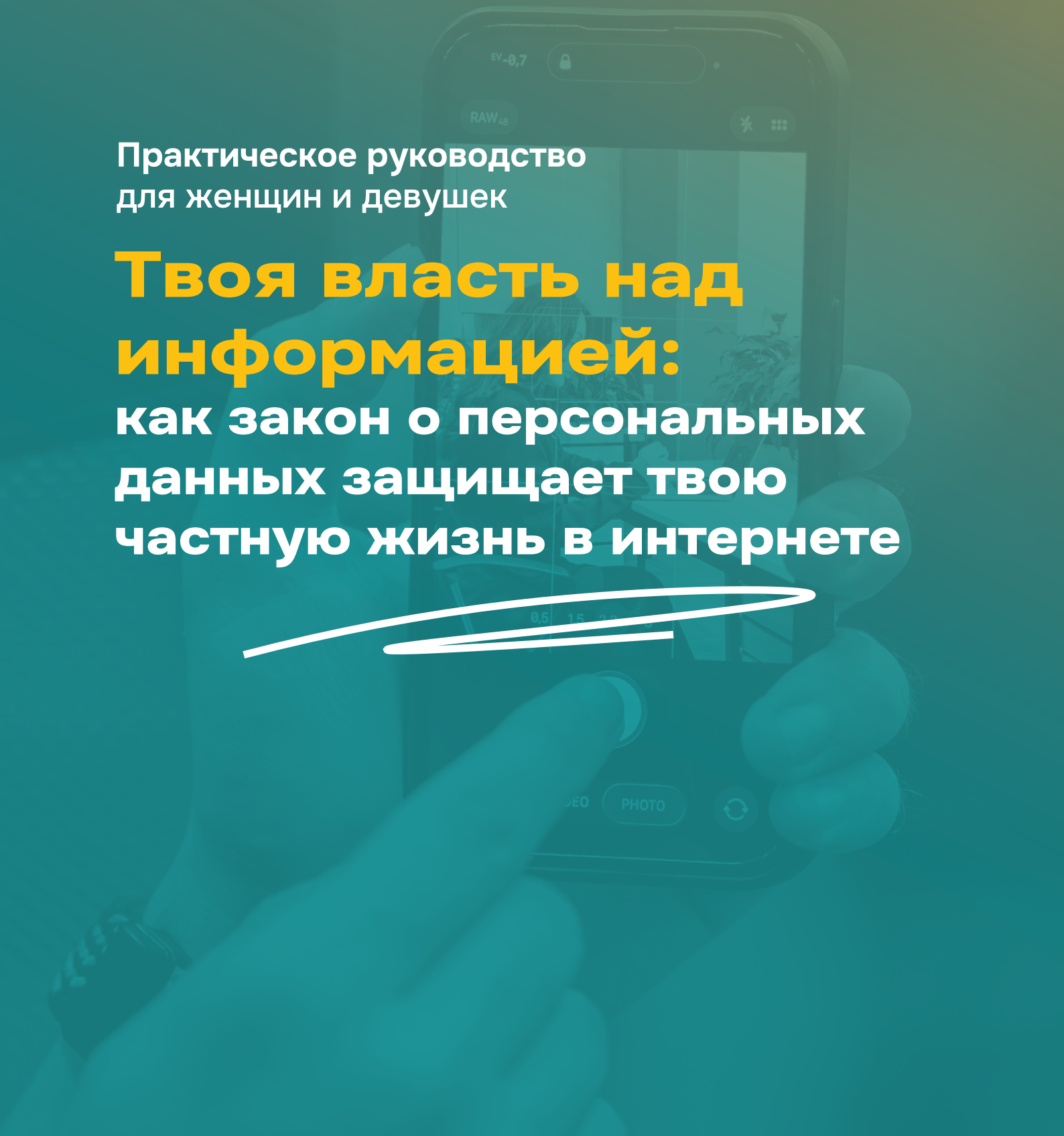
eviolența.md

Практическое руководство
для женщин и девушек

Твоя власть над информацией:

как закон о персональных данных защищает твою частную жизнь в интернете



Введение:
почему твоя фотография, твоё имя и твои переписки защищены законом

В мире, где мы публикуем посты, делимся контентом и общаемся в цифровом пространстве, граница между нашей публичной и частной жизнью, кажется, стирается. Но это не значит, что она исчезла. Использование онлайн-платформ не лишает нас одного из фундаментальных прав человека – права на частную жизнь и контроля над собственной идентичностью.

Возможно, ты когда-то чувствовала себя уязвимой. Возможно, фотография, которой ты поделилась в личной переписке, оказалась в публичном пространстве. Возможно, информация о тебе – твой адрес, номер телефона или даже личные переписки – были использованы без твоего разрешения и вызвали у тебя страх или чувство унижения. Эти действия – не «цена, которую мы платим за технологии». Это нарушения.

Законодательство Республики Молдова, в частности Закон № 133 от 2011 года о защите персональных данных, вместе с положениями Уголовного кодекса, создает мощный правовой щит вокруг твоей идентичности. Цель этой статьи – подробно исследовать этот правовой щит. Мы разберём технические и юридические термины, чтобы точно понять, что такое «персональные данные», какую огромную силу дает тебе понятие «согласие», и какая ключевая правовая разница между публичным и приватным контентом.
Понимание своих прав на данные – это не техническое упражнение. Это жизненно важное действие самозащиты и отстаивания достоинства в цифровую эпоху.

Применимое правовое поле (часть 1):
что на самом деле означают «персональные данные»?

Это основа всей твоей защиты. Закон № 133 сформулирован ясно и охватывает очень широкий круг ситуаций.

Согласно статье 3 закона, персональные данные определяются как «любая информация, связанная с идентифицированным или идентифицируемым физическим лицом (субъектом персональных данных)».
Давай разберём, что это значит, простыми словами:

«Идентифицированное физическое лицо» – это ты. Когда информация напрямую связана с твоим именем, ты уже идентифицирована.

«Идентифицируемое лицо» – более широкое понятие. Человек считается «идентифицируемым», если его можно распознать прямо или косвенно «посредством ссылки на идентификационный номер(IDNP) либо на один или несколько факторов, специфичных для его физической, физиологической, психической, экономической, культурной или социальной идентичности».

Что это означает на практике для тебя?

Твои персональные данные – это не только имя или персональный идентификационный номер (IDNP). Этот перечень гораздо шире и охватывает почти любой элемент твоей цифровой и реальной идентичности. Исходя из юридического определения, к твоим персональным данным относятся:

1. **Твоё изображение (фотография или видео):** Это главная персональная информация. Даже если твоё имя не указано, лицо является элементом, который идентифицирует тебя физически. Публикация твоей фотографии без твоего согласия считается обработкой персональных данных.
2. **Твоё имя и фамилия:** Самый очевидный идентификатор личности.
3. **Контактная информация:** Адрес проживания, адрес электронной почты (если он позволяет тебя идентифицировать, например: имя.фамилия@...), номер телефона.
4. **Онлайн-идентификаторы:** Имя пользователя (username), если его можно связать с тобой, или IP-адрес (в определённых технических контекстах).
5. **Твои личные переписки:** Хотя само содержание переписки защищено тайной переписки, информация внутри неё (подробности о твоей жизни, здоровье, отношениях) является информацией, относящейся к тебе как к идентифицируемому лицу.
6. **Данные «особых категорий»:** Закон № 133 предусматривает усиленную защиту данных, раскрывающих «расовое или этническое происхождение лица, политические убеждения, религиозные... данные, касающиеся состояния здоровья или половой жизни». Любая онлайн-информация, затрагивающая эти темы, находится под особо строгой защитой.

Таким образом, когда ты находишься в сети, практически каждый след, который ты оставляешь и который может быть связан с тобой, является «персональными данными», которые защищаются законом.

Применимое правовое поле (часть 2):
согласие – твой ключ к контролю

Это самое важное понятие, которое тебе нужно запомнить. Если твои данные – это твоя собственность, то **согласие** – это юридическое основание, с помощью которого ты решаешь, что будет происходить с этой собственностью.

Закон 133 устанавливает золотое правило в статье 5: **обработка** персональных данных может осуществляться, за очень редкими исключениями (такими как законные обязанности государства), только с **«согласия субъекта персональных данных».**

Что означает «обработка»? «Обработка» – это юридический термин, который означает любые действия, которые кто-то совершает с твоими данными. Статья 3 Закона №133 приводит длинный перечень: «сбор, запись, организация, хранение, восстановление, адаптация... консультирование, использование, раскрытие посредством передачи, распространения... блокирование, стирание или уничтожение».

Почему это жизненно важно для жертв цифрового насилия?

Потому что это напрямую охватывает действия агрессоров:

Бывший партнёр, который **хранит** твои интимные фотографии после того, как ты попросила их удалить, осуществляет обработку данных.

Человек, который **распространяет** (публикует, пересылает другим) фотографию с тобой, осуществляет обработку данных.

Человек, который **собирает** информацию о тебе (фотографии, адреса) с целью причинить вред, осуществляет обработку данных.

Огромная сила согласия в случаях несогласованного распространения интимных изображений

Здесь Закон № 133 является твоим самым сильным союзником – в тандеме с Уголовным кодексом. Агрессоры часто говорят: «Но ты же сама отправила мне фото!»

Закон № 133 определяет согласие (ст. 3) как «волеизъявление, свободное, конкретное и безоговорочное... которым субъект

персональных данных соглашается на обработку касающихся его персональных данных».

Это означает следующее:

1. То, что ты отправила интимное фото одному человеку (Партнёру X), является согласием только на одну конкретную обработку: «просмотр Партнёром X».
2. Это согласие НЕ ЯВЛЯЕТСЯ и НИКОГДА не будет согласием на другую обработку, такую как «публичное распространение» или «передача Другу Y».
3. Для каждой новой обработки (например, публикации на сайте) агрессору требуется новое, явное согласие с твоей стороны. Поскольку такого согласия нет, обработка (распространение) является незаконной в соответствии с Законом № 133.

Более того, статья 12 Закона № 133 предоставляет тебе право на возражение, позволяя «в любой момент возразить против обработки данных, касающихся тебя». Это – твоя правовая основа требовать удаления твоих данных отовсюду и в любое время, даже если изначально ты соглашалась на их хранение (право отозвать согласие).

Права и юридические шаги (часть 1): линия разграничения – публичный контент против частного

Ещё одна ложная защита агрессоров звучит так: «Это было в интернете, значит, публично. Я могу делать с этим фото всё, что захочу». Закон проводит очень чёткое различие между тем, что действительно является публичным, и тем, что остаётся частным, даже если находится в онлайн-среде.

Щит свободы выражения мнения и его пределы

Закон № 64 от 2010 года о свободе выражения мнения часто неверно истолковывается. Да, закон гарантирует право на свободу выражения. Но уже статья 1 этого закона прямо устанавливает, что его цель – найти «баланс между обеспечением права на свободу выражения и защитой чести, достоинства, деловой репутации лица, его частной и семейной жизни».

Более того, статья 3 Закона № 64 чётко указывает, что свобода выражения может быть законно ограничена (то есть она не является абсолютной), когда это необходимо для «защиты... репутации или прав других лиц».

Твоё право на частную жизнь и твоё право на собственные персональные данные (согласно Закону № 133) – это как раз те самые «права других лиц», которые устанавливают законный предел свободе выражения агрессора.

Итак, что является публичным, а что – частным?

По-настоящему публичный контент: Публикация, которую ты сама настроила как «Публичную» в своём профиле Facebook. Веб-страница, которую ты создала. Газетная статья. Но даже здесь «публичное» не означает «без ограничений». Любой, кто берёт такую «публичную» фотографию и использует её для другой цели (например, для создания фальшивого аккаунта), всё равно осуществляет обработку персональных данных (Закон № 133) и совершает преступление (Уголовный кодекс, ст. 177[1]).

Частный контент: именно эта категория для нас наиболее важна

1. **Твои переписки (чаты):** Сообщения в Messenger, WhatsApp, Instagram DM и т. д. являются частными и защищёнными. Публикация скриншотов таких переписок – это серьёзное нарушение закона.
2. **Твои аккаунты с настройками конфиденциальности:** Если твой профиль настроен как «Приватный» или «Только для друзей», размещённый там контент не является публичным. Любой, кто берёт фотографию из этого закрытого круга и публикует её в другом месте, нарушает закон. Твои настройки конфиденциальности – это юридически значимое выражение твоего ограниченного согласия.
3. **Интимные изображения, отправленные лично:** Это самый высокий уровень частного контента. Они ни при каких условиях не предназначены для публичного распространения.
4. **Твои электронные письма:** Являются частными и защищёнными.

Когда кто-то берёт контент из этих частных пространств и выносит его в публичную сферу, он не реализует свободу выражения мнения – он нарушает твоё право на частную жизнь.

Права и юридические шаги (часть 2): когда нарушение данных становится уголовным преступлением

Нарушение Закона 133 (обработка без согласия) – серьёзное нарушение, которое может повлечь административную

ответственность. Но когда такое нарушение является особо тяжким и совершено умышленно, оно превращается в уголовное преступление, наказуемое в соответствии с Уголовным Кодексом.

Преступление 1: Нарушение неприкосновенности частной жизни (Уголовный кодекс, статья 177)

Этот закон является твоим прямым защитником от публикации личной информации. Статья предусматривает ответственность за «незаконный или умышленный сбор» и, что особенно важно, за «распространение информации, относящейся к личной или семейной жизни» без твоего согласия.

Что означает «распространение»? Именно то, что делают агрессоры: публикация на сайтах, рассылка в группах, публичное размещение.

Что означает «информация о личной жизни»? Это тот самый частный контент, о котором мы говорили: твои переписки (скриншоты), сведения о твоих отношениях, здоровье, адресе.

Цифровой усугубляющий фактор: Закон полностью адаптирован к современным реалиям. Часть (2) статьи 177 предусматривает более строгое наказание, если деяние совершено с «помощью информационных технологий или средств электронных коммуникаций». Закон был написан именно для Facebook, Instagram и других онлайн-платформ.

Преступление 2: Конкретный случай несогласованного распространения интимных изображений (Уголовный кодекс, статья 177, часть 3)

Поскольку распространение интимных изображений – это крайне травмирующая форма насилия, основанная на данных, закон рассматривает её отдельно и с максимальной серьёзностью. Эта часть статьи предусматривает ответственность за «распространение информации сексуального характера... в целях мести, ненависти или унижения, нанесения ущерба чести и достоинству человека».

Это преступление сочетает нарушение данных (Закон № 133) с нарушением частной жизни (ст. 177 УК) и с явным намерением причинить вред (психологическое насилие, согласно Закону № 45).

Преступление 3: Кража твоих данных для фальшивых аккаунтов (Уголовный кодекс, статья 177[1])

Когда кто-то крадёт твои фотографии (персональные данные) и имя для создания фальшивого аккаунта, это не шутка. Это преступление

– «фальсификация личности». Закон предусматривает наказание за «регистрации и/или использования учетных записей (аккаунтов) пользователей на социальных платформах... для введения в заблуждение или оставления в заблуждении».

Агрессор крадёт твои данные, чтобы присвоить твою личность, грубо нарушая твоё право на контроль собственных данных.

Права и юридические шаги (часть 3):
какие конкретные права у тебя есть и к кому обращаться

Теперь, когда ты знаешь, что закон на твоей стороне, вот что можно делать на практике в соответствии с Законом № 133.

Твои права как «субъекта данных» (статьи 11-16 Закона № 133):

1. **Право на доступ к данным:** Ты имеешь право спросить любую компанию или лицо (в законе они называются «контролер») о том, какие данные о тебе у них есть и как они используются.
2. **Право на вмешательство (исправление, удаление):** Это особенно важно. У тебя есть законное право требовать «исправление, актуализацию, блокирование или удаление персональных данных, обработка которых противоречит настоящему закону». Если фотография с тобой опубликована без твоего согласия, у тебя есть законное право требовать её удаления.
3. **Право на возражение:** Как уже упоминалось, ты можешь сказать СТОП. Ты можешь отозвать своё согласие в любой момент, и обработка твоих данных должна быть прекращена (за исключением случаев, когда существует законное обязательство).

Куда обращаться,
чтобы защитить эти права?

Существует два основных пути, которые можно использовать параллельно:

Путь 1: Надзорный орган – НЦЗПД

Закон № 133 учредил Национальный Центр по Защите Персональных Данных (НЦЗПД). Это официальный «страж» закона.
Что делать: Ты можешь подать жалобу (петицию) в НЦЗПД. В жалобе объясняешь, как твои данные были обработаны без согласия (например: «Моя фотография была опубликована на сайте X без моего согласия»).

Что делает НЦЗПД: Они проводят расследование. Имеют законные полномочия констатировать нарушение и выдавать предписания, обязывая оператора (сайт, лицо) удалить твои данные и прекратить незаконную обработку.

Путь 2: Органы уголовного преследования – полиция и прокуратура

Этот путь предназначен для тяжких случаев, являющихся преступлениями (описанными ранее).

Что делать: Если тебе угрожают, если были опубликованы твои интимные изображения (ст. 177, ч. 3 УК), если создан фальшивый аккаунт (ст. 177[1] УК) или опубликованы твои личные переписки (ст. 177 УК), обратись в полицию.

Что происходит: Ты подаёшь уголовную жалобу, прилагая все доказательства (скриншоты, ссылки). Полиция расследует деяние как преступление, с гораздо более серьёзными последствиями для агрессора, включая уголовный штраф или лишение свободы.
Поддержка и ресурсы: твои данные – это твоё достоинство
Видеть, как твою личную жизнь выставляют напоказ в интернете – глубоко травмирующий опыт. Может казаться, будто у тебя украли часть тебя самой, будто ты потеряла контроль над собственной историей.

Важно помнить:
закон даёт тебе явный контроль.

Согласие – это не просто технический термин; это юридическое слово для твоей силы решать. Закон № 133 и Уголовный кодекс – твои инструменты, чтобы вернуть этот контроль.

Разглашение твоих персональных данных – это форма психологического насилия, а в случае несогласованного распространения интимных изображений – ещё и форма сексуального насилия. Ты не должна проходить через это одна. Юридический процесс подачи жалоб может быть долгим и стрессовым, поэтому крайне важно искать эмоциональную поддержку в это время.

Платформа eViolenta.md создана, чтобы направлять тебя. Информация из этой статьи – твой щит. Источники психологической поддержки и юридической консультации, доступные через нас, являются твоими союзниками в этом процессе. Ты не одна, и закон на твоей стороне.

Данный материал был разработан Международным Центром «La Strada» и Фондом ООН в области народонаселения (UNFPA в Молдове) при финансовой поддержке Великобритании.