

невидими ДАННИ

Кибер и технологичното измерение на домашното насилие срещу жени в България

20 препоръки в
екосистемна перспектива



COUNTER
INTUITIVE
INSTITUTE



БЪЛГАРСКИ
ФОНД ЗА
ЖЕНИТЕ



Съфинансирано от
Европейския съюз

Кибер и технологичното измерение на домашното насилие (КТИДН) се утвърждава като **структурен проблем** в държавите членки на Европейския съюз (ЕС) и представлява нарушение на основните права, като например правото на човешко достойнство, правото на живот и неприкосновеност на личността, правото на защита на лични данни, правото на недискриминация, включително въз основа на пола. В България явлението е документирано недостатъчно: съществуващата нормативна уредба не обхваща изрично множество негови форми, институционалният капацитет за реакция е ограничен, а статистическите данни са оскъдни. България не е ратифицирала Истанбулската конвенция, което прави **Директива (ЕС) 2024/1385** основния инструмент за модернизация на правната рамка със задължение за транспониране до 14 юни 2027 г.

Настоящият документ представя основни констатации от проекта **„Невидими данни: Базиран на знание подход за противодействие на кибер и технологично насилие, основано на пола“**, анализира пропуски в действащото законодателство и предлага двадесет конкретни препоръки към правителството, институциите, медиите, частния сектор и организациите на гражданското общество (НПО).

The Counterintuitive Institute
Април 2026
София

База от
Невидими данни



С финансовата подкрепа на Български фонд за жените и Европейския съюз. Изразените възгледи и мнения са единствено на автора(ите) и не отразяват непременно тези на БФЖ, ЕС, Генералната дирекция „Правосъдие и потребители“ на Европейската комисия или на ЕК. Нито БФЖ, нито ЕС, нито ЕК и нейните структури могат да бъдат държани отговорни за тях.



Понятието **кибер и технологично насилие (КТН)** съчетава широк спектър от поведения, при които технологиите и онлайн пространствата се използват като инструмент за упражняване на контрол, сплашване, унижение или вреда спрямо жени и момичета. Директива (ЕС) 2024/1385 изрично урежда: споделяне без съгласие на интимни или манипулирани материали (чл. 5), киберследене (чл.6), кибертормоз (чл. 7), и подбуждане към насилие или омраза в киберпространството (чл. 8). По-конкретно, явлението обхваща доксинг, deepfake сексуално съдържание, технологично-опосредстван принудителен контрол, онлайн тормоз и заплахи. Последното проучване на ниво ЕС за насилието, основано на пола, потвърждава, че **1 от 3 жени в ЕС е преживяла насилие през живота си**. В същото време нови изследвания показват, че дигиталните технологии все по-често се използват за **тормоз, наблюдение и заглушаване на жени** – особено на тези, които вече преживяват други форми на насилие, както и на жени, активни онлайн или в публичния живот ([FRA & EIGE, 2026](#)).



Изследването на The Counterintuitive Institute в периода юли 2025 г. – януари 2026 г. показва:

- **83%** от случаите на домашно насилие имат кибер или технологичен аспект, като в **64%** от случаите този тип насилие е системно.
- Най-често срещаните форми на кибер и технологично насилие са:
 - Обиди или заплахи в лична комуникация онлайн или по телефона (**91%**)
 - Използване на заплахи, унижителни или обидни коментари за жертвата в лична комуникация с други хора онлайн (**73%**)
 - Изискване от насилника към жертвата за постоянна информация по телефона или онлайн (**71%**)
 - Ограничаване на онлайн и телефонната комуникация на жертвата с непознати (**33%**)
 - Обсебване на пароли за интернет платформи и сайтове (**29%**).
- Половият елемент при този тип насилие е силно изразен: 1) от извършителите: **86%** са мъже, **14%** са жени; 2) от жертвите: **91%** са жени, **9%** са мъже. Значително преобладават мъжете насилници и жените жертви. По-вероятно е жена да бъде насилник, отколкото мъж да бъде жертва.
- Средностатистическата жертва е малко по-млада (на **36** години) от средностатистическия извършител (на **40** години).
- Преобладава насилието, извършвано от мъже над жени в условията на интимна връзка. **95%** от насилието в интимна връзка се извършва от мъже. **54%** от кибер и технологичното насилие в интимна връзка се извършва в приключили връзки (между бивши съпрузи или партньори).
- При **30%** от кибер и технологичното насилие в условията на домашно насилие, то е насочено към близки, роднини и приятели на жертвата (т.нар. насилие „by proxy“).
- Жертвите изпитват трайни последици от кибер и технологичното насилие, включително:
 - Страх и чувство на безпомощност (**82%**)
 - Депресия, тревожност, или паник атаки (**77%**)
 - Проблеми със съня и/или с концентрацията (**73%**)
 - Трудности в личните взаимоотношения (**64%**)
 - Проблеми на работното място или в професионално развитие (**37%**)
 - Финансови проблеми (**30%**)
 - Проблеми със Закона или неприятности с органите на реда (**13%**).

За повече информация относно методологията и резултатите от изследването, посетете „[База от Невидими Данни](#)“.

Законодателни и регулаторни практики от ЕС за справяне с кибер насилието

- **Австрия:** Приет е Национален план за действие за борба с насилието срещу жени и момичета (2025–2029 г.) (Nationaler Aktionsplan zur Bekämpfung von Gewalt an Frauen und Mädchen 2025-2029), който включва около 350 мерки, разработени с участието на практики, академици, представители на администрацията и създатели на политики, и е съобразен с Истанбулската конвенция и Директива 2024/1385. Планът се основава на разбирането, че всички жени и момичета – независимо от произход, възраст, увреждане, професия или начин на живот – имат право на самоопределяне и живот без насилие. Документът предвижда и координирани действия срещу омразата в интернет и кибернасилието, включително в контекста на домашното насилие.
- **Нидерландия:** От 1 юли 2024 г. са в сила нови законови разпоредби за сексуалните престъпления, които значително разширяват защитата на жертвите – например, премахва се изискването за доказване на физическа принуда при случаи на изнасилване и сексуално посегателство. Изрично се криминализира сексуалният тормоз в публични пространства, включително в социалните мрежи и онлайн платформи и се утвърждава принципът, че сексуалното насилие онлайн и офлайн следва да бъде санкционирано по еднакъв начин.
- **Ирландия:** От юли 2025 г. Кодексът за онлайн безопасност (Online Safety Code) въвежда задължителни изисквания за определени категории онлайн платформи, включително платформи за видео споделяне и такива, хостващи съдържание за възрастни или екстремно насилие. Мерките включват механизми за удостоверяване на възрастта, ограничаване на достъпа на деца до вредно съдържание, задължения за управление на риска и отчетност към регулатора, като при неспазване са предвидени значителни финансови санкции.

20 препоръки в екосистемна перспектива

Към правителството и законодателя

Формално включване на темата за кибер и технологичното насилие като приоритет в национални стратегии и програми с определени отговорни институции, срокове и индикатори за изпълнение.

Приоритизирането на темата е критична стъпка за преодоляване на устойчивата тенденция за омаловажаване на кибер и технологичното измерение на насилието, основано на пола и в условията на домашно насилие от институциите.

01

Навременно (до юни 2027 г.) транспониране на Директива (ЕС) 2024/1385 в българското законодателство, като се осигури съгласуваност с останалата приложима европейска правна рамка (например, защита на данните, цифрови услуги, изкуствен интелект) и се отчетат интерсекционалните фактори.

Особено внимание следва да се обърне на жените, които са обществени представителки, журналистки или защитнички на правата на човека като уязвими групи, особено във връзка с различните форми на кибернасилие (чл. 11 (н)). Съответно, мерките за превенция и защита трябва да вземат предвид специфичния риск, свързан с публичната роля на тези жени. При транспонирането на Директива (ЕС) 2024/1385, както и при изготвянето на стратегически документи и политики за превенция и противодействие на КТН, следва да се вземат предвид интерсекционалните уязвимости на засегнатите групи. Необходимо е да се отчетат фактори като дигитално изключване, етническа принадлежност, джендър идентичност, мигрантски статус, увреждания, възраст, социално-икономически статус, които могат да увеличат риска от насилие и да ограничат достъпа до защита и правосъдие.

02



Регулярно събиране на официални данни за случаите на кибернасилие на национално и местно ниво.

Трябва да е налице национална „система за събиране, разработване, изготвяне и разпространение на статистически данни относно насилието над жени или домашното насилие“ (чл. 44 (1)), която да има ясно определена водеща институция, стандартизирани индикатори и механизми за обмен на данни между институциите. Събраните статистически данни, които не съдържат лични данни, следва да бъдат предоставяни на разположение на обществеността по леснодостъпен начин (чл. 44 (6)).

03

Криминализиране на всички форми на кибер и технологично насилие, описани в Директивата.

Извършване на цялостен преглед на действащото наказателно законодателство и при необходимост въвеждане или адаптиране на наказателноправни състави, съответстващи на изискванията на Директива (ЕС) 2024/1385, включително по отношение на споделяне без съгласие на интимни или манипулирани материали, киберслеждане, кибертормоз, и подбуждане към насилие или омраза в киберпространството. Дефинициите следва да са достатъчно технологично неутрални, за да адресират бъдещи форми на злоупотреба, и да осигуряват ефективна защита на всички жертви, като отчитат специфичните рискове при насилие, основано на пола.

04

Разширяване на 33ДН чрез технологичен компонент в дефиницията за домашно насилие.

Изрично включване на кибер и технологичното насилие, тормоз и принудителен контрол в дефиницията за домашно насилие по чл. 2 от 33ДН. Различните форми на КТН следва да бъдат разглеждани като самостоятелно и достатъчно основание за издаване на заповед за защита по 33ДН. Необходими са ясни правила за събиране, оценка и допустимост на електронни доказателства (напр. скрийншотове, логове, метаданни), както и възможност за спешни мерки за ограничаване на достъпа до вредно съдържание.

05



Насърчаване на партньорство между държавата, академичните среди и НПО за анализ и разработване на политики, базирани на данни.

В рамките на съществуващ или нов механизъм за сътрудничество да се предприеме, подпомага и утвърди събирането, анализа и интерпретацията на данни за КТН в условията на домашно насилие. Препоръчително е механизмът да включва функционални и тематични работни групи, ясни правила за споделяне на анонимизирани данни, регулярни експертни срещи и допитвания между държавните институции, академичната общност и неправителствените организации (НПО). НПО следва да бъдат признати като ключови партньори, тъй като разполагат с практически опит, пряк достъп до жертви и ценна емпирична информация, както и да бъдат подпомагани с устойчиво и достатъчно финансиране за работа по тази тема.

06

Към институциите

Изготвяне и публикуване на задълбочен правен анализ на българската нормативна уредба и съответствието ѝ с Директивата.

Експертна работна група към Министерството на правосъдието следва в рамките на 2026-та година да предложи необходимите нормативни промени за пълно транспониране на Директивата. Докладът, изготвен от работната група, трябва да бъде публично достъпен с цел повишаване на прозрачността и обществената информираност по темата.

07

Активно участие в национални и международни инициативи и проекти с цел повишаване на ангажираността и обмяната на опит.

Българските държавни и общински институции следва активно да участват в европейски и национални проекти, свързани с превенцията и борбата с насилието над жени и кибер и технологичното насилие. Това спомага за обмяна на добри практики, изграждането на капацитет и внедряването на иновативни технологични решения, често разработвани на европейско ниво. Необходимо е да се работи в посока преодоляване на резервираността към включване в подобни инициативи и проекти от страна на тези институции.

08



Постоянно, устойчиво и прозрачно функциониране на Националния съвет за превенция и защита от домашното насилие.

Следва да се гарантира устойчивото функциониране на Националния съвет за превенция и защита от домашното насилие чрез ясно определен мандат, бюджет, публичност на дейността, участие на експерти от държавни институции и неправителствени организации, както и експерти по КТН.

- Препоръчително е да се създаде механизъм, по който да се консултират неправителствени организации, които получават държавно финансиране, за да се обхванат организации със значителна експертиза, работещи пряко с жертви.
- Следва на уебсайта на Министерски съвет да се публикуват протоколи от заседанията на Националния съвет за превенция и защита от домашното насилие, както и съпътстващи материали (анализи, проучвания, статистики).
- Във функциите на Националния съвет следва изрично да се спомене КТН като форма на домашно насилие.
- Препоръчително е в Националния съвет да се включи представител на гражданския сектор или на академичната общност със задълбочени познания в областта на КТН, основано на пола.

09

Устойчив, активен фокус над превенцията и повишаване на публичната чувствителност относно кибер и технологичното насилие.

Отговорните институции трябва да поставят силен фокус върху превенцията, включително „целенасочени кампании за повишаване на осведомеността или програми, насочени към широката общественост от ранна възраст“. Важно е те да повишават и разбирането за различните форми и първопричините на насилието над жени и домашното насилие (чл. 34 (2) от Директивата). В основата на добрата превенция са образователни мерки от ранна възраст, включително инициативи, които насърчават мъжете и момчетата да действат като положителни ролеви модели в подкрепа на промени в поведението в обществото, свързани с уважаване на личната неприкосновеност, равенството между половете и взаимното уважение (чл. 34 (5)).

10

Повишаване на капацитета сред институциите, ангажирани с превенцията и противодействието на КТН.

Необходимо е системно изграждане на знания, умения и координация между ангажираните органи, така че да се гарантира навременна и адекватна защита на жертвите, например:

- Провеждане на специализирани обучения за служители в полицията, прокуратурата, съдебната система и местната власт относно формите, механизмите и доказването на КТН, включително избягване на вторичното и повторното виктимизиране при работа и комуникация с жертви (чл. 21 (е)). Това е особено важно в случаи на кибернасилие, което се отличава с голям мащаб (напр. споделяне на видеа с жертвата в платформи, социални медии или сайтове с порнографско съдържание).
- Разработване на практически насоки и стандартизирани процедури за работа по случаи на КТН за всички ангажирани институции. Те следва да предвиждат разработване на процедури за събиране, съхранение и верификация на електронни доказателства в съответствие с процесуалните изисквания, както и изрично включване на проявите на КТН в прилаганите методи за оценка на риска.
- Определяне на специализирани експерти и изграждане на капацитет в рамките на съществуващи институции, звена, дирекции (напр. оперативни звена в ГДНП с компетентност за случаи на КТН за съхранение и анализ на електронни доказателства и специализирани прокурори по кибер насилие в окръжните прокуратури с приоритет в районите с по-висока натовареност).
- Насърчаване на междуинституционалното сътрудничество и обмен на добри практики, включително чрез съвместни обучения и координационни механизми като провеждане на специализирани обучения за практики, работещи с жертви и/или извършители, които да помагат на преживяващите домашно насилие да разпознават неговите кибер и технологични форми.
- Изрично отчитане на важността и разпространеността на икономическото измерение на КТН, което включва ограничаване на достъпа до онлайн банкиране и дигитални финансови услуги, неправомерно използване на лични данни за теглене на кредити или покупки, контрол върху електронни плащания и акаунти и саботиране чрез технологични средства на трудовата заетост и възможностите за професионално развитие на жертвите.



Подкрепа на усилията на ЕС за ефективно модерирание и докладване на съдържание, свързано с КТН.

Българските институции следва активно да подкрепят и насърчават усилията на европейско ниво за по-ефективно предотвратяване, докладване и премахване на съдържание, свързано с КТН чрез прилагане на европейската регулаторна рамка и участие в общи механизми за координация.

- В рамките на Закона за дигиталните услуги (Digital Services Act), компетентните национални органи следва да прилагат и използват механизмите, предвидени в европейската регулаторна рамка (вкл. координация с националния координатор по цифровите услуги), за гарантиране на ефективно докладване и премахване на съдържание.
- Националните компетентни органи следва да съдействат за засилен мониторинг, прозрачност относно предприетите мерки, оценка на системните рискове и ефективно сътрудничество между платформите, държавните институции и гражданския сектор с оглед по-добра защита на засегнатите лица.

12

Към медиите

Редакционни стандарти за отразяване на кибер насилие срещу жени.

В контекста на нарастващото разпространение на КТН срещу жени е необходимо българските медии да поемат активна и отговорна роля както в неговото отразяване, така и в превенцията му. Това предполага разработване и прилагане на ясни редакционни стандарти, които да гарантират етично, балансирано и чувствително към жертвите медийно съдържание, включително избягване на сензационализъм, обвиняване на жертвата и разпространение на вредни стереотипи. В тази връзка е уместно засилване на ролята на Съвета за електронни медии и Комисията за журналистическа етика при разработването и популяризирането на насоки и саморегулаторни механизми за отразяване на случаи на КТН.

13



Медийни кампании за обществена информираност.

Следва медиите да насърчават, реализират и участват в целенасочени кампании за повишаване на обществената информираност относно различните форми на кибернасилие, рисковете за жертвите и възможностите за защита и подкрепа. Такива кампании могат да се осъществяват в партньорство с държавни институции, неправителствени организации и образователни структури (училища, университети, читалища). Препоръчително е да се използват съвременни, актуални и разнообразни комуникационни канали с цел достигане до различни възрастови и социални групи.

14

Сътрудничество с онлайн платформите и социалните медии за разпознаване и поддържане на стандартите за отразяване на КТН.

От значение е укрепването на сътрудничеството между медиите и онлайн платформите и социалните мрежи, включително Meta Platforms, Google и TikTok, за по-ефективно разпознаване и премахване на КТН. Това сътрудничество може да включва обмен на добри практики, разработване на общи стандарти и участие в инициативи за саморегулация, съобразени с българската правна рамка и европейските изисквания.

15

Към частния сектор

Превенция и противодействие на технологичното финансово насилие.

Банките и небанковите финансови институции следва да разработят вътрешни политики и процедури за идентифициране на рискови модели, съобразени с регулаторните изисквания и правата на клиентите (включително подозрителни модели на контрол върху сметки, принудително споделяне на достъп или злоупотреба с дигитално банкиране).

- Това може да се реализира чрез обучение на служителите, създаване на специализирани протоколи за сигнализиране и защита на жертвите, както и разработване на „безопасни“ банкови услуги (напр. дискретни канали за комуникация и временно ограничаване на достъп).
- Дейността следва да бъде съобразена с изискванията на Общия регламент относно защитата на данните (GDPR), като се гарантира защита на личните данни и сигурност на информацията.

16

Безопасен дизайн на ИИ срещу технологично насилие.

Компаниите, разработващи и предлагащи услуги с изкуствен интелект (AI) и свързани устройства (IoT / smart devices), следва да интегрират подходи „safety-by-design“ и „privacy-by-design“, включително чрез оценки на риска, механизми за откриване на злоупотреби (сексуални deepfake, дигитално проследяване и контрол чрез технологии) и прозрачност, съобразени с приложимата европейска регулаторна рамка.

- Това включва внедряване на механизми за откриване и ограничаване на манипулирано съдържание, защиты срещу неоторизиран достъп до устройства и ясни потребителски контроли.
- Спазването на Общия регламент относно защитата на данните (GDPR), Закона за дигиталните услуги (Digital Services Act) и Закона за изкуствения интелект (EU AI Act) следва да бъде съчетано с редовни оценки на риска и прозрачност относно функционирането на алгоритмите и мерките за защита на потребителите.

17

Към организациите на гражданското общество

Цялостна и добре информирана правна и психологическа подкрепа за жертви.

Организациите на гражданското общество следва да предоставят координирана и цялостна подкрепа на жертвите на КТН, която обхваща както правни, така и психологически аспекти:

- Създаване на мултидисциплинарни екипи (юристи, психолози, социални и здравни работници).
- Осигуряване на безплатна или достъпна правна помощ, включително при онлайн прояви на насилие и тормоз.
- Предоставяне на психологическа подкрепа, съобразена със спецификите на КТН.
- Разработване на координационни механизми за насочване към институции и услуги.

18



Дигитална безопасност: обучение на специалисти от първа линия.

Повишаването на дигиталната грамотност и уменията на специалистите от първа линия е от съществено значение за разпознаването и адекватната реакция при случаи на КТН. Обученията следва да бъдат практически насочени и адаптирани към реалните предизвикателства, с които се сблъскват жертвите.

- Организиране на регулярни обучения по дигитална безопасност и киберрискове от организации с експертиза по темата.
- Разработване на практически ръководства и инструменти за работа по случаи на КТН чрез междусекторни инициативи и сътрудничество.
- Обучение за защита на лични данни, устройства и онлайн профили от организации с експертиза по темата.
- Изграждане на умения за оценка на риска и насочване към подходяща помощ чрез междусекторно и междуорганизационно споделяне на знания.

19

Мониторинг, събиране на данни и застъпничество.

Гражданските организации трябва да продължат да играят важна роля в събирането на данни и наблюдението на тенденциите при КТН, като допълват официалната информация и идентифицират пропуски в системата. Тези данни са основа за ефективно застъпничество и за формулиране на политики, базирани на доказателства. Дейностите следва да включват:

- Систематично събиране и анализ на данни от случаи, с които организациите работят.
- Публикуване на доклади, анализи и препоръки към институциите.
- Участие в обществени консултации и законодателни процеси.
- Изграждане на партньорства с институции, академични среди и други НПО за съвместно застъпничество.

20



Ефективното противодействие на кибер и технологичното насилие изисква цялостен, междусекторен и координиран подход, който обединява усилията на държавните институции, създателите на закони и политики, частния сектор, медиите и гражданското общество. Необходима е модернизация на правната рамка, пълноценно транспониране на европейските изисквания и последователно признаване на новите форми на дигитално насилие като реални и сериозни рискове за сигурността, правата и достойнството на жертвите. Успоредно с това следва да се развият устойчиви механизми за превенция, обучение, събиране на данни и междуинституционално сътрудничество, които да гарантират не само реакция при случаи на насилие, но и предотвратяването на КТН в дългосрочен план.

Кибер и технологичното измерение на насилието изисква по-добър екосистемен капацитет: специализирани звена, цифрово грамотни специалисти, стандарти за работа с жертви на КТН, достъпни услуги и подобро междусекторно сътрудничество.



невидими ДАННИ



COUNTER
INTUITIVE INSTITUTE