съчетават онлайн и офлайн елементи, включително случаи, при които жертвите се набират чрез социални мрежи или онлайн платформи и впоследствие се експлоатират в реална среда, както се посочва и в констатациите от четвъртия кръг на оценка на Експертната група за борба с трафика на хора ГРЕТА, към Съвета на Европа (GRETA, CoE).

От оперативна гледна точка дигитализацията въвежда редица практически предизвикателства за превенцията, разкриването и защитата на жертвите. Дейностите, свързани с трафик, все по-често са децентрализирани, фрагментирани между множество платформи и юрисдикции и интегрирани в легитимни онлайн услуги, което затруднява установяването на отговорност и предприемането на навременни действия. В същото време дигиталната среда променя рисковете, уязвимостта на потребителите и властовите асиметрии, като влияе както върху поведението на извършителите, така и върху преживяванията на жертвите. Следващите раздели разглеждат тези предизвикателства чрез анализ на това как дигитализацията трансформира профилите на трафикантите и жертвите, променя начина на извършване на престъплението и усложнява процесите на разкриване, идентифициране и доказване в практиката.



## 4.1. Дигитализация на профила на трафикантите

Дигитализацията значително промени профила на извършителите на трафик на хора, като улесни навлизането в тази престъпна дейност, но същевременно създаде нови форми на организация и контрол. Докато традиционно трафикът се свързваше със структурирани престъпни мрежи, изискващи физическа близост, логистичен капацитет и пряк контакт с жертвите, дигиталната среда все по-често позволява на извършителите да действат дистанционно, анонимно и “под радара”. Тази трансформация разширява спектъра от участници в трафика на хора — от организирани престъпни групи, които адаптират дейността си към онлайн среда, до по-малки или индивидуални извършители, които използват възможностите на дигиталните платформи.

Особено при случаи на сексуална експлоатация профили в социалните мрежи, приложения за съобщения и съдържание, публикувано в платформи, се използват за рекламиране на жертвите, представяне на изображения или видеа и сигнализиране за „наличност“ към потенциални клиенти чрез различни социални мрежи, платформи за стрийминг на живо и споделяне на съдържание, включително такива, които позволяват директно взаимодействие и генериране на доходи<sup>3</sup>. Тези дигитални „каталози“ позволяват на трафикантите да достигат до широка аудитория с минимални разходи, бързо да актуализират съдържанието и да го адаптират към различни пазари, като същевременно прикриват експлоатационния характер на дейността.

Дигитализацията променя и набора от умения, необходими за извършване на дейности, свързани с трафик. Освен традиционните форми на принуда и контрол, трафикантите все по-често разчитат на дигитални компетентности, включително умения за навигация в социалните мрежи, използване на алгоритмите на платформите, управление на множество онлайн идентичности и работа с крипто-



рани комуникационни инструменти. Уменията, свързани с онлайн маркетинг, изграждане на визуално съдържание, ангажиране на аудитория и извършване на финансови трансакции чрез дигитални платежни системи, се превръщат в неразделна част от тези дейности. В този контекст трафикът на хора все по-често се преплита с практики, характерни за инфлуенсър културата, онлайн рекламата и платформено базираната икономика.

В същото време дигиталната среда позволява фрагментиране и децентрализация на дейностите, свързани с трафик. Задачи като набиране, рекламиране, комуникация с клиенти, финансово управление, контрол и наблюдение на жертвите могат да бъдат разпределени между различни платформи или делегирани на посредници, което намалява необходимостта от пряко участие и ограничава риска от разкриване. В някои случаи извършителите действат изцяло дистанционно, координирайки експлоатацията през граници без физическо присъствие в държавата, където тя се осъществява, като същевременно поддържат контрол чрез постоянна дигитална комуникация, наблюдение и принудителни онлайн практики. Това разпределение на ролите затруднява идентифицирането на йерархични структури и поставя под въпрос традиционните индикатори за организирана престъпна дейност.

Дигиталните инструменти все по-често се използват и за осъществяване на нови, по-малко видими форми на принуда и контрол върху жертвите. Дигиталните форми на принуда, включително заплахи за разкриване, изнудване и злоупотреба с интимни изображения или лични данни, все по-често заместват или допълват физическата сила. В същото време постоянният мониторинг чрез приложения за съобщения, функции за споделяне на местоположение и манипулиране на онлайн идентичности позволява устойчив контрол върху поведението и движението на жертвите. Записани изображения, видеа или лични данни често се използват за засилване на зависимостта и подчинението, особено в случаи, свързани



със сексуална експлоатация и деца. Тези механизми са устойчиви, мащабни и трудни за разкриване, като същевременно оставят ограничени физически доказателства.

Накрая, дигитализацията на профила на извършителите допринася за все по-тясното преплитане на трафика на хора с други форми на онлайн престъпност. Извършителите често действат в припокриващи се среди с лица, участващи в онлайн сексуална злоупотреба, измами или други форми на киберпрестъпност, което размива границите между различните категории престъпления. Това увеличава риска случаите на трафик да бъдат неправилно квалифицирани или разглеждани изолирано, вместо да бъдат разпознати като част от продължителен процес на експлоатация

Като цяло, развитието на профила на трафикантите отразява преход от видими, локално обвързани структури към по-гъвкави, дигитално компетентни и адаптивни форми на престъпна дейност. Разбирането на тези промени е ключово за разработване на ефективни стратегии за превенция, разкриване и разследване на случаи на трафик на хора, улеснен чрез технологиите.

## 4.2. Дигитализация на профила на жертвите

Дигитализацията оказва съществено влияние върху профила на жертвите на трафик на хора, като променя моделите на уязвимост, начините на попадане в трафик и възможностите за самоидентификация. Онлайн средата все по-често се превръща в първата точка на контакт между трафикантите и жертвите, особено при деца и млади хора, но също така и при възрастни, търсещи работа, приятелски или интимни взаимоотношения или възможности за миграция. В резултат на това виктимизацията често започва в привидно легитимни или познати дигитални пространства, като се размиват границите между доброволното онлайн участие и експлоатацията.



Дигиталните платформи улесняват целенасоченото набиране, като позволяват на трафикантите да идентифицират и достигат до различни хора въз основа на възраст, пол, местоположение, социално-икономически статус, миграционен статус или заявени интереси. Профилите в социалните мрежи, онлайн общностите и приложенията за съобщения предоставят достъп до значителен обем лична информация, голяма част от която се споделя доброволно от потребителите, които не осъзнават потенциалните негативни последици в дългосрочен план. Възприеманата анонимност и усещането за сигурност в онлайн средата могат да намалят индивидуалната предпазливост, като водят до споделяне на лични данни, изображения, предпочитания и уязвимости, които допринасят за изграждането на видим дигитален профил. Този самогенериран дигитален отпечатък оформя начина, по който хората се възприемат от другите, и може неволно да увеличи тяхната уязвимост към лица, търсещи потенциални жертви. Трафикантите използват тази информация, за да адаптират стратегиите си за набиране, да изградят доверие и постепенно да въвлекат жертвите в зависимост и експлоататорски отношения. В този процес често се прилагат манипулативни техники, включително емоционално въздействие, създаване на привидна близост и доверие, както и въвличане на жертвите в създаване или споделяне на интимно съдържание, което впоследствие може да бъде използвано за изнудване и контрол. В този контекст процесите на груминг могат да се развиват продължително във времето и през множество платформи, което ги прави особено трудни за разпознаване и прекъсване.

Дигитализацията на процеса на набиране допринася и за промени в начина, по който жертвите възприемат собственото си участие и навлизане в експлоатация. В някои случаи хората първоначално възприемат участието си като доброволно, като приключение или нещо временно, особено когато експлоатацията е представена като работа, самостоятелна дейност или онлайн активност. Това е особено видимо при случаи на сексуална експлоатация, осъществявана



чрез дигитални платформи, където границата между създаване на съдържание, комерсиален секс и експлоатация може да изглежда размита. Тези динамики могат да забавят, изкривят или дори да предотвратят самоидентифицирането като жертва, като по този начин намаляват вероятността за търсене на помощ или включване в механизми за подкрепа.

Дигиталната среда създава специфични условия, при които жертвите развиват форми на зависимост и подчинение, които са по-малко видими, но също толкова въздействащи и принудителни. Постоянната онлайн комуникация, възможността за непрекъснато наблюдение и заплахата от разпространение на интимни изображения, видеа или лична информация засилват усещането за страх, срам и изолация. За много жертви, особено деца и млади хора, преживяването на експлоатацията се съчетава с объркване, чувство за вина и постепенно нормализиране на ситуацията, което допълнително затруднява разпознаването ѝ като насилие. В този контекст жертвите често не се самоидентифицират като такива, изпитват силни притеснения от разкриване и срещат сериозни вътрешни бариери при търсенето на помощ или противопоставянето на извършителя.

Дигитализацията влияе и върху видимостта и идентифицирането на жертвите от страна на институциите и услугите за подкрепа. Жертвите, чиято експлоатация се осъществява предимно онлайн, може да имат ограничен физически контакт с извършителите, да не бъдат държани на едно конкретно място и да не отговарят на класическите индикатори за трафик на хора. Често дори да не знаят със сигурност кой ги експлоатира. Това поставя предизвикателства пред утвърдените практики за идентификация и увеличава риска жертвите да останат неразпознати или престъплението срещу тях да бъде неправилно класифицирано, особено когато експлоатацията се преплита с други форми на онлайн злоупотреба или неформална икономическа дейност.



В обобщение, дигитализацията на профила на жертвите отразява преход към по-малко видими, по-фрагментирани и често вътрешно нормализирани форми на експлоатация. Разбирането на начина, по който дигиталната среда оформя уязвимостта, автономността и контрола, е от съществено значение за разработването на ефективни мерки за превенция, идентифициране и подкрепа, съобразени с реалния опит на жертвите в случаите на трафик на хора, улеснен чрез технологии.

#### **4.3. Modus Operandi на трафика на хора, улеснен от технологиите**

Дигитализацията трансформира начина на извършване (modus operandi) на трафика на хора, като позволява експлоатацията да се осъществява чрез обичайни онлайн дейности и услуги. Вместо да разчита единствено на физическо придвижване или задържане, трафикът, улеснен чрез технологии, често се развива като поредица от дигитално медиирани действия, обхващащи множество платформи, юрисдикции и етапи на експлоатация. Експертната група за борба с трафика на хора (ГРЕТА)<sup>4</sup> към Съвета на Европа, отбелязва, че информационните и комуникационните технологии (ИКТ) се използват във всички етапи на процеса на трафик — особено при набирането и контрола на жертвите — като същевременно подчертава, че наличната доказателствена база исторически е фрагментирана и неравномерна между различните държави.

Набирането все по-често започва в онлайн среда, включително чрез социални мрежи, приложения за съобщения, платформи за запознанства и онлайн обяви за работа. Мониторингът и изследванията на ГРЕТА показват, че набирането чрез социални мрежи и приложения за запознанства е повтарящ се модел, като ИКТ улесняват идентифицирането, локализирането и осъществяването на контакт с потенциални жертви. Европол също отбелязва, че трафикът



на хора все повече се развива като „бизнес модел“, в който онлайн компонентът е съществена част от начина на действие на извършителите, позволявайки им да действат зад „виртуален щит“, като същевременно оставят дигитални следи. С течение на времето трафикантите обикновено преместват комуникацията от публични или полу-публични пространства към частни или криптирани канали, което затруднява ранното разкриване и ограничава ефективността на изолирани интервенции.

Самата експлоатация също все по-често се осъществява чрез дигитални средства. При случаи на сексуална експлоатация жертвите могат да бъдат принуждавани да създават изображения, видеа или съдържание на живо (live-stream), докато трафикантите контролират разпространението, „рекламирането“, ценообразуването и взаимодействието с клиенти. Изследване на ГРЕТА към Съвета на Европа отбелязва, че ИКТ се използват не само за набиране, но и за упражняване на контрол и натиск върху жертвите, включително чрез поддържане на контакт дори след напускане на експлоатацията с цел сплашване и възпрепятстване на сигнализирането. Технологии влияят и върху динамиката на трудовата експлоатация чрез дигитална координация, дистанционен контрол и посредничество чрез платформи, особено в неформални или несигурни форми на заетост — процеси, които ICAT определя като част от по-широки технологично обусловени промени в тенденциите, предизвикателствата и възможностите, свързани с трафика.

Механизмите за контрол при трафика, улеснен чрез технологии, все по-рядко се основават на физическо задържане и все по-често на психологически натиск, наблюдение и дигитална зависимост. Постоянната свързаност позволява наблюдение в реално време чрез приложения за съобщения, функции за споделяне на местоположение и непрекъсната дигитална комуникация. Заплахите, свързани с разпространение на интимни изображения или лични данни, функционират като средство за принуда, засилвайки страха и подчине-



нието — динамики, които съответстват на анализа на ГРЕТА относно контрола, осъществяван чрез ИКТ.

Дигитализацията съществено променя и трафика с цел принудително извършване на престъпления — област, която все по-често се откроява както от разследващите органи, така и от мониторинговите механизми. Данните на Европол и ГРЕТА показват, че деца и уязвими възрастни все по-често се набират онлайн за дейности като принудителни кражби, участие в разпространение на наркотици, злоупотреби със социални помощи, онлайн измами и други форми на криминална експлоатация, често чрез социални мрежи, приложения за съобщения или онлайн игри. Дигиталните инструменти позволяват дистанционно даване на инструкции, наблюдение и контрол, като дават възможност на трафикантите да управляват престъпната дейност, минимизирайки директния контакт и риска от разкриване. ГРЕТА отбелязва, че дигиталната комуникация се използва за поддържане на постоянен контрол върху жертвите, даване на инструкции, наблюдение на „изпълнението“ и налагане на подчинение чрез заплахи, манипулиране на дългове или злоупотреба с лични данни. ICAT допълва, че технологиите позволяват бързо адаптиране и мащабиране на трафика с цел криминална експлоатация, като същевременно допринасят за погрешното третиране на жертвите като извършители. Тези дигитално медириани процеси усложняват разкриването и идентифицирането на жертвите, тъй като експлоатираните лица често се възприемат предимно като извършители, което води до неразпознаване на жертвите и ограничен достъп до защита и подкрепа.

Дигитализацията допълнително размива границите между сексуалната експлоатация на деца, нарастващото разпространение на материали със сексуално насилие над деца (CSAM) и трафика на деца с цел сексуална експлоатация. Европол последователно отчита значително увеличение на онлайн сексуалната експлоатация на деца, включително съдържание, създадено от самите деца при условия



на принуда, манипулация или груминг. Макар този тип съдържание често да се разглежда основно в рамките на сексуалното насилие над деца, ГРЕТА подчертава, че тези процеси често се преплитат с трафик, особено когато създаването, разпространението или монетизирането на изображения и видеа се организира или контролира от трети лица. В случаи на трафик, улеснен чрез технологии, самогенерираното съдържание може да се превърне във входна точка към продължителна експлоатация, като впоследствие се използва за контрол, изнудване или многократна злоупотреба от различни извършители. Тези припокриващи се динамики поставят под въпрос традиционните правни и оперативни разграничения между престъпления, свързани с онлайн сексуалната експлоатация на деца и трафика на хора, увеличавайки риска от фрагментирани реакции, неправилна класификация и недостатъчно разпознаване на специфичните нужди от закрила на децата жертви на трафик.

Финансовите потоци, свързани с трафика, също се влияят от дигитализацията. Европол подчертава, че ключови елементи от престъпните процеси все по-често се преместват онлайн, включително платежните системи, като дигитализацията подпомага скоростта, обхвата и прикриването при тежката и организирана престъпност. В контекста на трафика това се изразява в по-широко използване на онлайн транзакции, плащания чрез платформи и разпокъсване на финансовите потоци през различни държави, което създава сериозни практически затруднения за финансовите разследвания и отнемането на активи.

В обобщение, начинът на извършване на трафика, улеснен чрез технологии, отразява преход към по-децентрализирани, адаптивни и устойчиви форми на експлоатация. ГРЕТА подчертава необходимостта правоохранителните органи и системите на наказателното правосъдие да се адаптират към тези структурни промени в начина, по който хората взаимодействат и как се осъществява трафикът, докато Европол акцентира върху нарастващата централна роля на он-



лайн компонентите в тези дейности. Разбирането на тези развиващи се модели е от ключово значение за разработването на ефективни разследващи стратегии, прекъсването на експлоататорските мрежи и своевременното идентифициране и защита на жертвите на практика. Последните данни на Нидерландския национален докладчик по трафика на хора и сексуалното насилие над деца допълнително подчертават нарастващото участие на деца в криминална експлоатация и ролята на онлайн средата при набирането и контрола.

Нарастващото припокриване между трафика на хора, сексуалната експлоатация на деца и престъпленията, свързани с материали (снимки и видео) съдържащи сексуална експлоатация, поставя по-широки въпроси относно адекватността на съществуващите правни и оперативни подходи към класификацията и разследването на престъпления в дигитална среда. Макар тези престъпления да се регулират от различни правни рамки, дигитализацията размива традиционните граници между тях, създавайки ситуации, при които един случай може едновременно да включва елементи на трафик, онлайн сексуална злоупотреба и създаване или разпространение на материали съдържащи сексуална експлоатация на деца. На практика това често води до разследващи стратегии, които приоритизират престъплението, което е по-лесно за доказване или по-вероятно да доведе до успешна присъда, вместо да отразяват пълния обхват на експлоатацията. Това повдига ключови въпроси дали е необходимо допълнително развитие на правните рамки или дали следва да се постави по-силен акцент върху гъвкави, ориентирани към жертвите и интегрирани разследвания, които позволяват паралелно разглеждане на множество престъпления. Преодоляването на подходи, изискващи избор на едно престъпление, и преминаването към признаване на съвместното съществуване на различни форми на експлоатация в рамките на един случай, може да се окаже ключово за гарантиране на отчетност, избягване на фрагментирани производства и осигуряване на цялостна защита на жертвите.



#### **4.4. Предизвикателства при разкриването, идентифицирането и доказването на престъплението**

Дигитализацията на трафика на хора въведе съществени предизвикателства пред разкриването, идентифицирането и събирането на доказателства, като разкри ограниченията на традиционните разследващи подходи, основани на физически индикатори, териториално присъствие и линейни наративи за престъплението. Трафикът, улеснен чрез технологии, често е децентрализиран, транснационален и интегриран в легитимни онлайн среди, което затруднява ранното му разпознаване и установяването на ясни връзки между извършители, жертви и експлоатацията.

Едно от основните предизвикателства е идентифицирането на жертвите. Жертвите, чиято експлоатация се осъществява чрез дигитални платформи, може да не бъдат физически задържани, да имат ограничен пряк контакт с трафикантите и да не се самоопределят като жертви, особено когато експлоатацията е представена като доброволна онлайн дейност или неформална заетост. Както подчертава ГРЕТА, случаите на трафик, улеснен чрез технологии, често остават недостатъчно идентифицирани, като жертвите остават невидими за институциите или се класифицират като други форми на злоупотреба или престъпна дейност. Този риск е особено висок при деца и при жертви, експлоатирани с цел принудително извършване на престъпления, които често се третират от разследващите предимно като извършители, а не като жертви на престъпление.

Разкриването допълнително се усложнява от това, че дигиталните доказателства са разпръснати между различни платформи и услуги, често в различни юрисдикции. Дейностите, свързани с трафик, могат да бъдат разпределени между множество онлайн услуги, включително социални мрежи, приложения за съобщения, платежни системи и облачни услуги, често разположени в различни юрисдикции. Европол многократно подчертава, че макар дигитализацията да оставя



използваеми данни и следи, достъпът до тях, тяхното съхраняване и свързване остават оперативно сложни. Забавянията при запазването на данни, трудностите при трансграничното сътрудничество и непоследователната реакция на платформите могат съществено да възпрепятстват разследванията.

Предизвикателствата, свързани с доказването, са тясно свързани и с класификацията на престъпленията. Когато даден случай включва припокриващи се елементи на трафик, сексуална експлоатация, престъпления, свързани с онлайн сексуална експлоатация на деца, или принудително извършване на престъпления, разследващите стратегии често приоритизират престъплението, което се възприема като по-лесно за доказване или по-вероятно да доведе до осъдителна присъда. Макар тези решения да са продиктувани от практически съображения, те крият риск от стесняване на доказателствения обхват, фрагментиране на случаите и прикриване на продължителния характер на експлоатацията. ГРЕТА отбелязва, че трафикът, улеснен чрез технологии, често остава недостатъчно отразен в наказателните производства, отчасти поради трудности при достигане на доказателствения праг за специфичните състави на трафик в дигитална среда.

Оценката на принудата, контрола и експлоатацията поставя допълнителни предизвикателства в онлайн среда. Дигиталните форми на контрол — като постоянна комуникация, наблюдение, заплахи за разпространение на съдържание или злоупотреба с интимни изображения — може да са по-малко видими от физическото насилие, но са също толкова ефективни. Въпреки това тези форми на принуда невинаги се разпознават адекватно в рамките на съществуващите доказателствени подходи, особено когато правните тълкувания продължават да поставят акцент върху физическите индикатори за сила или задържане. Това може да доведе до подценяване на вредата и до неправилна правна квалификация на престъплението.



Накрая, институционалният капацитет и експертизата играят решаваща роля. Ефективното разкриване и разследване на трафика, улеснен чрез технологии, изисква специализирани умения в областта на дигиталната криминалистика, онлайн разследванията и взаимодействието с платформи, както и устойчиво сътрудничество между правоохранителните органи, прокуратурата, услугите за подкрепа на жертви и технологичните компании. Както ГРЕТА, така и Европол подчертават, че пропуските в обучението, ресурсите и междуйнституционалната координация продължават да ограничават способността на институциите да реагират ефективно на дигитално медираните форми на трафик.

В обобщение, тези предизвикателства показват, че дигитализацията не просто добавя допълнителна сложност към съществуващите случаи на трафик, а фундаментално променя условията, при които експлоатацията се разкрива, разследва и преследва наказателно. Преодоляването им изисква адаптивни разследващи практики, гъвкави правни интерпретации и интегрирани подходи, способни да обхванат пълния обхват на експлоатацията в случаи на трафик, улеснен чрез технологии.



## 5. Въздействието на дигитализацията върху жертвите

Дигитализацията оказва съществено влияние върху преживяванията на жертвите на трафик на хора, като променя както пътищата им към експлоатация, така и възможностите им да потърсят помощ и да излязат от ситуацията на насилие. Онлайн средата разширява обхвата на действие на трафикантите и увеличава излагането на риск, особено при деца и млади хора, като едновременно с това променя начина, по който жертвите възприемат, преживяват и реагират на експлоатацията.

Интеграцията на дигиталните технологии в ежедневието създава нови пространства, в които уязвимостите могат да възникват и да бъдат използвани, често по начини, които са по-малко видими и по-трудни за разпознаване. Набирането, манипулацията и контролът могат да се осъществяват дистанционно, постепенно и чрез множество платформи, което намалява вероятността жертвите или хората около тях да разпознаят ситуацията като експлоатация в ранен етап. В резултат на това границите между доброволно взаимодействие, рисково поведение и принуда все повече се размиват.

В същото време дигитализацията прави експлоатацията по-устойчива, мащабируема и по-инвазивна. Жертвите могат да бъдат подложени на непрекъснато наблюдение, многократно излагане и постоянно разпространение на съдържание, свързано с експлоатацията, което разширява вредите отвъд непосредствената ситуация на експлоатация. Тези процеси не само задълбочават въздействието върху жертвите, но и затрудняват тяхното дистанциране от ситуацията, търсенето на помощ и възстановяването на автономността.

### 5.1. Онлайн уязвимост и динамика на експлоатацията

Дигитализацията създава и усилва уязвимостите чрез осигуряване на постоянен достъп до потенциални жертви и възможности за



целенасочено набиране. Онлайн средата позволява събиране и използване на лична информация, модели на поведение и социални връзки, което улеснява изграждането на доверие и постепенно въвличане в отношения на зависимост и експлоатация.

Дигиталните технологии позволяват процесите на манипулация и контрол да се развиват поетапно и в различни онлайн пространства, което затруднява тяхното разпознаване. В този контекст границите между доброволно участие, рисково поведение и експлоатация могат да бъдат неясни, особено когато взаимодействието се възприема като част от нормална онлайн активност.

Дигиталната среда също така създава условия за форми на психологически контрол и зависимост, които са по-малко видими от физическата принуда, но не по-малко ефективни. Манипулацията, емоционалният натиск, заплахите за разкриване и злоупотребата с лични данни могат да създадат устойчив страх и подчинение, дори при липса на пряко физическо насилие. В такива ситуации жертвите могат да изпитват объркване, чувство за вина или намалено възприемане на вредата, което допълнително забавя разпознаването на експлоатацията и търсенето на помощ.

Дигитализацията влияе и върху социалния контекст на експлоатацията. Жертвите могат да останат физически част от своите семейства, общности или социални среди, като едновременно с това бъдат експлоатирани онлайн, което затруднява разкриването на ситуацията от страна на околните. Тази динамика на „скрито на видно място“ ограничава възможностите за външна намеса и засилва изолацията, особено когато жертвите поддържат привидно нормален начин на живот.

В обобщение, преживяванията на жертвите при трафик, улеснен чрез технологии, следва да се разглеждат като комплексни, динамични и често нелинейни. Това изисква подходи, които надхвърлят традиционните индикатори и отчитат специфичните рискове и вреди,



свързани с дигиталната среда. В този контекст укрепването на дигитално-медийната грамотност и устойчивостта сред деца, млади хора и други уязвими групи е ключов елемент от превенцията, като подпомага разпознаването на рисковете, критичната оценка на онлайн взаимодействията и своевременното търсене на подкрепа.

## **5.2. Рискове от вторична виктимизация и предизвикателства пред закрилата**

Дигитализацията създава нови рискове от вторична виктимизация и допълнителни бариери пред идентифицирането и закрилата на жертвите. Постоянството и потенциално неконтролируемостта на разпространение на онлайн съдържание, включително изображения и видеа, могат да доведат до траен страх, срам и психологическа травма, което възпира жертвите да търсят помощ или да сътрудничат на институциите. В много случаи жертвите се опасават, че сигнализирането ще доведе до допълнително разпространение на съдържанието, което засилва мълчанието и нежеланието за разкриване.

В същото време жертвите, чиято експлоатация се осъществява предимно онлайн, често не проявяват традиционните индикатори за трафик. Те може да не са физически задържани, да имат ограничен или никакъв пряк контакт с извършителите и дори да не знаят със сигурност тяхната самоличност. Това затруднява идентифицирането и увеличава риска жертвите да останат неразпознати или да бъдат неправилно класифицирани в рамките на наказателното правосъдие.

Дигитализацията влияе и върху естеството на доказателствата и тяхното използване в процеса, което може неволно да доведе до вторична виктимизация. Жертвите могат да бъдат многократно излагани на съдържание, свързано с експлоатацията им, по време на разследвания и съдебни производства, докато използването на дигитални доказателства — като изображения, видеа или комуника-



ции — може да удължи травмата и да засили усещането за загуба на контрол. Освен това трансграничният характер на тези случаи може да доведе до забавяния, фрагментирани процедури и ограничен достъп до информация, което допълнително отслабва доверието в институциите и системите за подкрепа.

Допълнително, жертвите, въввлечени в престъпна дейност в резултат на експлоатация — особено деца — често се третират като извършители, а не като жертви, което създава сериозни бариери пред тяхната закрила. Това е особено характерно за случаи на принудително извършване на престъпления, включително такива, улеснени чрез технологии, при които връзката между експлоатацията и извършеното деяние не винаги се разпознава. В резултат жертвите могат да бъдат подложени на наказателно преследване, задържане или административни санкции, вместо да получат защита и подкрепа.

Преодоляването на тези предизвикателства изисква по-гъвкави и ориентирани към жертвите подходи за идентификация, които отчитат комплексния и често непоследователен характер на експлоатацията в дигитална среда. Необходими са също така мерки за предотвратяване на вторична виктимизация в рамките на разследващите и съдебните процеси, включително внимателно боравене с дигитални доказателства, прилагане на подходи, основани на разбирането за травмата и засилена координация между органите на наказателното правосъдие и услугите за подкрепа на жертвите.



## 6. Глобални тенденции и нововъзникващи модели

Дигитализацията на трафика на хора отразява по-широки глобални тенденции в развитието на организираната престъпност, при които технологиите позволяват по-голям мащаб, по-висока скорост и по-голяма адаптивност. Мрежите на трафикантите все по-често действат едновременно в дигитална и физическа среда, създавайки хибридни и транснационални модели на експлоатация, които поставят под въпрос традиционните подходи за разкриване и реакция. Тези процеси не са изолирани, а са част от по-широка трансформация към по-децентрализирани, мрежови и технологично обусловени форми на престъпна дейност.

В глобален план дигитализацията допринася за разширяване на моделите на трафик, като позволява на извършителите да достигат до по-широк кръг от потенциални жертви, да действат едновременно на множество пазари и бързо да адаптират методите си в отговор на действията на правоохранителните органи. Все по-ясно се наблюдава и сближаване между трафика на хора и други форми на организирана престъпност, включително киберпрестъпления, финансови престъпления и онлайн сексуална експлоатация, което допълнително усложнява класифицирането на престъплението и институционалният отговор.

### 6.1. Трансграничен трафик и експлоатация, осъществявани чрез онлайн платформи

Трафикът на хора, улеснен чрез технологии, по своята същност е транснационален. Онлайн платформите позволяват на извършителите да набират, контролират и експлоатират жертви едновременно в множество юрисдикции, често без физическо присъствие в държавата, в която се осъществява експлоатацията. Това създава съществени предизвикателства за правоохранителните и съдебните



органи, особено по отношение на юрисдикцията, събирането на доказателства и трансграничното сътрудничество.

В същото време дигиталната инфраструктура позволява на извършителите да действат чрез разпределени мрежи, а не чрез ясно структурирани йерархии, като различни участници изпълняват специализирани роли в различни държави и платформи. Тази фрагментация затруднява идентифицирането на организирани престъпни групи и поставя под въпрос традиционните разследващи подходи, основани на ясно очертани организационни структури. Допълнително, извършителите все по-често използват частни или затворени онлайн групи, включително комуникационни канали с ограничен достъп или временно съществуване, за да координират дейността си и да избягват разкриване, като понякога се възползват от периоди с по-ниска степен на наблюдение или ограничен институционален капацитет, като например извън работно време или през почивни дни.

Екосистеми, функциониращи чрез онлайн платформите, също така позволяват бързо разпространение на съдържание свързано с експлоатацията и координация на престъпни дейности в широк мащаб. Използването на социални мрежи, приложения за съобщения, онлайн пазари и криптирани комуникационни канали улеснява фрагментирането на дейностите, свързани с трафик, като едновременно с това свързва извършители, жертви и „клиенти“ в сложни дигитални мрежи. В някои случаи платформите функционират като посредници, които улесняват контакта, договарянето и самата експлоатация, размивайки границите между легитимни и незаконни дейности.

Освен това дигитална среда, която може да е с различна юрисдикция може да създаде пропуски в закрилата, когато жертвите се набират в една държава, експлоатират се в друга и се контролират от трета юрисдикция. Тези динамики затрудняват достъпа до помощ, забавят идентифицирането и могат да доведат до фрагментирани или непоследователни реакции между държавите.



## 6.2. Технологиите изпреварват регулаторните и институционалните отговори

Ключова нововъзникваща тенденция е нарастващото разминаване между темпа на технологично развитие и способността на регулаторните и институционалните рамки да реагират ефективно. Макар правните инструменти все по-често да отчитат ролята на дигиталните технологии в трафика на хора, оперативният капацитет, разследващите инструменти и механизмите за трансгранично сътрудничество често изостават.

Нововъзникващите технологии, включително изкуствен интелект, инструменти за запазване на анонимност, включително криптирани комуникационни системи, продължават да променят средата на експлоатация, създавайки нови възможности за извършителите и едновременно усложнявайки разкриването и наказателното преследване. В същото време трафикантите демонстрират висока степен на адаптивност, като бързо променят платформи, инструменти и методи в отговор на регулаторни мерки и действия на правоохранителните органи.

Допълнително предизвикателство е фрагментацията на правните и регулаторните подходи между различните юрисдикции. Различията в законодателството, режимите за защита на данните и процесуалните правила могат да възпрепятстват своевременния достъп до дигитални доказателства и да ограничат ефективното сътрудничество между институциите. Участието на частния сектор, и по-специално на дигиталните платформи, допълнително усложнява въпросите, свързани с отговорностите, отчетността и достъпа до данни.

Ограничената наличност на данни и несъответствията в класификацията допълнително затрудняват цялостното разбиране на трафика на хора, улеснен чрез технологии. Много случаи остават неидентифицирани или се регистрират под различни категории



престъпления, което прави трудно оценяването на мащаба и характеристиките на явлението. В резултат на това политическите отговори често се основават на непълна или фрагментирана информация.

Преодоляването на тези предизвикателства изисква постоянна адаптация, инвестиции в експертиза и по-тесна интеграция между правните, технологичните и политическите подходи както на национално, така и на международно ниво. Необходимо е също така подобряване на събирането на данни, развитие на аналитичния капацитет и устойчив обмен на практики, за да се гарантира ефективност на отговорите в условията на бързо променяща се дигитална среда.



## 7. Добри практики и нововъзникващи подходи

### 7.1. Междуинституционални и многостранни подходи

Противодействието на трафика на хора, улеснен чрез технологии, все по-често изисква координирани реакции, които надхвърлят традиционните действия на правоохранителните органи. Добри практики, наблюдавани в Европа, подчертават значението на структурираното сътрудничество между правоохранителните органи, прокуратурата, службите за закрила на детето, организациите за подкрепа на жертви, регулаторните органи и технологичните компании. Подобно сътрудничество е от ключово значение за обхващане на пълния мащаб на дигитално медираната експлоатация, особено в случаи, включващи припокриващи се престъпления като трафик на хора, онлайн сексуално насилие и принудително извършване на престъпления.

Констатациите от мониторинга на ГРЕТА подчертават, че ефективните реакции зависят от ранния обмен на информация и съвместния анализ между различни сектори. Мултидисциплинарните екипи, които съчетават разследващ, прокурорски и експертен капацитет за подкрепа на жертви, се доказват като особено ценни при сложни случаи, в които едновременно трябва да се адресират дигитални доказателства, идентификация на жертви и тяхната защита. Тези подходи допринасят за избягване на фрагментирано разглеждане на случаите и намаляват риска жертвите да бъдат неправилно идентифицирани или изключени от механизми за подкрепа поради ограничена правна квалификация на престъплението.

Наблюдаваните практики показват и нарастващата роля на сътрудничеството с технологичните компании и доставчиците на платформи. Макар да съществуват предизвикателства, свързани с достъпа до данни, времето за реакция и юрисдикционните огра-



ничения, структурирани механизми за взаимодействие — като определени контактни точки за правоохранителните органи, системи за „доверени податели“ (trusted flaggers)<sup>5</sup> и специфични за платформите канали за докладване — подобряват способността на институциите да идентифицират и съхраняват релевантни дигитални доказателства. Европол подчертава, че проактивното сътрудничество с частния сектор е все по-необходимо за прекъсване на трафикантски дейности, които в значителна степен разчитат на онлайн услуги и дигитална инфраструктура.

Изграждането на капацитет остава ключов елемент на ефективните междуинституционални подходи. Добри практики включват специализирани обучения за разследващи органи, прокурори и съдии по теми като трафик, улеснен чрез технологии, дигитални форми на принуда и използване на онлайн доказателства. Също толкова важно е интегрирането на подход, ориентиран към жертвите, в оперативната дейност, така че разследващите действия да не задълбочават вредите или да създават допълнителни бариери пред разкриването и защитата.

Предвид по същество транснационалния характер на трафика, улеснен чрез технологии, международното сътрудничество е критичен елемент на ефективния отговор. Дигиталната среда позволява на извършителите да действат едновременно в множество юрисдикции, което прави своевременния обмен на информация, съвместните разследвания и координираните действия от съществено значение. Съществуващите механизми, включително сътрудничеството чрез Европол, взаимната правна помощ и съвместните екипи за разследване, играят важна роля, но предизвикателства остават по отношение на достъпа до данни, различията в правните рамки и процедурните забавяния. Поради това укрепването на международното сътрудничество, включително с държави извън Европейския съюз, е от ключово значение за ефективното разследване, наказателно преследване и защита на жертвите в случаи на дигитално медиран трафик.



## 7.2. Механизми за докладване и специализирани отговори

Ефективните механизми за сигнализиране и насочване са от съществено значение за ранното разкриване на трафик, улеснен чрез технологии, особено в случаи, свързани с деца и онлайн експлоатация. Добри практики все по-често подчертават необходимостта от достъпни и добре популяризирани канали за подаване на сигнали, които позволяват на жертви, специалисти и трети лица да съобщават за съмнения за експлоатация в дигитална среда. Това включва онлайн инструменти за докладване, горещи линии<sup>6</sup> и функции за сигнализиране, интегрирани в платформите, които могат да уловят индикатори за трафик наред с други форми на онлайн злоупотреба.

Специализираните реакции се доказват като особено важни в случаи, при които експлоатацията се осъществява основно онлайн или има трансграничен характер. Специализирани звена в рамките на правоохранителните органи, прокурори със специфична експертиза и служби за закрила на детето с дигитални компетентности са по-добре подготвени да оценяват сложни случаи, включващи множество платформи и припокриващи се престъпления. ГРЕТА отбелязва, че липсата на такива специализирани структури често води до забавяния, неправилна класификация и пропуснати възможности за защита на жертвите, особено при случаи, улеснени чрез технологии<sup>7</sup>.

Добри практики включват и интегрирането на механизмите за сигнализиране в по-широки системи за насочване и подкрепа на жертви. Осигуряването на това сигналите за онлайн експлоатация да водят както до разследващи действия, така и до предприемане на защитни мерки, спомага за преодоляване на разрива между разкриването и оказването на помощ. При случаи на трафик на деца, тясната координация между правоохранителните органи, органите за закрила на детето и специализираните неправителствени организации е от ключово значение, за да се гарантира, че децата се разпознават като жертви на трафик и получават адекватна подкрепа, независимо от начина, по който експлоатацията е била разкрита.



Накрая, нововъзникващите подходи подчертават значението на адаптивността. С бързото развитие на дигиталните платформи, комуникационните инструменти и моделите на експлоатация, механизмите за сигнализиране и институционалните реакции трябва да бъдат редовно преглеждани и актуализирани. Гъвкавите процедури, непрекъснатото обучение и устойчивият диалог между заинтересованите страни са ключови за гарантиране на ефективността на добрите практики в условията на нарастваща дигитализация.

### **7.3. Подходи, ориентирани към превенция и изграждане на устойчивост**

Превенцията на трафика на хора, улеснен чрез технологии, изисква устойчиви инвестиции в изграждането на устойчивост сред деца, млади хора и други уязвими групи в дигитална среда. Добри практики все по-често поставят акцент върху превантивни стратегии, които адресират онлайн рисковете, властовите асиметрии и динамиката във видовете експлоатацията още преди настъпването на вредата. Това включва инициативи, насочени към повишаване на дигитално-медийната грамотност, критичното мислене и осведомеността относно онлайн груминг и манипулация, както и насърчаване на по-безопасно онлайн поведение, без да се прехвърля отговорността върху потенциалните жертви.

Модели като националните центрове за безопасен интернет и специализираните горещи линии представляват ценни примери за интегрирани рамки за превенция. Чрез образование, повишаване на осведомеността, консултиране и механизми за сигнализиране, тези структури допринасят за ранното идентифициране на рискове и за ограничаването на вредно онлайн съдържание и поведение. Тясното им сътрудничество с училища, организации на гражданското общество, правоохранителни органи и технологични компании позволява прилагането на цялостен подход към онлайн безопасността, който е особено релевантен в контекста на трафика на деца и онлайн



сексуалната експлоатация.

Целенасочените превантивни мерки са също толкова важни и за възрастни и групи с повишена уязвимост, включително мигранти, деца в алтернативна грижа, млади хора, напускащи институционална среда, и лица, изправени пред социално-икономическа изолация. Индивидуализирани подходи, базирани на работа в общността и културно съобразени информационни кампании, показват добри резултати за намаляване на излагането на риск от онлайн набиране и експлоатация, особено когато са съчетани с достъпни услуги за подкрепа.

Публично-частните партньорства играят все по-важна роля в усилията за превенция. Сътрудничеството между публични институции, гражданското общество и доставчици на дигитални услуги може да подобри оценката на риска, модерирването на съдържание, механизмите за сигнализиране и разпространението на превантивна информация. Участието на технологичните компании в идентифицирането на системни рискове, подкрепата на кампании за осведоменост и улесняването на потребителското сигнализиране допринася за изграждането на по-проактивна превантивна среда, като същевременно подчертава споделената отговорност за справяне с експлоатацията, улеснена чрез технологии.

В обобщение, подходите, ориентирани към превенция, допълват разследващите и защитните механизми, като адресират основните фактори, които позволяват възникването на трафик, улеснен чрез технологии. Укрепването на устойчивостта, насърчаването на информирано онлайн поведение и изграждането на координирани превантивни стратегии са ключови елементи на цялостния отговор в условията на нарастваща дигитализация.

Нарастващо внимание се обръща и на използването на изкуствен интелект (ИИ) и автоматизирани инструменти за подпомагане на



разкриването и превенцията на трафика на хора, улеснен чрез технологии. Системи, базирани на ИИ, вече се използват от дигиталните платформи за идентифициране на модели, свързани с материали със сексуално насилие над деца (CSAM), координирани експлоаторски мрежи и подозрително поведение на потребители в широк мащаб. Дигитални криминалистични инструменти, традиционно използвани в разследвания, свързани с CSAM, все по-често се прилагат и в случаи на трафик на хора за анализ на онлайн комуникации, извличане и съхраняване на дигитални доказателства, както и за подпомагане на идентифицирането на жертви и извършители.

В контекста на трафика подобни инструменти имат потенциал да подпомогнат ранното откриване на рискове, да идентифицират модели на набиране, да сигнализируют за повтарящи се индикатори за експлоатация и да подпомогнат приоритизирането на сигналите. Освен това някои държави, включително Нидерландия, Германия, Норвегия и Обединеното кралство, използват уеб-кроулери и други автоматизирани инструменти за откриване на съдържание, свързано с трафик на хора, включително обяви, свързани със сексуална експлоатация, като по този начин подпомагат проактивните разследвания и идентифицирането на жертви.

В същото време ефективността на тези технологии зависи от прозрачността, качеството на използваните данни и наличието на постоянен човешки контрол. При липса на адекватни гаранции съществува риск ИИ системите да възпроизвеждат съществуващи пристрастия, да пропускат по-малко видими форми на експлоатация или да генерират фалшиви сигнали, които могат да навредят на жертвите. Поради това добрите практики подчертават, че ИИ следва да се използва като допълващ инструмент в рамките на по-широки разследващи, превантивни и ориентирани към жертвите подходи, а не като самостоятелно решение.



## 8. Политически изводи и препоръки

Дигитализацията на трафика на хора има съществени последици за политиките, законодателството и практиката. Макар съществуващите правни рамки да осигуряват стабилна нормативна основа за противодействие на трафика, анализът в настоящата статия показва, че експлоатацията, улеснена чрез технологии, все по-често поставя под въпрос традиционните разбирания за класификацията на престъпленията, идентифицирането на жертвите, събирането на доказателства и институционалните реакции. Преодоляването на тези предизвикателства изисква не само спазване на правните норми, но и адаптивни, координирани и ориентирани към жертвите подходи, способни да отговорят на динамично развиващата се дигитална среда.

На първо място, политическите отговори следва да поставят акцент върху гъвкавостта в разследването и наказателното преследване. Когато фактите сочат наличие на различни форми на експлоатация едновременно — като трафик на хора, сексуална (онлайн) експлоатация на деца, или принудително извършване на престъпления — институциите следва да бъдат насърчавани да прилагат паралелни или комбинирани разследващи подходи, вместо да ограничават случаите до една правна квалификация поради процесуални съображения. Това изисква ясни оперативни насоки, координация между прокуратурата и повишена чувствителност на съдебната система към дигитално медираните форми на принуда и контрол.

На второ място, укрепването на институционалния капацитет остава от съществено значение. Правоохранителните органи, прокурорите и съдиите се нуждаят от специализирано обучение, свързано с трафика на хора, улеснен чрез технологии, включително за моделите на онлайн набиране, дигиталните механизми на контрол и специфични доказателствени предизвикателства в дигитална среда. Инвестициите в дигитална криминалистика, механизми за тран-



сгранично сътрудничество и своевременен достъп до данни, съхранявани от платформите, са ключови за ефективното разследване и наказателно преследване.

На трето място, механизмите за идентифициране и защита на жертвите трябва да бъдат адаптирани към реалностите на онлайн експлоатацията. Критериите за идентификация и процедурите за насочване следва изрично да отчитат формите на трафик, улеснен чрез технологии, включително случаи, при които жертвите не се самоопределят като такива, не проявяват физически признаци на насилие или първоначално са третираны като извършители. Особено внимание следва да се обърне на деца, експлоатирани онлайн, както и на жертви на принудително извършване на престъпления, за които са необходими гаранции срещу криминализация и осигуряване на достъп до специализирани услуги за подкрепа.

На четвърто място, превенцията следва да бъде призната като основен компонент на отговорите срещу трафика, улеснен чрез технологии. Изграждането на устойчивост сред деца, млади хора и други уязвими групи чрез дигитално-медийна грамотност, повишаване на осведомеността и целенасочена работа на терен може да намали излагането на риск от онлайн набиране и експлоатация. Интегрирани модели, съчетаващи образование, консултиране, механизми за сигнализиране и публично-частно сътрудничество — като Центровете за безопасен интернет<sup>8</sup> и Горещите линии — предоставят ценни рамки за ранна интервенция и ограничаване на риска.

На пето място, сътрудничеството с доставчиците на дигитални услуги следва да бъде засилено чрез ясни очаквания, структурирано взаимодействие и споделена отговорност. Платформите играят централна роля във формирането на онлайн средата и могат да допринасят за оценка на риска, създаване на механизми за сигнализиране и откриване на модели на експлоатация. Използването на изкуствен интелект и автоматизирани инструменти може да подпомогне тези



усилия, при условие че се прилагат прозрачно, с необходимите гаранции, човешки контрол и спазване на основните права.

На шесто място, политическите отговори следва изрично да отчитат ролята на дигитализацията за създаване и задълбочаване на уязвимостите към трафик и експлоатация. Това включва признаване на начина, по който онлайн средата влияе върху излагането на риск, поведението и възможностите за целенасочено набиране, особено при деца и други уязвими групи. В същото време транснационалният характер на трафика, улеснен чрез технологии, изисква засилено международно сътрудничество, включително своевременен трансграничен достъп до данни, съвместни разследвания и координация между участници, действащи в различни юрисдикции. Подобряването на събирането на данни, изследванията и доказателствената база в тази област е също от ключово значение за по-доброто разбиране на развиващите се модели на експлоатация и за разработването на ефективни политики и практики.

Накрая, разработването на политики следва да се основава на непрекъснат мониторинг, изследвания и обмен на добри практики както на национално, така и на международно ниво. В условията на бързо развитие на дигиталните технологии, отговорите срещу трафика трябва да бъдат динамични, основани на данни и включващи мултидисциплинарни перспективи. Преодоляването на разминаването между нормативната рамка и оперативната реалност е от съществено значение за гарантиране, че мерките срещу трафика, улеснен чрез технологии, са ефективни, пропорционални и насочени към правата и нуждите на жертвите.



## 9. Заключение

Дигитализацията фундаментално промени облика на трафика на хора, като трансформира начина, по който експлоатацията се инициира, поддържа и прикрива през граници и платформи. Както показва настоящата статия, технологиите не създават нови форми на трафик, но съществено променят профилите на извършителите и жертвите, начина на извършване на експлоатацията и условията, при които престъпленията се разкриват, разследват и преследват. В същото време те разширяват уязвимостта към трафик и експлоатация, засягайки значително все по-широк кръг от лица. Тези трансформации поставят под въпрос утвърдените разбирания, заложили в правните рамки, институционалните практики и изискванията към доказването на престъплението.

Нарастващото припокриване между трафика на хора, онлайн сексуалната експлоатация на деца и принудителното извършване на престъпления разкрива ограниченията на разнородни правни и оперативни подходи. В дигитална среда твърдата класификация на престъпленията и раздробените разследващи практики могат да прикрият пълния обхват на експлоатацията и да отслабят защитата на жертвите. Поради това разпознаването и отчитането на множеството форми на експлоатация в рамките на един случай е от съществено значение за ефективното разследване и цялостната подкрепа на жертвите.

В същото време дигитализацията създава и възможности за укрепване на превенцията, разкриването и сътрудничеството. Нововъзникващите практики показват огромното значение на прилагане на мултидисциплинарните подходи: взаимодействие с доставчиците на дигитални услуги, изграждане на устойчивост сред уязвимите групи и отговорното използване на технологични инструменти, включително изкуствен интелект. Тези възможности обаче изискват постоянно инвестиране в институционалния капацитет, ясни опе-



ративни насоки и гаранции, които да осигурят ефективност и зачитане на права на жертвите.

Противодействието на трафика на хора, улеснен чрез технологии, изисква преодоляване на разрыва между правните рамки и оперативната реалност. С развитието на дигиталната среда, отговорите трябва да останат адаптивни, координирани и основани на защитата на правата на жертвите. Осигуряването на способността на системите (правни и институционални) да реагират ефективно на тези трансформации е не само въпрос на ефективност, но и предпоставка за реална и ефективна защита в един все по-дигитализиран свят.

---

1 **Тъмната мрежа (Dark Web)** представлява малка, умишлено скрита част от интернет пространството, която не е достъпна чрез стандартни търсачки и изисква използването на специализиран софтуер за достъп, като например Tor. Тя позволява повишено ниво на анонимност както за потребителите, така и за администраторите на сайтове, което я прави среда, използвана както за легитимни цели, така и за извършване на незаконни дейности, включително разпространение на незаконно съдържание, онлайн пазари и комуникация между извършители на престъпления.

2 Виж., наред с другото, Конвенцията на Съвета на Европа за закрила на децата срещу сексуална експлоатация и сексуално насилие (Конвенция Лансарот, 2007 г.); Директива 2011/93/ЕС; Регламент (ЕС) 2022/2065 (Акт за цифровите услуги); както и Предложение за регламент COM(2022) 209 final.

3 Примери за такива платформи включват широко използвани социални мрежи, платформи за стрийминг на живо и услуги за съдържание на абонаментен принцип (напр. OméTV, OnlyFans, TikTok, Instagram), които предлагат функционалности като директно взаимодействие, споделяне на съдържание и възможности за генериране на доходи (монетизация) и могат да бъдат използвани неправомерно от извършители с цел експлоатация.

4 GRETA - Group of Experts on Action against Trafficking in Human Beings, <https://www.coe.int/en/web/anti-human-trafficking/greta>.

5 Съгласно Регламент (ЕС) 2022/2065 (Акт за цифровите услуги), „доверени податели“ (trusted flaggers) са организации, определени от националните координатори за цифровите услуги въз основа на доказана експертиза и компетентност при идентифициране на незаконно съдържание. Онлайн платформите са задължени да разглеждат сигналите, подадени от такива податели, с приоритет и без неоправдано забавяне, като по този начин се подобрява откриването и премахването на незаконно съдържание и се повишава ефективността на механизмите за сигнализиране.

6 Горещите линии, функциониращи в рамките на мрежата INHOPE (Международна асоциация на интернет горещите линии), която обединява 57 горещи линии в над 50 държави по света, предоставят механизми за гражданите да сигнализират за незаконно онлайн съдържание, включително материали със сексуално насилие над деца. Подадените сигнали се оценяват от обучени анализатори и, когато е приложимо, се препращат към правоохранителните органи и доставчиците на онлайн услуги, като по този начин се улесняват премахването на съдържание, трансграничното сътрудничество и идентифицирането на жертви.

7 Виж докладите на ГРЕТА от четвъртия оценителен кръг (различни държави), Съвет на Европа, 2021–2025 г.; както и ГРЕТА, 11-ти общ доклад за дейността на ГРЕТА (2021 г.).

8. Мрежа на Центровете за безопасен интернет в Европа, <https://better-internet-for-kids.europa.eu/en/sic>.



## 10. Библиография

- 1) Council of Europe. (2005). Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197). <https://rm.coe.int/168008371d>
- 2) Council of Europe. (2007). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201). <https://rm.coe.int/1680084822>
- 3) European Parliament and Council of the European Union. (2011a). Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0036>
- 4) European Parliament and Council of the European Union. (2024). Directive (EU) 2024/1712 amending Directive 2011/36/EU. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1712>
- 5) European Parliament and Council of the European Union. (2011b). Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093>
- 6) European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065>
- 7) European Commission. (2022). Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (COM(2022) 209 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209>
- 8) Council of Europe, GRETA. (2022). 11th General Report on GRETA's activities. <https://rm.coe.int/greta-11th-general-report-of-activities-2022-en/1680a72bb8>
- 9) Council of Europe, GRETA. (2021). 10th General Report on GRETA's activities. <https://rm.coe.int/10th-general-report-on-greta-activities/1680a2d43b>



- 10) Council of Europe. (2020). Online and technology-facilitated trafficking in human beings (GRETA thematic chapter in General Report). <https://www.coe.int/en/web/anti-human-trafficking/online-and-technology-facilitated-trafficking-in-human-beings>
- 11) UNODC. (2022). Global Report on Trafficking in Persons. <https://www.unodc.org/unodc/en/data-and-analysis/glotip.html>
- 12) Inter-Agency Coordination Group against Trafficking in Persons (ICAT). (2023). Issue brief: The role of technology in trafficking in persons. <https://icat.un.org/publications>
- 13) ICAT, 2020, Technology and Trafficking in Persons during COVID-19 and beyond, <https://icat.un.org/events/05-2020/technology-and-trafficking-persons-during-covid-19-and-beyond>
- 14) ICAT, 2019, Issue Brief 7, Human Trafficking and Technology: trends, challenges and opportunities, [https://icat.un.org/sites/g/files/tmzbd1461/files/human\\_trafficking\\_and\\_technology\\_trends\\_challenges\\_and\\_opportunities\\_web.pdf](https://icat.un.org/sites/g/files/tmzbd1461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf)
- 15) ICAT, 2022, Use and abuse of technology, [https://icat.un.org/sites/g/files/tmzbd1461/files/publications/icat\\_statement\\_wdat\\_2022.pdf](https://icat.un.org/sites/g/files/tmzbd1461/files/publications/icat_statement_wdat_2022.pdf)
- 16) ICAT, 2022, Issue Brief 12, Addressing vulnerabilities to Trafficking in Persons, [https://icat.un.org/sites/g/files/tmzbd1461/files/publications/icat\\_issue\\_brief\\_12\\_vulnerability\\_to\\_tip.pdf](https://icat.un.org/sites/g/files/tmzbd1461/files/publications/icat_issue_brief_12_vulnerability_to_tip.pdf)
- 17) Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment>
- 18) Europol. (2025). European Union Serious and Organised Crime Threat Assessment (EU SOCTA). <https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment>
- 19) WeProtect Global Alliance. (2021). Global Threat Assessment 2021. <https://www.weprotect.org/global-threat-assessment-21/>
- 20) Dutch National Rapporteur on Trafficking in Human Beings and Sexual



Violence against Children. (2024). Annual figures Human Trafficking 2023. <https://www.dutchrapporteur.nl/documents/2024/10/18/annual-figures-human-trafficking-2023>

21) Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children. (2024). Broad perspectives of offending: backgrounds of domestic sex traffickers. <https://www.dutchrapporteur.nl/documents/2025/04/04/broad-perspective-on-offending-backgrounds-of-domestic-sex-traffickers>

22) OSCE. (2024). Policy action to address technology-facilitated trafficking in human beings. <https://cthb.osce.org/cthb/579190>

23) Aronowitz, A. A. (2009). Human trafficking, human misery: The global trade in human beings. Praeger, [https://www.researchgate.net/publication/373884084\\_Human\\_Trafficking\\_Human\\_Misery\\_The\\_Global\\_Trade\\_in\\_Human\\_Beings](https://www.researchgate.net/publication/373884084_Human_Trafficking_Human_Misery_The_Global_Trade_in_Human_Beings)

24) Shelley, L. (2010). Human trafficking: A global perspective. Cambridge University Press. [https://assets.cambridge.org/97805211/13816/excerpt/9780521113816\\_excerpt.pdf](https://assets.cambridge.org/97805211/13816/excerpt/9780521113816_excerpt.pdf)

25) Lee, M. (Ed.). (2011). Trafficking and global crime control. Sage. [https://sk.sagepub.com/book/mono/trafficking-and-global-crime-control/toc#\\_](https://sk.sagepub.com/book/mono/trafficking-and-global-crime-control/toc#_)

26) Kempadoo, K., Sanghera, J., & Pattanaik, B. (Eds.). (2015). Trafficking and prostitution reconsidered. Routledge. [https://christusliberat.org/journal/wp-content/uploads/2018/08/Trafficking-and-Prostitution-Reconsidered\\_Kamala-Kempadoo.pdf](https://christusliberat.org/journal/wp-content/uploads/2018/08/Trafficking-and-Prostitution-Reconsidered_Kamala-Kempadoo.pdf)

27) Broad, R., & Turnbull, N. (2019). From human trafficking to modern slavery. European Journal on Criminal Policy and Research, 25(2), 119–133. <https://research.manchester.ac.uk/en/publications/from-human-trafficking-to-modern-slavery-the-development-of-anti-/>

28) Lavorgna, A. (2014). Organised crime goes online. Journal of Money Laundering Control, 18(2), 125–138. <https://www.emerald.com/jmlc/article-abstract/18/2/153/236674/Organised-crime-goes-online->



realities-and?redirectedFrom=fulltext

29) Leukfeldt, R., & Yar, M. (2016). Applying routine activity theory to cybercrime. *European Journal of Criminology*, 37(3), 263–280. [https://www.researchgate.net/publication/286923434\\_Applying\\_Routine\\_Activity\\_Theory\\_to\\_Cybercrime\\_A\\_Theoretical\\_and\\_Empirical\\_Analysis](https://www.researchgate.net/publication/286923434_Applying_Routine_Activity_Theory_to_Cybercrime_A_Theoretical_and_Empirical_Analysis)

30) Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2014). Victims' voices in online grooming. *Journal of Child Sexual Abuse*, 23(5), 532–550. [https://www.hrpublish.org/journals/article\\_info.php?aid=240](https://www.hrpublish.org/journals/article_info.php?aid=240)

31) Livingstone, S., & Smith, P. K. (2014). Online risks to children. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://acamh.onlinelibrary.wiley.com/doi/10.1111/jcpp.12197>

*Тази аналитична статия е създадена в рамките на проект „Укрепване на капацитет, обмен на опит и изследователска дейност в сферата на сигурността“, с номер BG65ISPR001-3.004-0002, по договор № 812108-68-02.10.2024, финансиран по Програмата на Република България по фонд „Вътрешна сигурност“ за периода 2021 – 2027 г.*

*Цялата отговорност за съдържанието на материала е на неговия автор и фондация „Европейски институт“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на ЕС и Отговорния управляващ орган.*