

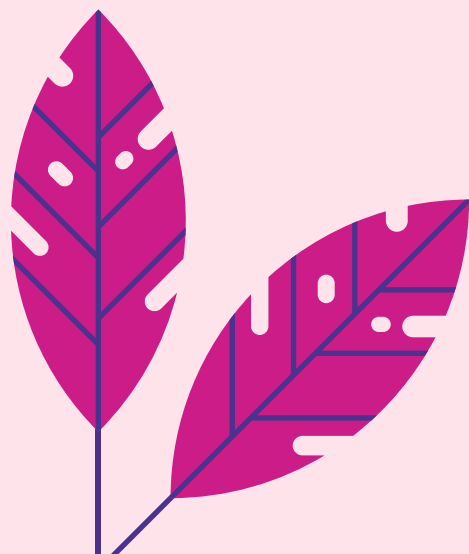
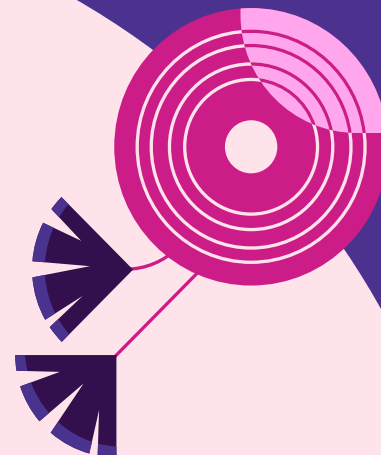
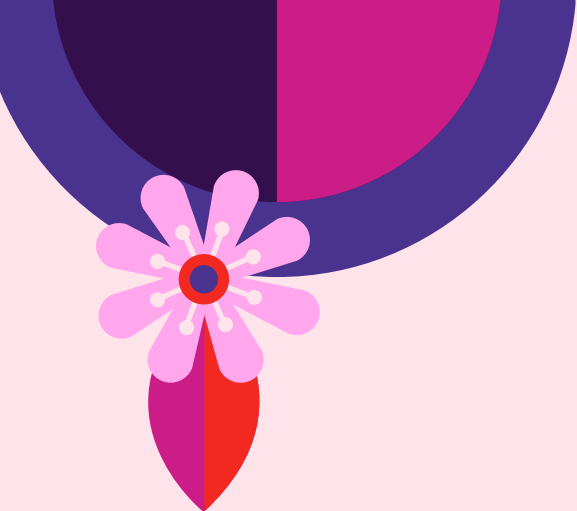
невидими ДАННИ

Наръчник

Какво е кибер и технологично
насилие и как да говорим
за него?



COUNTER
INTUITIVE INSTITUTE



Абревиатури

ДН	Домашно насилие
ЕС	Европейски съюз
ЕК	Европейска комисия
КЗЛД	Комисия по защита на личните данни
ИИ	Изкуствен интелект
ИКТ	Информационни и комуникационни технологии
КТИДН	Кибер и технологични измерения на домашното насилие
КТН	Кибер и технологично насилие
НК	Наказателен кодекс
НПО	Неправителствена организация
CSAEM	Child Sexual Abuse or Exploitation Materials
EIGE	European Institute for Gender Equality
GREVIO	Group of Experts of Action against Violence against Women and Domestic Violence
IoT	Internet of Things

Съдържание

Абревиатури	4
Съдържание	5
Благодарности	7
Въведение	8
Какво е кибер и технологично насилие и как да говорим за него?	10
Нормативна уредба	15
Членове на Директива 2024/1385	20
Кибер и технологично насилие в българското законодателство	24
Чеклист на кибер и технологичното насилие	30
Какво да направим, ако сме жертва на кибер или технологично насилие?	33
Как да работим с жертви на КТИДН?	35
Как да говорим за КТН?	38
Как да говорим за насилие основано на пола, с грижа за хората и обществото?	39
Какво са данни, с които можем да комуникираме?	42
Как да структурираме комуникацията в социалните мрежи?	44
Как да разказваме истории с данни?	47
Приложение 1	56
Таксономия на кибер и технологичното насилие, основано на пола	56
Приложение 2	66

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.

Наръчникът “Какво е кибер и технологично насилие и как да говорим за него?” представя ключова информация за кибер и технологичното насилие и отправя насоки, добри практики и тактически стъпки за организациите, работещи на първа линия срещу домашното насилие и насилието, основано на пола. С него целим да предложим информация, умения и знания, които да помагат за по-ясната и по-добра комуникация относно КТН, както и за по-ефективното справяне с това измерение на насилието.

The Counterintuitive Institute
Април 2026
София

База от
Невидими данни



Благодарности

Благодарим на Български фонд за жените за подкрепата и предоставената възможност да работим по тази изключително важна за обществото тема. Благодарим на всеотдайните ни партньори - Фондация „Х и Д Перспективи“ и Асоциация „Деметра“, които с готовност и желание изпълниха пилотирането на индикаторите и допринесоха за качеството и достоверността на изследването. Но преди всичко, дълбоко оценяваме смелостта на жертвите на насилие, които косвено споделиха историите си с нас, благодарение на което успяхме да реализираме настоящото изследване. Надяваме се, че то ще бъде полезно и ще допринесе за намаляването не само на домашното насилие, но и на насилието, основано на пола като цяло.



COUNTER
INTUITIVE
INSTITUTE



БЪЛГАРСКИ
ФОНД ЗА
ЖЕНИТЕ



Съфинансирано от
Европейския съюз

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.

Въведение

Голяма част от живота на социално и граждански активните хора преминава онлайн. Социалните медии са каналът, по който достъпваме информационния поток и по който поддържахме връзка с близки и приятели. Смартфоните са продължения на ръката и личността ни, телевизорите са умни и интерактивни, а домовете ни се обитават от „мислещи“ хладилници, прахосмукачки, отоплителни системи, гласови асистенти, таблети, аларми и т.н.

Но, за съжаление, тези нововъведения са и опасности за много от нас. И ако изследванията и медиите вече са поели по своя път по установяване и даване на гласност на този така остър и вече набиращ сила проблем, то политическата реакция на национално и местно ниво изостава значително. Причина за това изоставане е липсата на аргументи и доказателства за сериозността, размерите и проявленията на кибер и технологичното измерение на полово-базираното и домашното насилие в България. На този фон политиките и нормативната уредба не отразяват реалността и превръщат тези форми на насилие в невидим проблем. В опит да дадем гласност на този проблем, ние от екипа на Института за контраинтуитивни идеи събрахме първите в България данни за кибер и технологичното измерение на домашното насилие (КТИДН). Инициативата беше част от проекта „Невидими данни“, в който разработихме първите приспособени към българския контекст индикатори за идентификация и разбиране на КТИДН, насочени към практиките от първата линия на борбата с домашното насилие в България. В хода на изследването открихме, че КТИДН съществува, жертвите го преживяват и осъзнават, а доставчиците на кризисни

услуги го възприемат като основна част от спектъра на насилието.

Ето защо създадохме този (непълн) Наръчник по кибер и технологично насилие и как да говорим за него. В него споделяме знанието си по проблема и неговите измерения в България и предлагаме методи и инструменти, с които той да бъде идентифициран, разпознат, назован и публично оповестен. Този Наръчник е за всички **организации, които работят на първа линия** срещу домашното насилие, за всички институции, които нямат задължението, но могат да открият пространството и законовата пролука, с която да му противодействат, за всички **комуникационни експерти**, които искат да допринесат към подобряване на публичния разговор за насилието над жени и за полово-базираното насилие, **за всички хора**, които не знаят какво да кажат и как да реагират по повод на своята позната, близка, или приятелка, чийто партньор чете чатове ѝ, снима я без изричното ѝ съгласие или желание, ревнува я дотолкова, че, изисква видеообаждания и инсталира видеонаблюдение в дома ѝ. Този Наръчник е за всички, които могат и искат да се противопоставят на насилието над жени и на домашното насилие. Дори и само като говорят за него.





Какво е кибер и технологично насилие и как да говорим за него?

Преди да можем да разбираме новите форми на насилие в дълбочина и да им противодействаме, трябва да ги назовем и опишем по разбираем начин. Важно е обаче да се изгради социално приложимо определение на кибер и технологичното насилие (КТН), защото това е първата стъпка към осъзнаването, че то се случва и нанася сериозни щети на жертвите, на техните общности и на цялото общество. За целта до момента е изминат път основно в две направления: научно и нормативно. Първото се съсредоточава върху индивидуално-психологическите и социално-политическите аспекти на КТН и се опитва да разбере същността му през тенденциите на неговото развитие и връзката му с културните и институционални системи. Второто бори със законови дефиниции и цели закодирането на КТН в регулативни рамки така, че то да може да бъде третирано като престъпление, а извършителите преследвани.

Кибернасилието е насилие, което се случва онлайн и използва или засяга дигитални средства на комуникация. Технологичното насилие използва нови и традиционни технологии като инструмент за подчинение и/или нарушаване на свободата и правата на жертвата.

Кибер и технологичното насилие не е по дефиниция обвързано с пола и динамиките на половото

неравенство. Но е такава на практика. Жените и децата са значително по-уязвими както в материалния свят, така и в дигиталния. Всъщност [данните показват](#), че ако си жена или момиче в ЕС е по-вероятно да си изпитвала кибертормоз, отколкото да не си. В почти половината от случаите става въпрос за кибернасилие с женомразки или сексуален характер. В същото развитието на големи езикови модели и тяхното комерсиализиране и повишена достъпност разкриват тенденция по „естествена насока“ на злоупотребата с инструментите на изкуствения интелект (ИИ) в посока към незначителното на телесната автономност на жените и момичетата и съответно погаването на техните човешки права и достойнство.

В края на 2025 година се разиграва илюстративен случай, от който светът видя от първа ръка мащабите и скоростта на изкуственият интелект (ИИ) да се превърне в инструмент за кибернасилие над жени и деца. Потребителите на X (по-известен с предишното си име twitter) получават достъп до Grok – вътрешноплатформен чатбот с ИИ. Инструментът е използван за генериране и разпространение на милиони нежелани, неодобриени, вулгарни и сексуализирани фалшиви изображения. В първите 9 дни на съществуването си Grok генерира 4.4 милиона изображения, от които поне 41% са сексуализирани образи на жени. Значителна част от обектите на това онлайн насилие са публични личности, знаменитости, политически фигури – разпознаваеми реални жени по бельо, в сексуални или насилствени ситуации.

В отговор Службата за комуникации (Ofcom) на Великобритания започва разследване, Европейската комисия - проверка по Закона за цифровите услуги (DSA), Франция, Индия, Малайзия и Индонезия - разследвания или временно ограничаване на





достъпа до бота. Като резултат, на Grok е забранено произвеждането на изображения с голота в държави, в които разпространението на снимки и изображения на голи хора са забранени сами по себе си. Чатботът обаче все още е активен, а реални ограничения върху най-богатия в този момент човек на планетата (собственикът на X – Илон Мъск) не са ефективно наложени.

Да, всеки би могъл да е жертва на КТН. Но кибер и технологичното насилие срещу жени и момичета е предизвикано от пола им и от социални структури, които налагат стереотипни роли и поддържат система на неравенство. Така, насилието придобива съвсем нови мащаби, когато се развива в дигиталното пространство или чрез технологични средства. КТН, основано на пола, е проявление на полово-базираното насилие. То създава поле за нови практики на насилие над жени, улеснява го и затруднява преследването му.

КТН **въплъщава властовите динамики, системните неравенства, желанието за упражняване на контрол и битуващите стереотипи за ролята на жената в семейството и обществото**, които характеризират ДН и насилието, основано на пола като цяло. КТН е проявление на същия сериозен и често скрит социален проблем, които често причинява сериозни и трудно обратими психически, физически и емоционални травми с дългосрочни последици за личния и професионалния живот на жертвата.

Общи черти между насилието над жени в материалния и в дигиталния свят:

- ☀ **Основната цел на насилието е да се установи контрол над жертвата:** Независимо дали става въпрос за партньор насилник, който държи жертвата си заключена у дома, без да ѝ позволява

да се среща със свои близки, или за партньор насилник, който отнема електронни устройства и отказва достъп до чат или телефонна комуникация на жертвата, крайната цел на тези отношения е установяването на доминация.

- ☀ **Насилникът може да бъде познат или непознат за жертвата.** Въпреки че данни от световен мащаб показват, че най-вероятният насилник е роднина или партньор, основаното на пола насилие онлайн и офлайн може да бъде извършено и от непознат.
- ☀ **Взаимоотношенията между жертвата и насилника могат да започнат доброволно и реципрочно, но да прераснат в насилие.**
- ☀ **В обществото съществува тенденцията вината да се прехвърля върху жертвата (victim-blaming), особено когато насилието е от сексуален или интимен характер.**
- ☀ **Някои форми на насилието се нормализират с помощта на вкоренените патриархални норми и не се разпознават като обществен проблем.**
- ☀ **Насилието води до тежки последици за жертвите, независимо дали е онлайн или офлайн или извършено с технологични средства.** И ако физическото насилие може да доведе до загуба на животи, то насилието във всичките му форми води до травми, от които жертвите понякога не успяват да се възстановят.

Ключови разлики между насилието в дигиталния и материалния свят:





☀ **КТН може да се случва постоянно.** Насилието и/или неговите носители никога не спират да съществуват. Ако насилникът все пак спи, напуска дома, разделя се с жертвата и отнася със себе си самия акт на насилието, то видеосъдържанието със сексуален характер, каченото в Telegram чат със стотици членове, никога не спира да съществува. Актът на насилието продължава денонощно и всекидневно.

☀ **КТН може да се случва навсякъде.** Актът на насилието може да се извършва в пространства, които жертвата никога не е обитавала (онлайн форуми и дигитални пространства, до които жертва няма достъп). В същото време технологичните средства, с които жертвата споделя пространство, могат да бъдат достъпвани и активирани от насилника от разстояние – smart домашни устройства, видеокамери, шпионски софтуери, които позволяват на насилника да контролира личното пространство на жертвата, без физически да нахлува в него.

☀ **Кибернасилието въвежда елемент на публичност на насилието или последиците от него,** които при тормоз и принуда в материалния свят обикновено остават скрити. Така, жертвата се превръща в обект на многолик насилник – не само на този, когото познава и споделя нейна лична информация онлайн (например), но и на всички останали, които консумират продуктите на насилието. Така не само насилникът се умножава, но и насилието. То е там, където всички биха могли да го видят, постоянно, почти неотменно.

Нормативна уредба

Няма общоприето нормативно определение за кибер и технологичното измерение на насилието. Много международни, регионални, и национални организации формулират и възприемат различни дефиниции. Съветът за равните възможности между мъжете и жените към Европейската Комисия ([Advisory Committee on Equal Opportunities for Women and Men](#)), предоставя дефиниция, възприета и от Европейския институт за полово равенство ([EIGE](#)), която гласи следното:

„Кибернасилието над жени е акт на полово-базирано насилие, извършено директно или индиректно чрез технологични информационни и комуникационни средства, което води до, или е вероятно да доведе до, физическа, сексуална, психологическа или икономическа вреда или страдание на жени и момичето, включително заплахите за такива актове, независимо дали се случват в публичния или личния живот, или ги възпрепятства в достъпа им до техните фундаментални права и свободи. Кибернасилието срещу жени включва, но не е ограничено до, нарушение на лично пространство, преследване, тормоз, основана на пола реч на омразата, споделяне на лично съдържание без разрешение, сексуално насилие с използване на образа или изображение, хакване, кражба на идентичност и пряко насилие. Кибернасилието е част от континуума на насилието срещу жени: то не съществува във вакуум: а по-скоро произтича от и поддържа множество форми на офлайн насилието“.





В допълнение, [Обща препоръка № 1](#) на GREVIO (орган от независими експерти, който наблюдава изпълнението на Конвенцията на Съвета на Европа за превенция и борба с насилието над жени и домашното насилие) определя **дигиталното/цифровото насилие над жени като отделно, но не и самостоятелно измерение на насилието**. Така например, киберследењето (cyber stalking) не е изолирано явление, а е форма на преследване, която се осъществява в цифровото пространство или чрез технологични средства. Според GREVIO, дигиталното измерение на насилието срещу жени е съвкупност от множество действия, развиващи се онлайн или посредством технологии, които формират един **континуум на насилието**, на което жените и момичетата са подложени заради своя пол (gender), включително и в домашна среда.

Дигиталното насилие е реално съществуващо и еднакво вредно проявление на насилието, основано на пола и насилието срещу жени и момичета.

Съгласно дефиницията на GREVIO, дигиталното измерение на насилието включва два основни компонента: **онлайн аспекти и вредни, улеснени от технологиите поведения**.

Онлайн аспектите са всички действия и споделяне на данни в интернет, включително чрез интернет посредници (доставчици на интернет услуги, търсачки и социални медии) както в общодостъпната мрежа (surface web), така и в тъмната мрежа (dark web). Този аспект се отнася директно към кибернасилието.

Вредните, улеснени от технологиите поведения са действия, които използват за инструмент технологии и комуникационен хардуер (смартфони, проследяващи

устройства, камери и друго записващо оборудване, GPS проследяващи устройства, смарт часовници, фитнес тракери и смарт домашни устройства) и софтуер (шпионски софтуер и други мобилни приложения) срещу жени и момичета. Този аспект се отнася директно към технологичното измерение на насилието.

В [Доклад за онлайн насилието срещу жени](#) от 2024 г. на Европейско женско лоби разграничава между:

- ✱ **Най-разпространени форми**, сред които кибер тормоз, кибер слеждане, споделяне без съгласие на интимни материали и реч на омразата
- ✱ **Все по-заплашителни форми**, включващи използването на изкуствен интелект, виртуална реалност и онлайн гейминг
- ✱ **Макро форми** като сексуално изнудване (sextortion), заснемане на нападение (filmed assault), цифрово воайорство (digital voyeurism) и т.н.
- ✱ **Допълнителни форми** като негативни коментари относно външния вид (body-shaming), групови подигравки и обиди на сексуална основа (trolling and flaming), публично споделяне на лична информация за жертвата (doxing).

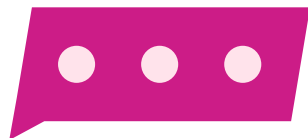
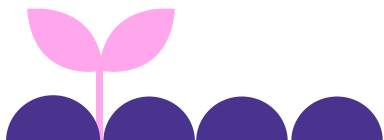
Най-значимият нормативен акт, който задава регулативната рамка около КТН като значим компонент от насилието над жени и момичета и домашното насилие, е [Директива \(ЕС\) 2024/1385](#) на Европейския парламент и на Съвета на Европа от 14 май 2024 година относно борбата с насилието над жени и домашното насилие (Директивата). Към смятаните вече за традиционни престъпни проявления на полово-базираното насилие (като убийството на жени,





изнасилването, сексуалният тормоз, сексуалното насилие, следенето, ранният брак, насилственият аборт, насилствената стерилизация, гениталното осакатяване и принудителния брак) тя причислява и конкретни действия в дигиталното пространство: 1) Споделяне без съгласие на интимни или манипулирани материали; 2) Киберслеждане; 3) Кибертормоз; 4) Подбуждане към насилие или омраза в киберпространството. Директивата е първият наднационален законов акт, който предлага конкретни дефиниции на престъпления, които от една страна се развиват в онлайн пространството (кибер аспект) и от друга, засягат вече установени социални динамики на полово неравенство (насилие, основано на пола). Важно уточнение в случая е, че Директивата разбира както самите действия като престъпление, така и заплахата за тяхното извършване.

Директивата е с обвързващ характер за страните членки на Европейския съюз. Това означава, че всички членове на ЕС трябва да успеят да транспонират Директивата (тоест, да включат нейните предписания в националното законодателство, според най-подходящата за това форма – с нов специален Закон или чрез изменение на вече съществуващи закони така, че те да отразяват кибер и технологичните аспекти на вече регулирани процеси). Определеният срок, в който Директивата трябва да бъде транспонирана, е 14 юни 2027 година. Към февруари 2026 г. няма публично налична информация за конкретните мерки, които България е предприела, за да транспонира Директивата.



КИБЕР И ТЕХНОЛОГИЧНО НАСИЛИЕ

КИБЕРТОРМОЗ

- Принуждаване към сексуална комуникация онлайн
- Групови подигравки и обиди на сексуална основа
- Публично споделяне на лична информация
- Разпространяване на слухове или лъжи за сексуалния живот на жертвата
- Кибертормоз над деца и подрастващи

ПОДБУЖДАНЕ КЪМ НАСИЛИЕ/ОМРАЗА ОНЛАЙН

- Публикуване и споделяне чрез ИКТ на съдържание, изпълнено с омраза
- Публикуване и споделяне чрез ИКТ на съдържание, което разпространява, подстрекава или оправдава омраза
- Третиране на жените като сексуален обект и осмиване на външния вид

КИБЕРСЛЕДЕНЕ

- Контрол над паролите за онлайн услуги и платформи
- Тайно използване на spyware/stalkerware или GPS устройства
- Злоупотреба с Интернета на нещата

СПОДЕЛЯНЕ НА ИЗОБРАЖЕНИЯ БЕЗ СЪГЛАСИЕ

- Сексуално изнудване
- Секстинг с цел злоупотреба
- Заснемане на нападение
- Upskirting и creepshots
- Цифрово воайорство

Фигура 1. Основни стъпки, ако сме жертва на КТН; Източник: CI





Членове на Директива 2024/1385

които се отнасят към КТН

Член 5

Споделяне без съгласие на интимни или манипулирани материали

1. Държавите членки гарантират, че следното умишлено деяние се наказва като престъпление:

а) Осигуряване на достъп на обществеността, чрез информационни и комуникационни технологии (ИКТ), на изображения, видеоматериали или подобни материали, изобразяващи явни сексуални дейности или интимните части на дадено лице, без съгласието на това лице, когато има вероятност това деяние да предизвика тежки вреди на това лице;

б) Създаване, манипулиране или изменение и последващо осигуряване на достъп на обществеността, чрез ИКТ, до изображения, видеоматериали или подобни материали, които създават представата, че дадено лице участва в явни сексуални действия, без съгласие на лицето, когато има вероятност това деяние да причини тежки вреди на това лице;

в) Отправяне на заплаха за извършване на деянията, посочени в буква а) или б), за да се принуди дадено

Членове на Директива 2024/1385

лице да извърши, да се съгласи с извършването или да се въздържи от извършването на определено действие.

2. Параграф 1, букви а) и б) от настоящия член не засяга задължението за зачитане на правата, свободите и принципите, установени в член 6 от ДЕС, и се прилага, без да се засягат основните принципи, свързани със свободата на изразяване на мнение и свободата на информация и свободата на изкуството и науката, въведени в правото на Съюза или в националното право.

Член 6

Киберслеждане

Държавите членки гарантират, че се наказва като престъпление умишленото многократно или непрекъснато поставяне на друго лице под наблюдение без неговото съгласие или законно разрешение за такова наблюдение чрез ИКТ с цел преследване или наблюдение на придвижването или дейността на това лице, когато има вероятност това деяние да причини тежки вреди на въпросното лице.





Член 7

Кибертормоз

Държавите членки гарантират, че следното умишлено деяние се наказва като престъпление:

- а) Многократна или непрекъсната проява на заплашително поведение чрез ИКТ, насочено срещу дадено лице, най-малкото когато това поведение включва заплахи за извършване на престъпления, когато това поведение е вероятно да причини основателен страх на лицето за собствената му безопасност или за сигурността на зависимите лица;
- б) Проява, заедно с други лица, чрез ИКТ и по такъв начин, че да стане обществено достояние, на заплашително или обидно поведение, насочено срещу дадено лице, когато това поведение е вероятно да причини тежки психически вреди на това лице;
- в) Нежелано изпращане, чрез ИКТ, на дадено лице на изображение, видеоматериал или друг подобен материал, изобразяващ гениталии, когато това деяние е вероятно да причини тежки психически вреди на това лице;
- г) Осигуряване на достъп на обществеността, чрез ИКТ, до материали, съдържащи личните данни на дадено лице, без съгласието на това лице, с цел подбуждане на други лица към причиняване на физически или тежки психически вреди на това лице.



Член 8

Подбуждане към насилие или омраза в киберпространството

1. Държавите членки гарантират, че умишленото подбуждане към насилие или омраза, насочено срещу група лица или срещу член на такава група, определена въз основа на пола, посредством публично разпространяване, чрез ИКТ, на материали, съдържащи такова подбуждане, се наказва като престъпление.
2. За целите на параграф 1 държавите членки могат да изберат да налагат наказания само за деяния, които са извършени по начин, който може да наруши обществения ред, или са заплашителни, обидни или оскърбителни.

Член 49

Транспониране

1. Държавите членки въвеждат в действие законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с настоящата директива, най-късно до 14 юни 2027 г. Те незабавно информират Комисията за това. Когато държавите членки приемат тези разпоредби, в тях се съдържа позоваване на настоящата директива или то се извършва при официалното им публикуване. Условиата и редът на позоваване се определят от държавите членки.
2. Държавите членки съобщават на Комисията текста на разпоредбите от националното законодателство, които те приемат в областта, уредена с настоящата директива.





Кибер и технологично насилие в българското законодателство

В началото на 2025 г., по инициатива на Министъра на правосъдието е създадена **работна група за справяне с домашното насилие** от над 70 експерти: практики, съдии, следователи, прокурори, представители на академичните среди, неправителствения и правителствения сектор. Сред задачите на групата е изготвянето на **цялостен анализ на българската нормативна уредба** за съответствието ѝ с Директива (ЕС) 2024/1385 и подготвянето на необходимите нормативни промени.

Към февруари 2026, няма публична информация за резултатите от дейността на работната група. Според [доклада за равенството на половете в България за 2025](#), все още **няма специфични национални разпоредби относно кибер насилието**. Защита може да се получи чрез гражданска и наказателна процедура в съответствие със закона и вида претърпяно насилие. Българската законова уредба все пак съдържа 6 разпръснати фрагмента, с които кибер и технологичните форми на насилие към жени могат да бъдат адресирани. **Чл. 32 от Конституцията на Република България** урежда личния живот на всички граждани като неприкосновен и на практика забранява заснемането (независимо дали е с цел разпространение, независимо дали е в условията на сексуален акт или голота) на хора без тяхното съгласие. АLINEA 2 гласи „Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на

други подобни действия без негово знание или въпреки неговото изрично несъгласие освен в предвидените от закона случаи“. Този член би следвало да се отнася до всички форми на заснемане на жертви, без тяхно знание, независимо къде и от кого.

Чл. 144а, ал. 2 от Наказателния кодекс на България криминализира всички форми на следене, включително следенето извършвано с технологични средства и нежеланата комуникация в дигиталната среда. Текстът гласи, че „Следене по ал. 1 е всяко поведение със заплашителен характер срещу конкретно лице, което може да се изразява в преследване на другото лице, показване на другото лице, че е наблюдавано, навлизане в нежелана комуникация с него чрез всички възможни средства за комуникация“. Тук фразата „всички възможни средства на комуникация“ предполага включване и на комуникация чрез технологични средства.

Чл. 155а от НК се отнася до склоняването към сексуални действия и може да бъде отнесен към поведението, познато като online grooming и обикновено засяга хищническо поведение към непълнолетни или малолетни. Текстът от НК гласи, че „който склонява друго лице към проституция или свежда към блудствени действия или съвкупление, се наказва с лишаване от свобода до три години и глоба от хиляда до три хиляди лева“. Това се съотнася към поведението, описвано в литературата като *online grooming*.

Чл. 159 от НК криминализира порнографията. В България създаването, споделянето и разпространението на порнография е забранено. В алинея 2 изрично се споменава и „Който разпространява чрез информационна или съобщителна технология или по друг подобен начин





порнографски материал“ също подлежи на наказание, което е по-голямо, ако са въввлечени и лица под 18-годишна възраст в произведеното или споделеното съдържание. Макар и често описван като „мъртъв член“ от правозащитници и активисти, макар и насочен по-скоро към съхранението на „публичния морал“, отколкото към закрилата на правата на личността, член 159 всъщност криминализира много от формите на изнудване и насилие с технологични средства и онлайн. Включително, но не ограничено до порното за отмъщение, разпространение на изображения със сексуален характер, разработването на фалшиви изображения със сексуален характер и др.

Чл. 162 (1) от НК на практика криминализира речта на омразата в онлайн пространството (наравно с всички други публични пространства). Текстът гласи: „Който чрез слово, печат или други средства за масова информация, чрез електронни информационни системи или по друг начин проповядва или подбужда към дискриминация, насилие или омраза, основани на раса, цвят на кожата, произход, народност или етническа принадлежност или сексуална ориентация, се наказва с лишаване от свобода от една до четири години и с глоба от пет хиляди до десет хиляди лева, както и с обществено порицание“. Изричното споменаване на възможността за използване на „електронни информационни системи“ е положително развитие. Такова е и добавянето на сексуалната ориентация като признак, въз основа на който дадено лице може да бъде предмет на дискриминация или език на омразата. За съжаление обаче, сред изброените защитени характеристики не фигурира „пол“;

Чл. 5, ал. 4 от Закона за защита от домашното насилие приобщава и дигиталната и технологична комуникация

към каналите за осъществяване на контакт между жертва и насилник, които трябва да бъдат прекъснати, когато жертвата поиска и получи закрила от домашно насилие (ДН). Текстът гласи, че сред мерките за защита от ДН е и „забрана на извършителя да осъществява контакт с пострадалото лице под каквато и да е форма, включително по телефон, чрез електронна или обикновена поща и факс, както и чрез всякакви други средства и системи за комуникация при условия и за срок, определени от съда“;

В допълнителните разпоредби на Закона за защита от дискриминация се упоменава, че „тормоз“ и „сексуален тормоз“ могат да бъдат изразени „физически, словесно или по друг начин“. Това би могло да се тълкува като обхващащо и изразяване в кибер пространството, но експлицитно споменаване на информационни и комуникационни технологии и технологични средства отсъства.

Чл. 15 от Проекта на Закон за използването и развитието на изкуствения интелект, внесен за разглеждане и обсъждане през 2025 година на практика забранява разпространението в социалните мрежи на дийпфейкове (deepfakes) без изричното съгласие на човека, чийто образ или глас биват пресъздадени от изкуствен интелект.

През февруари 2026 година медиите разпространяват информация, че в затворени Telegram групи или в платени сайтове за възрастни са разпространени видеа и снимки на жени в интимни ситуации (сексуални и/или съдържащи голота). Жертвите са заснети без да знаят, докато посещават козметичен салон в Бургас и Казанлък и гинекологичен кабинет в София. Сред заснетите жертви има малолетни и непълнолетни момичета. За





поне едно от видеата е известно, че е видяно поне 50 000 пъти. Гинекологът, собственик на кабинета, в който са заснети част от видеата, е задържан за 22 часа и вследствие – освободен. КЗЛД отказва директна намеса по случая, защото кадрите не позволяват идентификация на конкретни лица на записите.

Въпреки практическото наличие на законови текстове, които предоставят пътеки, с които жертвите на кибер и технологично насилие могат да търсят и защитават правата си, експлицитното въвеждане на кибер и технологичните престъпления, основани на пола, в българското законодателство е крайно наложително. Това не само ще назове и регламентира новите явления, за които цялостно гражданската и юридическата система е преобладаващо неподготвена. Криминализирането на „по-леките“ форми на сексуално насилие може да доведе до достъп до системата към насилници, които извършват и други, по-„тежки“ сексуални престъпления. Кибер и технологичното насилие рядко е изолирано само по себе си и обикновено е обвързано с други по-„традиционни“ форми на полово базирано или сексуално насилие, които обаче са по-щателно прикривани от насилниците.

Един от най-мощните случаи на сексуално насилие, завършил с осъдителни присъди на десетки насилници и придал нов облик на движението за женски права, излиза наяве именно заради криминализиране на технологично насилие. Случаят Жизел Пелико става известен в цял свят, след като през 2024 година тя се отказва от правото на анонимност и застава с лицето си във френския съд, където подсъдим е съпругът ѝ и десетки негови съучастници. В продължение на десетилетия тя е неусетно дрогирана и изнасилвана от съпруга си и много познати и непознати за нея мъже. Самата тя научава за

насилието след като полицията ѝ показва видеозаписи. Видеозаписите са открити в устройства на съпруга ѝ, които са разследвани след като той е заловен да прави снимки под полите на непознати жени на публично място (upskirting) – необвързано със случая на насилие. Случаят Пелико е емблематичен не само защото поражда идеята за прехвърляне на срама от жертвата към извършителя, но и защото демонстрира, че по-„малките“ актове на насилие могат да бъдат вход към прекратяване на системно широкомащабно поведение от един и същ насилник. (За таксономия на типовете кибер и технологично насилие, вижте Приложение 1)





Чеклист на кибер и ТЕХНОЛОГИЧНОТО НАСИЛИЕ

или как да разберем, ако ние или някой
около нас е жертва?

Кибер и технологичното насилие се развива във виртуалния свят – пространство, което живее собствен живот извън физическото време-пространство, което обитаваме и с което сме свикнали. Възприемането на този виртуален свят като по-далечен и почти „нереален“, като свят, от който можем лесно да се откъснем и който трудно ще ни навреди, създава сериозен риск от negliжиране и дори нормализиране на КТН. Кибер и технологичното насилие може да ни нарани по абсолютно същия, и дори по-силен, начин като физическото или сексуалното насилие в реалността.

Представяме списък от поведения в кибер пространството, които биха могли да се определят като проблемни, причиняващи вреда и представляващи тормоз и насилие. Подчертаваме, че списъкът не е изчерпателен и че не всички действия в него са незаконни, макар и да се възприемат като зловредни, опасни и неморални. Всяко едно от тези действия обаче е червен флаг – индикация, че връзката е токсична или насилствена и трябва да потърсите помощ или да предложите съдействие.

Чеклист на кибер и технологичното насилие

- ☐ Настоява да знае всичките Ви пароли и контролира или ограничава достъпа Ви до електронни устройства, интернет, ел. поща или социални медии
- ☐ Инсталира в дома Ви камери или приложения за проследяване на електронните Ви устройства без Ваше знание или съгласие
- ☐ Получавате много съобщения и обаждания, които изискват незабавен отговор, особено когато не сте вкъщи
- ☐ Получавате заплашителни, обидни или унижителни съобщения (насочени към Вас или към Ваши приятели и роднини) по имейл, SMS, в социалните мрежи или в приложения
- ☐ Публикува онлайн или споделя с други (в социални медии или приложения) интимни снимки и видеа или лична информация без съгласието Ви
- ☐ Заплашва да сподели подобни материали, ако докладвате упражнявано домашно насилие във всичките му форми



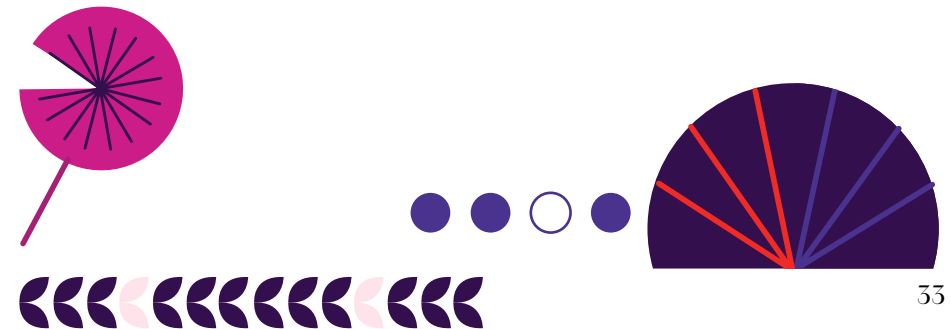


- ☐ Има достъп до Вашата банкова сметка и онлайн банкиране, контролира средствата и разходите Ви или ги използва без Ваше разрешение или знание
- ☐ Разпространява слухове или лъжи за Вас онлайн или в комуникация с други лица (по телефон или чрез приложения)
- ☐ Подстрекава други хора към тормоз върху Вас онлайн или чрез технологични средства
- ☐ Принуждава Ви да участвате в сексуална комуникация онлайн, с цел изнудване и тормоз
- ☐ Изпраща Ви порнографско съдържание без Ваше съгласие
- ☐ Принуждава Ви към сексуален контакт, който заснема без Ваше съгласие
- ☐ В случай на блокиране от Ваша страна, продължава да Ви тормози посредством профили или номера на други лица или нови, фалшиви профили

Какво да направим, ако сме жертва на кибер или технологично насилие?

Хората, подложени на кибер или технологично насилие, могат да предприемат някои действия, за да се защитят или преустановят тормоза – **да блокират и докладват извършителите в социалните мрежи, да блокират телефонния им номер, да сменят паролите си, да променят настройките за поверителност, да ограничат кой и какво вижда на профила им, да се обърнат към компетентните институции.** За съжаление, жертвите на интимно насилие често не могат да прибегнат до тези мерки, защото в повечето случаи живеят с насилника или поддържат контакт с него – например заради общо дете, общ бизнес и т.н. Те могат да бъдат принудени да възстановят достъп до устройствата или профилите си или пък да понесат физическо насилие с цел „наказание“.

Въпреки това, има три основни стъпки, които потърпевшите биха могли да предприемат, за да получат съвет, помощ и закрила.





1

Споделете за кибер тормоза с организация, работеща с жертви на насилие **и/или компетентни органи и следвайте единствено техните указания и инструкции**

2

След консултация с професионалист, съхранявайте доказателства за кибер тормоза (скрийншот на обидни и заплашителни съобщения, имейли, постове, фалшиви профили, фалшиви снимки и видеа, доказателства за инсталирани проследяващи устройства и т.н.)

3

Не съхранявайте доказателствата на устройство, до което насилникът има достъп! Възможност е да помолите за това Ваш близък, **но не предприемайте рискове** и винаги следвайте съветите на експертите

Фигура 2. Основни стъпки, ако сме жертва на КТН; Източник: CI

Как да работим с жертви на КТИДН?

Кибер и технологичното насилие е част от спектъра на домашното насилие. Изследването на Института за контраинтуитивни идеи показва еднозначно, че то присъства в 83% от случаите на домашно насилие. Кибер и технологичното насилие трябва да бъде адресирано, защото носи трайни негативни последици за жертвите. При прекъсването на физическия контакт дигиталните и технологични канали за достъп на насилника до жертвата стават основен способ за продължаващ тормоз и контрол. Прекъсването на дигиталната връзка е ключов процес от цялостното освобождаване на жертвата и процесът на насилието може да се счита за приключен, само когато и той бъде елиминиран. Закрилата на жертвата от дигиталния и технологичен процес е неотменна част от нейното възстановяване и условие за пълноценното ѝ реинтегриране в обществото.

Изследването в проекта „Невидими данни“ показва, че най-добрият подход за интервенция, закрила и рехабилитация е да се разчита на вече изградените умения и ресурси на социалните работници и практиците от първа линия на борба с домашното насилие. Цялостният подход към жертвата е процес, в чийто контекст трябва да бъдат разположени нови знания и инструменти за адресиране на кибер и технологичните аспекти на насилието.

Възможно е практиците да се сблъскват с някои





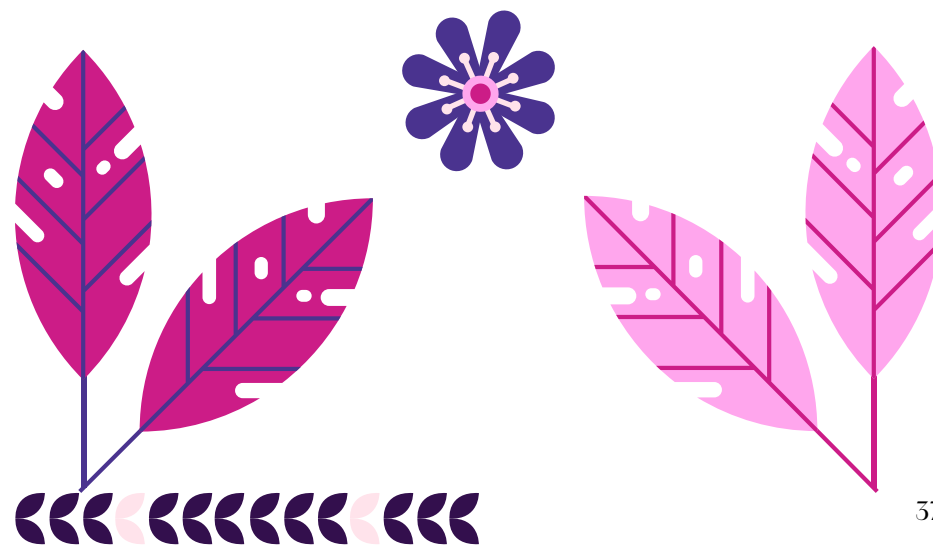
трудности при работата с жертви на домашно насилие с кибер или технологични измерения. Една пречка може да бъде недостатъчното познаване на дигиталното измерение на насилието, например кибер слеждане или контрол на банкови сметки и карти. Причината за непознаването не бива да се търси в нежелание от страна на практиците, а по-скоро в твърде бързото развитие на някои технологии. Възможно е и жертвите да изпитват колебание да споделят, поради срам и страх, че партньорът им разполага с интимни снимки или видеа, заснети с тяхно съгласие.

Въз основа на налична литература и най-вече на разговорите с експертите, които взеха участие в пилотирането на индикаторите по проекта „Невидими данни“, бихме могли да изведем следните насоки за работа с жертви на домашно насилие с кибер измерение:

- ✱ Препоръчително е практикът **изрично** да попита жертвата дали е била обект на поведения и действия, които могат да се окажат като кибер тормоз;
- ✱ Ако жертвата се колебае дали това ѝ се е случвало, експертът би следвало да **обясни** какви са различните кибер и технологични проявления на насилието, вкл. давайки **конкретни примери** и подчертавайки, че насилието в кибер пространството е **част от континуума на насилието**, за който говори Препоръка №1 на GREVIO;
- ✱ Експертът би следвало да включи сведенията за кибер насилието в доклада/досието на жертвата, както и да е подготвен да я насочи към съответния компетентен орган и да начертае основните стъпки, които жертвата да предприеме (напр. съхранение на доказателства за насилието);

- ✱ Съвместно с жертвата, експертът може да изготви **план за безопасност**, който включва контакти и имена на близки за жертвата хора, на които тя има доверие и които биха могли да помогнат в спешни случаи;
- ✱ В случай че разработват и изпълняват програми за работа с извършители, практиците могат да включват в тях и модули и информация, свързани с кибер и технологичните проявления на домашното насилие като **акцентират върху психологическите и емоционалните вреди, които то причинява на жертвите**.

Отвъд непосредствената работа с жертвите, призоваваме практиците да инициират и да продължават да участват активно в проекти, кампании и инициативи, които подпомагат събирането на данни за кибер и технологичните проявления на насилието, както и увеличаването на информираността и капацитета на НПО сектора и компетентните институции да се борят и справят с този тип насилие.

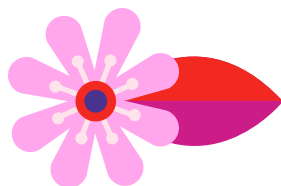
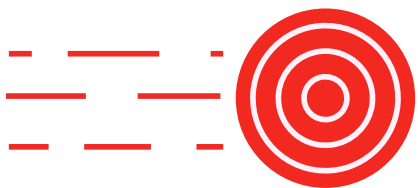




Как да говорим за КТН?

Важно е да говорим за кибер и технологичното насилие над жени, защото то се случва. Това може да образова практики, правозащитници и граждани – да го разпознават, да го идентифицират, да го откриват в своя живот или в животите на околните. Говоренето за него на всекидневен ниво сменя булото на страха от непознатото и необятното и то вече става победимо. Говоренето за него на експертно ниво позволява разбирането на характеристиките и тенденциите на насилието по начин, който може да бъде основа за противодействие. Говоренето за него на публично ниво може да доведе до положителни законодателни и културни промени, които са единственият инструмент за ликвидирането му.

Въпреки това, има правилен и грешен начин да говорим за КТН. Правилният начин е с уважение към жертвите, с факти, с данни, с убедителни аргументи и с реални истории. За да подпомогнем на НПО практиките и правозащитници да комуникират своето знание и експертиза по обществено полезен начин, сме разработили кратък пътеводител за комуникация, основана на данни, в социалните медии.



Как да говорим за насилие основано на пола, с грижа за хората и обществото?

Когато се говори публично за насилие, единствената цел трябва да бъде постигане на социална и политическа осъзнатост към обществените и контекстуалните особености, които позволяват насилието да се случва и (в случаите, в които е валидно) да остане безнаказано. Основният приоритет е жертвите да бъдат защитени и да не са подложени на вторична виктимизация (тоест, да не бъдат принудени отново да преживяват травматични събития и/или да бъдат подложени на допълнително страдание и болка). За целта, НПО, дори и когато не са професионални комуникатори, трябва да разпространяват своето знание и експертиза, като задължително междувременно се грижат за хората, преживели насилие. Ето основните правила ([основани на етичния кодекс на професионалните журналисти](#)), които трябва да се следват, за да се осигури постигането на целта с грижа за жертвите





Минимизирайте вредите

Ако разказвате истории от вашия опит, с които илюстрирате реалността на КТН в България, винаги го правете, само ако сте убедени, че ползите надделяват над вредите. Трябва да сте сигурни, че историята е достатъчно убедителна и въздействаща, за да успее да достигне до широката публика и да има способността да промени нагласите им към проблема. В същото време, трябва да сте убедени, че травмата и страданието на жертвата, при споделяне на историята, ще бъде сведена до минимум – особено психологическата и емоционалната травма, която често самите жертви не очакват.

Защитавайте личното пространство и автономността на жертвите

Никога не разкривайте имена или лична информация за жертвите, чиито истории разказвате. Избягвайте да споделяте детайли, които могат да помогнат на недоброжелатели да идентифицират участниците в историите. Никога не споменавайте имена на насилници, преди те да бъдат доказано виновни в съда.

Защитавайте достойнството на жертвите

Фокусирайте се върху моралните заключения от историите, които разказвате и върху евентуалното им въздействие върху релевантните политики. Не споделяйте подробности, с цел да привлечете внимание с шок фактор. Сведете разказите за физическо и сексуално насилие и подробностите около него до минимум, ако изобщо смятате, че са ключови за разказването на историите.

Фокусирайте се върху процеса, контекста и решенията

Говорете с равен тон. Не наблягайте на емоции, било то положителни или отрицателни. Излагайте факти, които можете да защитите с опита си или с данни. Описвайте социален контекст (законови, политики, регулации), а не обстоятелства (травми, подробности, детайли около физическо насилие). Отправяйте критики към закони, политики и културни норми. Предлагайте решения и отправяйте конкретни препоръки за действия. Не само идентифицирайте проблема, но и предложете решение за него.





Какво са данни, с които можем да комуникираме?

Всяко струпване на факти представлява данни. Свикнали сме да обвързваме идеята за данни с числа, проценти и графики. Информацията от директен достъп с конкретни събития също представлява данни. Разказите на жертви на КТН, когато те са систематизирани и коректно описани, също представляват данни. Данните, фактите и научното знание са ценни инструменти, върху които може да се изгради промяна в гражданските нагласи, с които обикновено се обосновават конкретни политически решения и с които може да се противодейства на дезинформацията, фалшивите новини и идеологизираното говорене.

До какви данни имат достъп НПО, които работят на първа линия на борбата с насилието над жени?

Количествени данни

НПО разполагат с достатъчно информация от всекидневната си работа, за да могат да произвеждат значими масиви от количествени данни. Например, оценката на риска, която трябва да се изготвя при всеки регистриран случай на домашно насилие, съдържа структурирана информация за особеностите на развилата се история. Тази информация може да бъде превърната в данни, ако бъде структурирана и

Какво са данни, с които можем да комуникираме?

„натрупванията“ в регистрираните карти преминат в категории. Тогава, експертите могат да изработят цялостна картина на насилието, която да онагледят с числа и проценти, различни от наратива и описанието на всеки отделен случай. Съществуват и отворени бази от данни, чиито резултати могат да бъдат използвани, за да илюстрират аргументите и твърденията на експертите.

Качествени данни

НПО разполагат с по-голям набор от качествени данни, отколкото те самите осъзнават. Всяка история, споделена от пострадалите, е информационна единица. Сама по себе си тя съдържа данни. Тя придобива повече валидност, когато е част от по-голям масив от истории – по възможност структурирани и категоризирани. Историите и разказите могат да бъдат използвани за илюстрация и онагледяване на тенденции и реалности, с които практиците се сблъскват всеки ден.

Експертиза и фактология

Експертните оценки на НПО също могат да бъдат основа за ефективна комуникация, основана на данни и наука. В тази категория попадат експертни становища и оценки за определени политики или събития. Те могат да бъдат съчетавани и онагледявани с данни. Тук попада и комуникацията, която обяснява на ясен и общодостъпен език термини от полето на експертиза (в случая, например, терминологията около различните форми на КТН) или която разяснява бюрократични пътеки и/или административни процедури така, че да могат да бъдат достъпни за всички граждани.





Как да структурираме комуникацията в социалните мрежи?

Данните са разликата между личното мнение и обективната истина и за това е важно те да бъдат силно и често комуникирани в каналите, които често размиват границата между двете – социалните медии. Ключово послание: или т.нар. „Master message“ е стратегически подход, при който първо формулирате в рамките на 1/3 до 1/2 страница ясно, стегнато и добре обмислено основното послание – с точните думи, тон и акценти, които искате да използвате. Този базов текст съдържа ключовата информация, основните аргументи и ценностното Ви позициониране и служи като фундамент за всички останали комуникационни формати – имейл, пост, стори, нюзлетър, изказване, презентация, рекламен материал и др. Така гарантирате последователност, разпознаваемост и стратегическа яснота във всяка външна и вътрешна комуникация.

Структура на пост в социалните медии

Обикновено всеки пост в социалните медии съдържа два основни компонента – описание и визуален компонент. Описанието е най-подходящата форма, в която да споделите основното си послание. Визуалният компонент е най-подходящата форма, в която да използвате данните за онагледяване или подкрепа към основното ви послание.

Описанието обикновено е в текстови формат. Спрямо

Как да структурираме комуникацията в социалните мрежи?

стила и вътрешната стратегия на всяка организация, в него могат да бъдат добавяни и други компоненти (например емотикони). Текстът в описанието в постове, които целят да комуникират послания, обосновани с данни и експертиза, трябва да следва пет основни правила, които гарантират за яснота, достоверност и достъпност.

Правило 1

Започнете с основното си послание

Структурирайте основния си аргумент в едно ясно и по възможност просто изречение (8-10 думи). Ако аргументацията ви изисква повече пояснения и по-дълъг текст – запазете ги за последващите изречения.

Правило 2

Бъдете кратки и ясни

Опитайте се цялото описание да не надвишава 150 думи. Форматът на социалните медии не предполага дълго внимание на четящите и рискувате посланието ви да остане недочетено и съответно недоизказано.





Правило 3

Не използвайте термини, които широката общественост не разбира

освен ако не разполагате с достатъчно пространство да ги обясните. Добра практика е обяснението на термините да се случва в специални, предназначени за това, постове.

Правило 4

Не подценявайте аудиторията

Не обяснявайте излишно очевидни неща и не се съмнявайте в способността на четящите да ви разберат, ако изложите ясно аргументите си.

Правило 5

Поместете допълнителни ресурси с обяснение и връзки (линкове)

ако призовавате към действие. Бъдете ясно за това към кого се обръщате и ако търсите гражданска активност (подписване на петиции, запознаване с правила, покана за възползване от допълнителни ресурси) дайте директен и лесен достъп, който да помогне при очакваните следващи действия.

Как да разказваме истории с данни?

Използването на данни или научно познание в комуникацията в социалните медии не трябва да бъде самоцелно. То трябва да цели онагледяване и разясняване на конкретно послание, което организацията се опитва да отправи към широката общественост и/или към хората, изготвящи политики. Данните трябва да разказват истории, за да подкрепят послания. Те трябва да са ясно и коректно изложени. Ето как:

Истории с количествени данни

Количествените данни обикновено са най-разпознаваемите от широката общественост като достоверни и необорими. При боравенето с количествени данни приоритизирайте споделянето на проценти.

Правило 1

Избирайте данни, които категорично онагледяват твърдението или посланието ви

Ако искате да покажете, че някое явление е значимо и заслужава обществено внимание, използвайте процента на честота на проявление (тоест, в колко процента от случаите се среща то). Ако използвате данни, които





се отнасят към посланието ви индиректно, важно е да обясните връзката между данните и твърденията, които отправяте в поста.

Правило 2

Използвайте визуализации

Количествените данни позволяват лесно онагледяване в графики и чартове. Те са ясно разбираеми от широката общественост и посланието достига бързо, ясно и ефективно. Етикетите на данните трябва ясно да показват коя стойност за каква категория се отнася. Стойностите винаги трябва да са ясно изписани.

Правило 3

Винаги цитирайте източника на данните

Достоверността на данните обикновено се носи от източника, който може да защити методологията на събирането и анализирането им. Винаги трябва ясно и от пръв поглед публиката да може да разбере от къде/от кого идват данните. Описвайте източника директно и еднозначно. Подходящ е форматът „Източник: [име на източника]“

Правило 4

Винаги бъдете откровени с ограниченията на данните

Как да разказваме истории с данни?

Всички данни имат определени ограничения, които могат да бъдат използвани като уязвимости, особено когато не сме прозрачни и откровени по отношение на тях с публиката си. Важни уточнения, които винаги могат да бъдат споменати, включват:

- ☀ **Времевия обхват на данните** – кога са събрани и за кой исторически период се отнасят.
- ☀ **Съвкупността, която обхващат** – сред кои хора конкретно са събрани данните

Пример





Истории с качествени данни

Качествените данни са удобни за разказване на истории. Директните цитати от потърпевши, експерти или практики служат добре за целите на илюстрацията и онагледяването. Обикновено имат силно въздействие и често са изказани на разбираем език. Ето основните правила, които да следвате, при комуникацията с качествени данни

Правило 1

Винаги ясно посочвайте, когато публикувате цитат

Най-лесният начин за това е да поставите цитата в кавички и/или курсив.

Правило 2

Винаги цитирайте коректно

Най-добрият вариант е да цитирате думите директно. Понякога това не е възможно, поради неяснота или когато има нужда цитатът да се съкрати. В тези случаи ясно показвайте, когато има вмешателство в оригиналния изказ. Удобен начин да го направите е като използвате квадратни скоби ([]) и в тях поставите многоточие (когато съкращавате) или думата/думите, с които заменят оригиналния цитат.

Правило 3

Винаги цитирайте източника

Той може да бъде анонимен и посочен едновременно. Без да изписвате имената, когато цитирате пострадали, можете да посочите говорител през позиция, функция, или ключова характеристика. Например „разказ на оцелял от насилие“, „оценка на експерт“, „разказ на активист“ и др.

Пример



Насилникът я принуждава да му даде споделена точка за местоположение, за да знае по всяко време тя къде се намира. Ако жената я изключи, следва телефонно обаждане със заплахи и обиди. Непрекъснат контрол върху живота ѝ, къде е, с кого е, защо е там, кога ще се прибере, засичал кога свършва работният ѝ ден и кога се прибира. Често тя го виждала, че я следи, а понякога той ѝ изпращал снимки, от деня ѝ, за да знаела, че той е наблизо.

- Разказ на социален работник, предоставящ закрила и консултация на жертви на домашно насилие



Домашното насилие все по-често има дигитално лице – чрез проследяване, контрол върху профили, заплахи за разпространение на материали и отнемане на устройства.

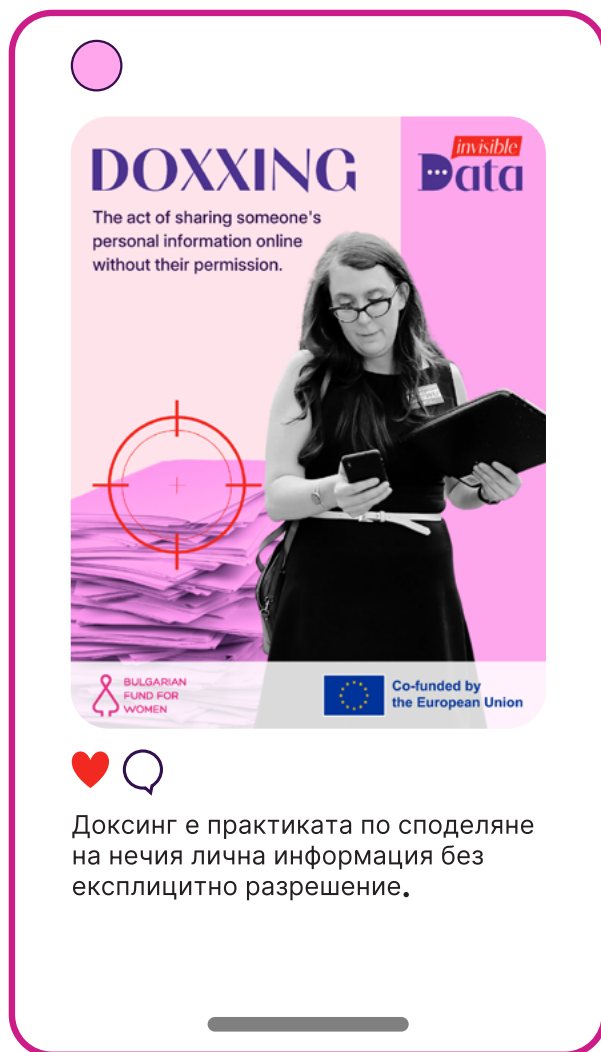




Терминология и познание

Форматът на социалните медии позволява научна комуникация, която да повиши запознатостта на обществото с КТН над жени с кратки, точни и ясни публикации, които да въведат в публичното пространство лексиката около проблема. Добра практика е да се съсредоточите върху един термин и да използвате визуализацията или описанието, за да го представите ясно и достъпно за публиката. Така образовате гражданите и правите процесите по-разбираеми.

Пример



Как и кога да влизаме в диалог

Всички НПО, които имат онлайн присъствие са наясно с рисковете на публичната комуникация, особено в социалните медии. Нелинейната комуникация предполага, че публиката може да избере да влезе в диалог с организацията и това е желан ефект, когато комуникацията е доброжелателна и нежелан в останалите ситуации.

Важно е да имате предвид, че носите отговорност за цялото съдържание на уебсайта на организацията ви, за който отговаряте. Това включва и коментарите, ако има опция за оставяне на такива. Парадоксално, ако коментари на външни потребители включват реч на омразата и/или друг тип забранено със закон съдържание, отговорността да ги свалите е ваша.

Когато получите коментари под своите постове, с които не сте съгласни, пред вас стоят две опции. Първата е по линия на стратегията „Не храни троловете“ („Don't feed the troll“) и предполага да игнорирате или изтриете коментара. Имате опцията в повечето социални медии да блокирате потребители, чиито коментари не искате да виждате на профила на организацията ви.

Втората възможна стратегия е да отговорите на недоброжелателите. Ако изберете тази опция, трябва да приемете риска, че негативите от тази интеракция най-вероятно ще „полепнат“ по вашия имидж. При всички случаи, ако решите да влезете в спор и/или диалог с недоброжелатели, опитайте се да спазите следните три правила





Правило 1

Не обиждайте, не осмивайте, не набеждавайте

Разногласията трябва да останат на идейно ниво и никога не трябва да опирате до лични аргументи, дори и когато недоброжелателят е публична личност. Силата на аргументите ви трябва да произлиза от посланието ви, а не от недостатъците на опонента.

Правило 2

Придържайте се към фактите, данните и познанието

Запазете самообладание и не се поддавайте на емоции. Истината е на ваша страна, когато комуникирате с данни и факти. Вашето знание, основано на данни и факти, не е равнопоставено на нечие мнение, неосновано на стабилна аргументация.

Правило 3

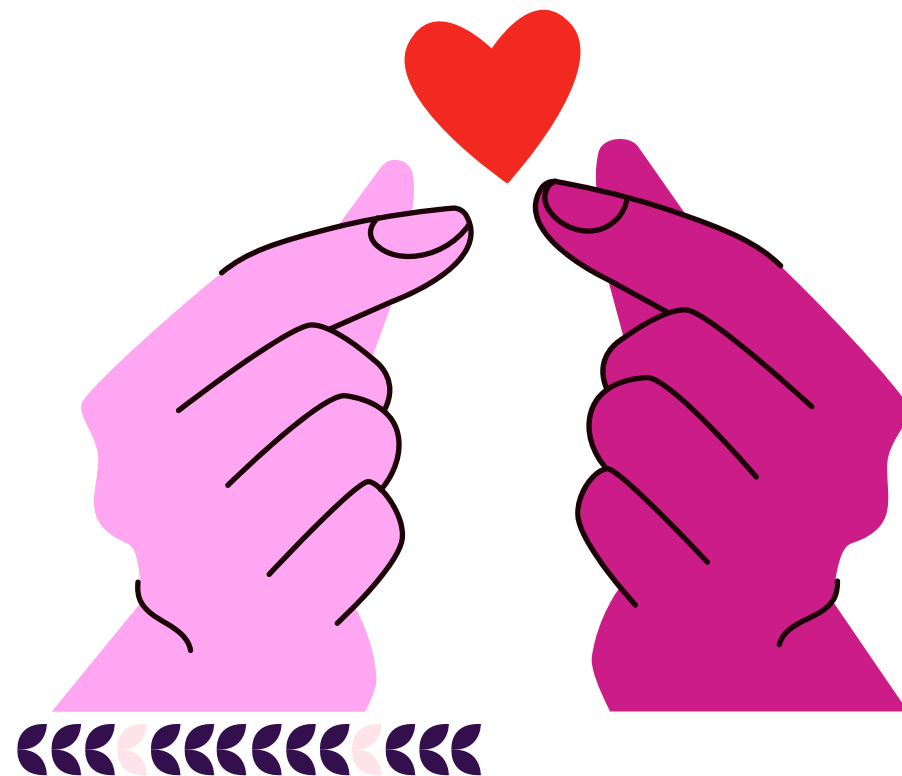
По-умният прекратява комуникацията, без да отстъпва

Изложете аргументите си и напуснете диалога, ако той не прераства в градивна критика. Не се чувствайте длъжни да кажете последната дума, особено когато още първата е била истинна, навременна и основана на факти.

Как да разказваме истории с данни?

Насоките и информацията, споделени в този наръчник имат насочващ и пожелателен характер. Те не са изчерпателни и общовалидни. Но те няма и как да бъдат – няма правила, които са монолитно истинни и приложими винаги и навсякъде. Ако можем да си позволим препоръка или предписание, от което всички хора, които се опитват да се противопоставят на КТН, да могат да се възползват винаги и навсякъде, то тя би била една:

Нека ви води желанието да няма повече потърпевши жени, деца и мъже, и убеждението, че пътят към разрешаването на обществените проблеми е ясният, достоверен и откровен разговор за възможните и постижими навременни решения. От всички и за всички.





Приложение

Шаблони и инструменти за публична комуникация по темата на КТН

Приложение 1

Таксономия на кибер и технологичното насилие, основано на пола

Назоваването на новите явления са първата крачка към тяхното овладяване. За да можем да противодействаме на дигиталните и технологични форми на насилие, трябва първо да ги назовем и разберем. За тази цел предлагаме една кратка основополагаща таксономия на кибер и технологичното насилие, която да послужи за по-добро разбиране от страна на практики, специалисти, изследователи и граждани. Списъкът не е изчерпателен.

Телефонен тормоз (Nuisance calls)

Многократни обаждания, често денонощно и особено през нощта, целящи да разтревожат жертвата, да нарушат нормалния ѝ ритъм на живот чрез стряскащи звуци или обиден език.

Заплахи за насилие (вкл. изнасилване и смърт) по телефон или чрез други ИКТ

Използване на съобщения и съдържание за предаване на заплахи към жертвата, нейното семейство, деца или дори имущество. Те биха могли да са еднократен акт, или системна практика по тормоз и нахлуване в личното пространство на жертвата. Извършителите могат да записват непристойни съобщения, да създават записи в календара или аларми на устройствата на жертвите, за да ги излагат многократно на вредно съдържание.

Създаване на порнография без съгласие

Записване на интимно съдържание без знанието на жертвата. Това включва записи на сексуални актове, заснемане на нищо неподозиращи жени (т.нар. „creepshots“) или записване на самото насилие и изнасилване. Разпространението на това съдържание чрез социални медии или в тъмната мрежа (dark web) е често кулминацията на насилието, която в контекста на дигитално насилие в интимни отношения е предхождана от дълъг период на заплахи за публикуване и разпространение. Мотивите варират от отмъщение („порно за отмъщение“) до изнудване или лично удовлетворение.





Секстинг с цел злоупотреба (abusive sexting)

Споделяне чрез електронни средства и без съгласието на жертвата изображения с голота или сексуално съдържание. Форма на този тип дигитално насилие е и засегнатият в Директивата киберфлашинг (Cyberflashing), който представлява изпращане на нежелани сексуални снимки (често с голото тяло на изпращащия) и съобщения към жертвата.

Заснемане на нападение (filmed assault)

Известно още и като „happy slapping“, е акт на нападение (физическо или сексуално) с цел записване и споделяне онлайн на нападението над жертвата и/или последиците от извършеното насилие. Това е злоупотреба с образа на жертвата, която се основава на властовата динамика между насилника и жертвата. Сами по себе си тези материали разобличават престъплението, извършено от насилника, но често насилниците използват този материал, за да изнудват жертвата. Понеже срамът от преживяното насилие се носи от жертвата.

Воайорство и „creepshots“

Заснемане под полите („upskirting“), под блузите („downblousing“) на жените, заснемане на жени в публично достъпни пространства. Понякога насилниците се сдобиват с кадри чрез скрито оборудване в наети жилища, козметични студия или лечебни заведения. Тази форма на насилие представлява дигиталното проявление на опита за контрол върху женското тяло, за притежание на женската интимност, за нарушаване на личното право на всяка жена да разполага с тялото, с голотата и с образа си.

Проследяване и наблюдение

Инсталиране на софтуер за следене (stalkerware) или шпионски софтуер (spyware) в устройствата на жертвата или използване на устройства от „Интернета на нещата“ (IoT) в дома на жертвата като смарт звънци и скрити камери за следене на движенията на жертвата в дома ѝ - този тип контраол и наблюдение над жертвата може да се осъществява и чрез изглеждащи като „безобидни“ устройства - хладилници, прахосмукачки-роботи, бебелефони и отоплителни системи.





Дийпфейк (Deepfakes)

Реалистично изглеждащи, но фалшиви изображения, видеоклипове или аудиосъдържание на жертвата, генерирани от изкуствен интелект (ИИ). Съществуват също и така наречените шалоуфейкове (shallow-fakes) – фалшиво съдържание, което е очевидно манипулирано и неистинно. Въпреки това то използва образа или гласа на жертвата, за да направи внушение, да наруши достойнството, да разпространи зловредно съдържание. Фалшивото съдържание с образа на жени най-често се използва за злепоставяне на жени политици или публични личности чрез поставянето им в компрометиращи ситуации. Подтип на тази категория КТН е синтетичната порнография - генерирани с ИИ сексуални изображения и видеа на реални жени в измислени сюжети и без тяхното съгласие. „Синтетичното изнасилване“, от своя страна, е крайна форма, използвана за тормоз и изнудване.

Нудификация (nudification)

Използване на ИИ конкретно с цел да преработи реална снимка на жена така, че да я „съблече“ и да произведе огледално копие, в което обаче жената вече е гола или в оскъдно облекло.

Контрол върху устройствата

Конфискуване, повреждане или ограничаване на достъпа до телефона, смяна на пароли, премахване на SIM карти или спиране на интернет рутери, за да се изолира жертвата от близки и служби за помощ.

Насилието над деца е заплашително улеснено

Чрез дигитални и технологични средства. Не само познатият до момента онлайн тормоз (online bullying) в социалните медии и чатове, но и сексуалното съдържание, фалшиво или истинно. Най-притеснителната форма е създаване на материали със сексуално насилие над деца (CSAEM) чрез използване на дигитални инструменти за записване на реални или симулирани сексуални дейности с деца, което е незаконно в почти всички юрисдикции. Анонимността, предлагана от интернет, се използва за масово споделяне на материали със сексуално насилие над деца.

Онлайн тормоз

Включва „body shaming“ (подигравки за външния вид) и „slut-shaming“ (критика на сексуалното поведение с цел унижение).





Кибертормоз чрез посредник

Заливане на профилите на жертвата с незаконно съдържание (напр. терористична пропаганда или насилие), за да бъде тя сплашена или травмирана. Понякога съдържанието е на изображения, които могат да бъдат разчетени като заплаха за убийство – гроб, некролог, ковчег и др.

Онлайн реч на омразата, основана на пола

Съдържание, което оправдава враждебността към жените. В тази форма на насилие не е нападната директно личността на жертвата, а белезите и характеристиките на група, към която жертвата принадлежи. Това би могла да е група по полов, етнически, национален или сексуален признак.

Контрол върху онлайн присъствието

Контрол и слеждане на историята на търсене, управление на пароли и банкови сметки от насилника, което поставя жертвата в икономическа и емоционална зависимост.

Тролинг и флейминг

Групов и постоянен тормоз в онлайн пространство (форуми, чатове, социални медии, онлайн игри) срещу конкретна жертва, към която се отправят постоянни обиди, подигравки, заплахи от много хора. Когато хората го правят анонимно, насилието се нарича флейминг (flaming), а когато застават с имената си или по начин, който позволява на жертвата ясно да идентифицира кой стои зад аватара, тогава практиката се нарича тролинг (trolling).

Кибермобинг

Групово нападение на личност чрез разпространение на слухове и конспиративни теории. В тази форма на насилие, насилникът набира „армия“ от съмишленици, които да бомбардират дигиталното лично пространство на жертвата. Тази армия може да бъде от реални хора зад своите профили в социалните мрежи, или армия от тролове и ботове, или фалшиви профили, управлявани от насилника.





Подстрекателство към престъпления от омраза

Организиране на престъпни деяния срещу жени, които „прекрачват“ традиционните социални роли. В тази форма на насилие може подстрекателството да се осъществява онлайн – най-често проявление в случаите на насилие над интимен партньор. Възможно е и „основанието“ за поставянето на мишена върху жертвата да е публичното или онлайн поведението ѝ, изявления, изразени политически или граждански позиции – най-често проявление на насилие от непознати върху жени, публични личности.

Кражба на самоличност и „catfishing“

Създаване на фалшиви профили за измамване на жени или въвличането им в трафик на хора. Понякога насилниците се преструват на друга реална или въображаема личност (catfishing), за да заблудят жертвата и да изградят отношения на доверие, които помагат за злоупотреба и получаване на физически достъп до жертвата. В други случаи насилниците се преструват на жертвата като обсебват паролите ѝ за достъп до различни платформи, включително такива за онлайн банкиране и достъп до финансови институции. При тези случаи целта е кражба и нерегламентиран достъп до собствеността и имиджа на жертвата с цел злоупотреба.

Киберслеждане (Cyberstalking)

Събиране на информация за местоположение, навици и работно място чрез дигитални следи, което улеснява физическото нападение.

Доксинг (Doxxing)

Злонамерено публикуване на лична информация на жертвата (адрес, телефон) без съгласие, което често води до физическа опасност. Не са редки случаите, в които този тип контрол е подкрепен от директен призив към нанасяне на физическа вреда и/или досег с жертвата.

Онлайн сексуално изнудване (Sextortion)

Използване на интимни кадри (фалшиви или истинни) за принуда на жертвата към сексуални услуги или рекет. Тази форма на изнудване често се използва от насилници в контекста на интимна връзка, в която жертвата се страхува да напусне насилствената ситуация и/или да потърси помощ, защото е заплашвана с публично споделяне на сексуални или унижителни кадри.





Приложение 2

Планове за действие за специалисти, работещи с жертви на кибер и технологично насилие

Тези Планове са създадени, за да подпомогнат специалистите да обмислят всички възможни аспекти на онлайн и технологичната безопасност при работа с най-често срещаните случаи на кибер- и технологично насилие. Те предлагат насоки, приложими в глобален контекст, както и допълнителни съображения за докладване в българските условия. Включват практически стъпки относно:

- ☀ Споделяне на интимни изображения без съгласие, сексуално изнудване (sextortion) или заплахи за публикуване
- ☀ Киберпреследване, тормоз, контрол чрез принуда и други форми на партньорско насилие, осъществявано чрез технологии
- ☀ Доксинг, представяне за друго лице, фалшиви профили и разкриване на лични данни
- ☀ Финансово насилие чрез технологии

Не приемайте, че „просто блокирайте и сменете паролата“ е достатъчно. В случаи на контрол чрез принуда, злоупотребата често обхваща:

- ☀ процеси за възстановяване на имейли
- ☀ облачни архиви
- ☀ споделени семейни акаунти

- ☀ споделяне на местоположение
- ☀ достъп до банкови услуги
- ☀ устройства на деца
- ☀ системи за „умен дом“

Най-ефективната намеса обикновено е последователен план: **безопасност, доказателства, поверителност, защита на основните акаунти, проверка за наблюдение и докладване** – всичко насочено към дългосрочно възстановяване.

План за действие 1

Споделяне на интимни изображения без съгласие, сексуално изнудване (sextortion) или заплахи за публикуване

Използвайте при:

- ☀ споделени интимни снимки/видеа без съгласие
- ☀ заплахи за публикуване, ако жертвата не се подчини, не плати или не се върне при извършителя
- ☀ фалшиви интимни профили (напр. OnlyFans, Patreon, сайтове за запознанства)
- ☀ повторно публикуване в групи/канални
- ☀ сексуализирано съдържание тип „deepfake“





1. Какво да направите първо

- ☀ Оценете незабавния риск:
 - Извършителят настоящ или бивш партньор ли е?
 - Има ли изнудване, преследване или заплаха от физическо насилие?
 - Жертвата под 18 години ли е?
- ☀ Посъветвайте жертвата да не преговаря, да не плаща и да не изпраща допълнително съдържание.
- ☀ Обяснете, че премахването и докладването могат да се извършват паралелно със събирането на доказателства.

2. Доказателства: какво да съхраните

Посъветвайте жертвата да съхрани:

- ☀ екранни снимки (по възможност целия екран)
- ☀ URL / линк към профила / потребителско име
- ☀ дата и час
- ☀ имена на групи, канали, страници или акаунти
- ☀ заплашителни съобщения, искания за плащане или принуда
- ☀ доказателства за повторно публикуване или отбелязване на други хора
- ☀ номера на сигнали към платформите / потвърждения по имейл

Допълнително:

- ☀ съхранявайте файловете в една защитена папка
- ☀ опишете кратка хронология: какво, кога, кой, къде

- ☀ не редактирайте екранните снимки
- ☀ по възможност запазвайте страниците като PDF

3. Блокиране и ограничаване

- ☀ блокирайте извършителя и очевидните вторични акаунти (освен ако временно наблюдение е необходимо за доказателства)
- ☀ направете профилите частни
- ☀ скрийте списъците с приятели/последователи
- ☀ ограничете кой може да пише, тагва, споменава или отговаря
- ☀ премахнете публична лична информация (телефон, адрес, работа и др.)
- ☀ изключете автоматично синхронизиране на контакти

4. Докладване към платформи

Посъветвайте жертвата да избере категории като:

- ☀ интимни изображения без съгласие
- ☀ сексуална експлоатация
- ☀ тормоз
- ☀ представяне под чужда самоличност
- ☀ нарушаване на поверителността
- ☀ изнудване

Практически насоки:

- ☀ докладвайте и съдържанието, и профила
- ☀ докладвайте всички копия на съдържанието





- ☀ пазете номерата на сигналите
- ☀ отбележете ясно спешност или участие на дете

5. Защита на акаунти (приоритет)

Започнете с акаунтите / профилите, които могат да се използват за възстановяване на всичко останало:

1. основен имейл
2. телефонен номер
3. Apple ID / Google акаунт
4. облачен архив (Cloud)
5. социални мрежи
6. чат приложения
7. банкови приложения

За всяко от тях:

- ☀ променете паролата си от по-сигурно устройство, ако имате подозрения за компрометиране
- ☀ излезте от другите си сесии/устройства
- ☀ проверете имейла и телефона за възстановяване
- ☀ премахнете неизвестните устройства
- ☀ активирайте двуфакторна автентикация MFA / 2FA
- ☀ където е възможно, използвайте приложение за удостоверяване или хардуерен ключ вместо SMS
- ☀ прегледайте разрешенията на приложенията и свързаните приложения на трети страни
- ☀ прегледайте споделените албуми, споделените дискове и синхронизирани папки

Допълнително: Ако имате подозрения за шпионски софтуер или слеждане на устройството

Обърнете внимание на:

- ☀ необичайно бързо изразходване на батерията
- ☀ прегряване на устройството, когато не се използва
- ☀ внезапни скокове в потреблението на мобилни данни
- ☀ непознати приложения, особено с неясни или неспецифични имена
- ☀ активирани разрешения за достъпност за приложения, които не би трябвало да се нуждаят от тях
- ☀ разрешения за администратор на устройството, предоставени на непознати приложения
- ☀ непознати профили на устройството
- ☀ споделяне на местоположението, активирано на няколко места
- ☀ непознати Bluetooth тракери или споделяне чрез „Намери моето“
- ☀ извършителят знае съобщения, местоположения или планове, които не би трябвало да знае

Какво да направите:

- ☀ не възстановявайте веднага фабричните настройки, ако устройството може да съдържа доказателства и жертвата се намира в ситуация на ескалиращо насилие
- ☀ не инсталирайте произволни „антишпионски“ приложения





- ☀ изгответе план за безопасност на устройството:
 - използвайте второ, доверено устройство за чувствителни действия
 - първо документирайте подозрителни настройки/приложения
 - прегледайте инсталираните приложения и разрешенията
 - прегледайте споделянето на местоположение, свързаните устройства и акаунти
 - обмислете професионална цифрова криминалистика или специализирана подкрепа при технологично насилие, ако такава е налична

6. Подаване на сигнали в България

- ☀ Сигнализирайте за киберпрестъпления, хакерство, изнудване и онлайн заплахи на каналите за киберпрестъпления на Главната дирекция за борба с организираната престъпност (ГДБОП) към Министерството на вътрешните работи.
- ☀ Сигнализирайте за незаконно публикуване на лични данни към Комисията за защита на личните данни (КЗЛД). КЗЛД приема жалби и сигнали по официални канали.
- ☀ Насочвайте случаите, свързани с домашно насилие, към наличните национални горещи линии и местните служби за кризисна подкрепа.
- ☀ Ако случаят засяга дете, незабавно се обърнете към службите за защита на децата и за безопасност в интернет.

План за действие 2

Киберпреследване, тормоз, контрол чрез принуда и други форми на партньорско насилие, осъществявано чрез технологии

Използвайте при:

- ☀ повтарящи се обидни обаждания/съобщения
- ☀ следене на профила
- ☀ принудително споделяне на пароли
- ☀ проследяване на местоположението
- ☀ злоупотреба с устройства за „умен дом“
- ☀ подозрение за шпионски софтуер
- ☀ повтарящо се представяне за друго лице или профили, причиняващи неудобства

1. Какво да направите първо

Попитайте:

- ☀ Знае ли насилникът къде се намира жертвата в реално време?
- ☀ Появявал ли се е насилникът на място или е заплашвал да дойде лично?
- ☀ Страхува ли се жертвата да промени настройките, защото това може да доведе до ескалация на насилието?
- ☀ Ако е приложимо, наблюдават ли се и устройствата/профилите на децата?





Ако да, приоритет е планът за безопасност.

2. Доказателства: какво да съхраните

Посъветвайте жертвата да запази:

- ✧ екранни снимки на съобщения и обаждания (вкл. пропуснати обаждания)
- ✧ гласови съобщения, аудио бележки, имейли
- ✧ дати/часове на лични срещи след онлайн наблюдение
- ✧ регистри на подозрителни влизания в профила или опити за промяна на паролата
- ✧ екранни снимки на настройки за споделяне на местоположение, непознати сесии или устройства за проследяване
- ✧ снимки на подозрителни физически устройства: физически устройства за проследяване (напр. AirTag), скрити телефони, устройства за проследяване на автомобили, допълнителни камери

Насърчете създаването на дневник на инцидентите в документ:

- ✧ дата
- ✧ платформа/устройство
- ✧ какво се е случило
- ✧ подозирана връзка с извършителя
- ✧ въздействие върху безопасността

3. Блокиране и ограничаване

Посъветвайте жертвата да:

- ✧ блокира известните профили и номерата на насилника, когато това е безопасно
- ✧ заглуши, ограничи и филтрира заявките за съобщения
- ✧ засили настройките за поверителност:
 - преминаване към личен профил
 - скриване на статуса си на активност
 - деактивиране функцията „хора, които може би познавате“, ако е налична
 - деактивиране на маркирането на местоположението и споделянето на местоположението на живо
 - преглеждане на аудиторията на Stories
 - премахване на непознати последователи
- ✧ за приложения за чат / съобщения:
 - деактивиране на автоматичното изтегляне на медийни файлове
 - преглед на свързаните устройства
 - скриване на профилната снимка/информацията за профила към лица, които не са в списъка с контакти, където е възможно.





4. Проверка за наблюдение на устройствата и акаунтите

Проверявайте систематично следните устройства и канали:

Телефон

- ☀️ списък с инсталираните приложения
- ☀️ специални разрешения:
 - достъпност
 - администратор на устройството
 - разрешения за запис на екрана
 - достъп до известия
 - постоянно проследяване на местоположението
 - достъп до микрофона/камерата на заден план
- ☀️ настройки за пренасочване на повиквания
- ☀️ свързани Bluetooth устройства
- ☀️ споделено местоположение в екосистемите на Apple / Google / индивидуални приложения
- ☀️ неизвестни абонаменти за календар или споделени семейни групи

Имейл

- ☀️ правила за пренасочване
- ☀️ филтри, изпращащи копия на други места
- ☀️ имейл/телефон за възстановяване
- ☀️ устройства, на които сте влезли
- ☀️ сигнали за сигурност

Социални медии

- ☀️ сесии, в които сте влезли
- ☀️ свързани приложения
- ☀️ рекламни акаунти / бизнес мениджъри
- ☀️ синхронизиране на контакти
- ☀️ списък с блокирани и настройки за скрита аудитория

Умни устройства

- ☀️ умни тонколони / аудио системи
- ☀️ камери
- ☀️ домофони
- ☀️ споделени семейни акаунти
- ☀️ приложения за автомобили
- ☀️ умни брави / термостати

5. Защита на акаунти (приоритет)

Започнете с акаунтите / профилите, които могат да се използват за възстановяване на всичко останало:

1. основен имейл
2. телефонен номер
3. Apple ID / Google акаунт
4. облачен архив (Cloud)
5. социални мрежи
6. чат приложения
7. банкови приложения



**За всяко от тях:**

- ✱ променете паролата си от по-сигурно устройство, ако имате подозрения за компрометиране
- ✱ излезте от другите си сесии/устройства
- ✱ проверете имейла и телефона за възстановяване
- ✱ премахнете неизвестните устройства
- ✱ активирайте двуфакторна автентикация MFA / 2FA
- ✱ където е възможно, използвайте приложение за удостоверяване или хардуерен ключ вместо SMS
- ✱ прегледайте разрешенията на приложенията и свързаните приложения на трети страни
- ✱ прегледайте споделените албуми, споделените дискове и синхронизирани папки

Допълнително: Ако имате подозрения за шпионски софтуер или следене на устройството**Обърнете внимание на:**

- ✱ необичайно бързо изразходване на батерията
- ✱ прегряване на устройството, когато не се използва
- ✱ внезапни скокове в потреблението на мобилни данни
- ✱ непознати приложения, особено с неясни или неспецифични имена
- ✱ активирани разрешения за достъпност за приложения, които не би трябвало да се нуждаят от тях
- ✱ разрешения за администратор на устройството, предоставени на непознати приложения

- ✱ непознати профили на устройството
- ✱ споделяне на местоположението, активирано на няколко места
- ✱ непознати Bluetooth тракери или споделяне чрез „Намери моето“
- ✱ извършителят знае съобщения, местоположения или планове, които не би трябвало да знае

Какво да направите:

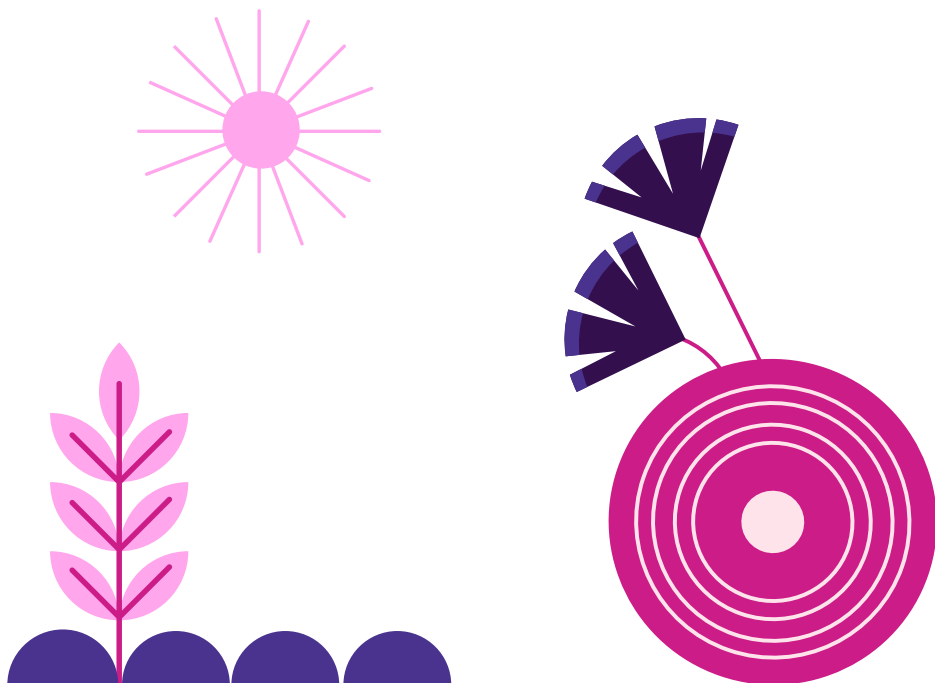
- ✱ не възстановявайте веднага фабричните настройки, ако устройството може да съдържа доказателства и жертвата се намира в ситуация на ескалиращо насилие
- ✱ не инсталирайте произволни „антишпионски“ приложения
- ✱ изгответе план за безопасност на устройството:
 - използвайте второ, доверено устройство за чувствителни действия
 - първо документирайте подозрителни настройки/приложения
 - прегледайте инсталираните приложения и разрешенията
 - прегледайте споделянето на местоположение, свързаните устройства и акаунти
 - обмислете професионална цифрова криминалистика или специализирана подкрепа при технологично насилие, ако такава е налична





6. Подаване на сигнали в България

- ☀ Полиция (Министерство на вътрешните работи) при заплахи, тормоз, манипулативен контрол или опасения за физическата безопасност.
- ☀ Генерална дирекция за борба с организираната престъпност (ГДБОП) относно сигнали за киберпрестъпления, свързани с хакерство, незаконен достъп, зловреден софтуер или техническо компрометиране на акаунт.
- ☀ Насочвайте случаите, свързани с домашно насилие, към наличните национални горещи линии и местните служби за кризисна подкрепа.
- ☀ Ако случаят засяга дете, незабавно се обърнете към службите за защита на децата и за безопасност в интернет.



План за действие 3

Доксинг, представяне за друго лице, фалшиви профили и разкриване на лични данни

Използвайте при:

- ☀ публично разгласяване на телефонен номер, адрес или работно място
- ☀ фалшиви обяви / реклами или обяви със сексуално съдържание, публикувани от името на жертвата
- ☀ фалшиви профили, чрез които се установява контакт с други лица
- ☀ изтичане на лични документи или лични данни
- ☀ злоупотреба с лични данни

1. Какво да направите първо

Посъветвайте жертвата да:

- ☀ събере доказателства, преди да подаде сигнал
- ☀ определи пълния обхват на проблема:
 - кои платформи са засегнати
 - какви данни са били разкрити
 - съществува ли риск и извън интернет
- ☀ уведоми работодателя, училището, рецепцията, съседите или охраната на сградата, ако е разкрито местонахождението ѝ у дома или на работа и съществува риск за безопасността ѝ





2. Блокиране и ограничаване

- ☀ настройте всички профили в социалните мрежи на личен режим
- ☀ премахнете публичните биографични данни
- ☀ скрийте имейл адреса и телефона, където е възможно
- ☀ прегледайте стари публични публикации за данни за местоположението
- ☀ премахнете публичния достъп до списъците с приятели
- ☀ прегледайте обяви в онлайн пазари, приложения за запознанства и стари форуми за наличие на снимки/данни
- ☀ потърсете онлайн името, телефонния номер и потребителските имена на жертвата, за да откриете други точки на разпространение

3. Докладване към платформи

Посъветвайте жертвите да:

- ☀ подадат сигнал чрез опциите „използване на чужда самоличност“, „фалшив профил“, „нарушение на правото на неприкосновеност“, „тормоз“ или „измама“ чрез каналите за докладване на платформата
- ☀ подадат сигнал за конкретната публикация и профила/страницата
- ☀ поискат премахване на лични данни като телефонен номер, адрес, личен номер, работно място, училище на детето

- ☀ ако са публикувани фалшиви обяви / реклами, да подадат сигнал незабавно и да посочат, че самоличността им се използва неправомерно
- ☀ запазят потвърждението и номера на случая

4. КЗЛД / процедура за защита на личните данни

В случаите, когато лични данни са публикувани или обработени незаконосъобразно, препоръчайте да се подаде жалба до Комисията за защита на личните данни (КЗЛД).

Примери за случаи, при които може да бъде подадена жалба:

- ☀ публикуван адрес на местоживеене
- ☀ публикуван телефонен номер в сексуален или тормозещ контекст
- ☀ изтекли документи за самоличност
- ☀ разкрити данни за заетост и контактни данни без законно основание

5. Мерки при риск от измама и представяне за друго лице

Посъветвайте жертвата да:

- ☀ предупреди близките си да не се доверяват на нови акаунти или искания за плащане
- ☀ публикува кратко съобщение на компрометираните профили, ако е уместно и безопасно





- ☀️ провери дали имейл, платежни или пазарни профили са били превзети
- ☀️ смени паролите (силни пароли, подкрепени от MFA / 2FA, ключове за достъп, FaceID или пръстов отпечатък) на всеки профил, който използва същата или подобна парола
- ☀️ провери правилата на пощенската кутия/препращането
- ☀️ следи финансовите си профили за подозрителна активност
- ☀️ води списък с фалшиви профили, които вече са докладвани

6. Подаване на сигнали в България

- ☀️ Комисия за защита на личните данни (КЗЛД) при незаконно обработване или публикуване на лични данни.
- ☀️ Главна дирекция за борба с организираната престъпност (ГДБОП) или полиция, когато подправянето на самоличност е свързано с измама, изнудване, хакерство или системно тормозене.
- ☀️ Насочвайте случаите, свързани с домашно насилие, към наличните национални горещи линии и местните служби за кризисна подкрепа.
- ☀️ Ако случаят засяга дете, незабавно се обърнете към службите за защита на децата и за безопасност в интернет.

План за действие 4

Финансово насилие чрез технологии

Използвайте при:

- ☀️ неоторизирани преводи
- ☀️ натиск за предоставяне на банкови данни за достъп
- ☀️ злоупотреба чрез приложения за мобилно банкиране
- ☀️ превземане на електронни портфейли или платежни услуги
- ☀️ злоупотреба с онлайн пазаруване, кредити, абонаменти или дигитални портфейли
- ☀️ контрол на финансите от страна на партньора чрез споделени акаунти/устройства

1. Какво да направите първо

Посъветвайте жертвата да:

- ☀️ се свърже незабавно с банката, като използва номера, посочен на официалния уебсайт/в приложението/върху картата на банката, а не номер, изпратен в съобщение
- ☀️ замрази или блокира банкови карти, ако е необходимо
- ☀️ съобщи незабавно за неоторизирани транзакции
- ☀️ поиска от банката да отбележи подозрение за измама / принудително контролиране / компрометиране на сметката
- ☀️ промени банковата парола/ПИН кода от по-





безопасно устройство

- ✱ излезе от други сесии, ако банката поддържа тази функция
- ✱ премахне биометричния достъп, ако биометричните данни на извършителя са регистрирани на устройството, той физически използва устройството или принуждава жертвата да предостави своите биометрични данни за достъп
- ✱ провери дали банковите известия се изпращат на жертвата или на някой друг

2. Какво да проверите

- ✱ история на влизанията в мобилното банково приложение / доверен списък с устройства
- ✱ имейл акаунт, свързан с банката
- ✱ телефонен номер, на който се получават еднократни пароли (OTP)
- ✱ споделени таблети/телефони с инсталирано банково приложение
- ✱ запазени карти в браузъри и приложения за пазаруване
- ✱ достъп до Apple Pay / Google Pay / дигитален портфейл
- ✱ абонаменти и периодични плащания
- ✱ акаунти за мигновени заеми / BNPL / онлайн пазари
- ✱ приложения за криптовалути или борси, ако е приложимо

Допълнително: Ако насилникът е партньор/бивш партньор

Проверете също:

- ✱ дали насилникът все още е упълномощен потребител или титуляр
- ✱ дали извлеченията се изпращат по пощата на общ адрес/имейл
- ✱ дали мобилният план на жертвата се контролира от насилника
- ✱ дали еднократните пароли могат да бъдат прихванати, тъй като насилникът контролира SIM-картата, имейла или устройството

3. Доказателства: какво да съхраните

- ✱ екранни снимки на транзакции
- ✱ банков известия / SMS / имейл
- ✱ дати и суми
- ✱ уведомления за подозрителни устройства или влизания в профила
- ✱ заплашителни съобщения, свързани с финансов натиск
- ✱ екранни снимки, показващи, че данни за достъп били поискани или предоставени под натиск

4. Защита на акаунти (приоритет)

Посъветвайте жертвата да защити профилите си в следния ред:

1. основния си имейл адрес
2. номера на мобилния си телефон / профила си при мобилния оператор
3. банковите приложения и онлайн банкирането





4. електронните портфейли / приложенията за карти
5. Apple ID / профила си в Google
6. профилите за пазаруване/плащания

За всеки от тях:

- ✱ уникална нова парола
- ✱ MFA / 2FA, където се поддържа
- ✱ актуализиране на данните за възстановяване
- ✱ изтриване на други сесии/устройства
- ✱ премахване на запазените методи за плащане от споделените устройства
- ✱ проверка дали еднократните пароли, одобрения чрез „push“ известия или потвърждения по имейл са видими на друго свързано устройство

5. Подаване на сигнали в България

- ✱ Незабавно съобщете на банката за неоторизирани транзакции
- ✱ Поискайте разследване на измамата и писмено потвърждение
- ✱ Ако става въпрос за хакерска атака, фишинг или зловреден софтуер, подайте сигнал чрез каналите за киберпрестъпления на Главната дирекция за борба с организираната престъпност (ГДБОП) и, ако е необходимо, към полицията.
- ✱ Насочвайте случаите, свързани с домашно насилие, към наличните национални горещи линии и местните служби за кризисна подкрепа.

За повече информация относно проекта посетете www.id.counterintuitive.eu



Библиография

Kuneva, L. & Tzvetkova, G. (2026). Digital dimension of violence against women. In Elgar Encyclopedia of Gender and Politics. Cheltenham, UK: Edward Elgar Publishing.
<https://doi.org/10.4337/9781035322619.00016>

Aggression and Violent Behavior. (2017). Elsevier. <https://www.sciencedirect.com/science/article/abs/pii/S135917891730157X>

Andriessen, P. E. (2021). A scoping research on gender-based violence in Dutch printed media. Share-Net Netherlands, Community of Practice on Gender-Based Violence.
https://share-net.nl/wp-content/uploads/2024/11/SN_Scoping_Research_Dutch_Media.pdf

Datawrapper. (n.d.). A friendly guide to choosing a chart type. Datawrapper Blog.
<https://www.datawrapper.de/blog/chart-types-guide>

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. (2024). Official Journal of the European Union, L, 2024/1385.
<https://eur-lex.europa.eu/eli/dir/2024/1385/oj/bul>

European Equality Law Network. (2025). Country report – Gender equality – Bulgaria – 2025. European Commission. <https://www.equalitylaw.eu/downloads/6390-bulgaria-country-report-gender-equality-2025>

European Institute for Gender Equality. (2022). Combating cyber violence against women and girls. Publications Office of the European Union.
https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf

European Women's Lobby. (2017). #HerNetHerRights – Report

on cyber violence against women: Policy overview and recommendations. European Women's Lobby.
https://dev.womenlobby.org/IMG/pdf/ewl_fullreport-2.pdf

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO). (2021). General Recommendation No. 1 on the digital dimension of violence against women. Council of Europe.
<https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>

Plan International. (2020). Free to be online? Girls' and young women's experiences of online harassment. Plan International.
<https://plan-international.org/publications/free-to-be-online/>

Society of Professional Journalists. (n.d.). Code of ethics of the Society of Professional Journalists. The Journalist's Resource.
<https://journalistsresource.org/home/code-of-ethics/>

Strategic analysis of intimate partner violence (IPV) and cycle of violence in the autobiographical text When I Hit You. (2022). Heliyon. PubMed Central.
<https://pmc.ncbi.nlm.nih.gov/articles/PMC9233205/>

The New York Times. (2026, January 22). Grok, X, and Elon Musk: AI deepfakes. The New York Times.
<https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html>

UC Irvine Libraries. (n.d.). Library record [alma991028498969704701]. UC Library Search.
https://uci.primo.exlibrisgroup.com/discovery/fulldisplay/alma991028498969704701/01CDL_IRV_INST:UCI

United Nations Regional Information Centre for Western Europe (UNRIC). (n.d.). Cyber violence against women and girls: The growing threat of the digital age.
<https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/>



НЕВИДИМИ ДАНИИ



COUNTER
INTUITIVE
INSTITUTE