



ARTICLE 19



# ОБУЧАЮЩИЙ МОДУЛЬ

ДЛЯ ФАКУЛЬТЕТОВ ЖУРНАЛИСТИКИ И  
ЮРИСПРУДЕНЦИИ ВУЗОВ КАЗАХСТАНА





ARTICLE 19

## ОБУЧАЮЩИЙ МОДУЛЬ

### ДЛЯ ФАКУЛЬТЕТОВ ЖУРНАЛИСТИКИ И ЮРИСПРУДЕНЦИИ ВУЗОВ КАЗАХСТАНА

Обучающий модуль разработан ОФ «Правовой медиа-центр» при поддержке Article 19 в рамках проекта «Защита цифровых прав в Центральной Азии» и адресован преподавателям факультетов журналистики и юриспруденции ВУЗов Казахстана. Модуль состоит из десяти разделов, посвященным наиболее актуальным интернет-направлениям: право на приватность, анонимность, доступ к информации, онлайн-активизм, фактчекинг, блокировки и другие. Разделы включают в себя обзор текущей ситуации в международном и национальном контекстах, промежуточные творческие задания для студентов, итоговый тест и глоссарий. Авторами модуля стали известные казахстанские эксперты – юристы, журналисты, члены Экспертной группы по цифровым правам. Модуль предназначен стать полезным источником информации для преподавания студентам дисциплины «Цифровые права».



## ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ В ЦИФРОВЫЕ ПРАВА.....	5
СВОБОДА ВЫРАЖЕНИЯ МНЕНИЯ ОНЛАЙН .....	15
ДОСТУП К ИНФОРМАЦИИ .....	24
АВТОРСКОЕ ПРАВО В ИНТЕРНЕТЕ.....	35
ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ.....	49
ЭЛЕКТРОННОЕ УЧАСТИЕ.....	63
ОГРАНИЧЕНИЕ ИНТЕРНЕТА И БЛОКИРОВКИ КОНТЕНТА .....	75
ОНЛАЙН-АДВОКАЦИЯ И ОНЛАЙН-АКТИВИЗМ .....	84
АНОНИМНОСТЬ В ИНТЕРНЕТЕ .....	89
ФАКТЧЕК КАК ЖУРНАЛИСТСКИЙ ФОРМАТ И НЕОБХОДИМЫЙ НАВЫК .....	99

# ВВЕДЕНИЕ

## В ЦИФРОВЫЕ ПРАВА



*Татьяна Чернобилъ*

## ВВЕДЕНИЕ В ЦИФРОВЫЕ ПРАВА

Эпоха цифровых прав как прав человека началась относительно недавно. До этого, как правило, права человека обсуждались в контексте необходимости их защиты в цифровой среде, но не продвижения. Например, на Всемирной встрече на высшем уровне по вопросам информационного общества в Тунисе в 2005 году говорили о защите детей от растления в интернете и недопустимости злоупотреблений цифровыми достижениями.

Но в 2011 году Коалиция прав и принципов человека при международном Форуме управления интернетом представила Хартию прав и принципов человека – результат своей работы в течение ряда лет, в которой подчеркнула, что «human rights apply online as they do offline» (англ. «права человека в онлайн – те же, что права человека в офлайн»).

С тех пор уже все стороны – государства, межправительственные (международные) организации, IT-корпорации, научное и правозащитное сообщества – согласились, что права, которые человек имеет в офлайн, должны также защищаться и онлайн.

Так что такое цифровые права? Цифровые права – это права, доступ к которым человеку открывает интернет и новые цифровые возможности. Вместе с тем это обычные права человека, но которые реализуются онлайн или с использованием цифровых технологий. Например, право на свободу объединения онлайн – это пользовательские чаты, группы и форумы. Привычное право на свободу мирных собраний в онлайн может выглядеть как сбор подписей под электронным воззванием или создание онлайн-петиций. Право на участие в управлении делами государства, которое в «обычной» жизни выражается, в частности, в нашем участии в выборах, при помощи новых технологий может быть электронным голосованием, а с использованием интернета – дистанционным электронным голосованием. То же - по другим правам. В интернете мы можем работать, отдыхать, учиться, знакомиться, жениться и выходить замуж, судиться, лечиться, говорить, слушать и многое другое,

а при помощи новых цифровых технологий - получать доступ к товарам и услугам, созидать и взаимодействовать.

Если говорить отдельно об интернете, отметим, что по данным ежегодного всемирного обзора Global Digital за 2022 год, сегодня 62,5% мирового населения или 4,95 млрд человек используют интернет. Количество пользователей социальных сетей составляет 4,62 млрд – это 58,4% от общей численности населения земного шара. И «поскольку количество человек по всему миру, которые не используют интернет, впервые сократилось до менее чем 3 млрд, можно говорить о начале важного этапа глобальной цифровизации, когда гаджеты из роскоши превратилась в необходимость», – заключают составители обзора из креативного агентства We Are Social.

Таким образом, можно сказать, что с развитием цифровых технологий «обычные» права человека приобрели свое цифровое выражение.

### **Чем отличаются цифровые права от нецифровых и кто должен их защищать?**

Основное отличие цифровых прав человека от «обычных» заключается в том, что если в оффлайн наши права в ответ порождают обязательства только государства – уважать, защищать и способствовать их наилучшей реализации, – то для реализации и защиты своих прав человека в цифровом пространстве мы, кроме государства, также полагаемся на бизнес. А это IT-гиганты, интернет-платформы, провайдеры, технологические компании, которые почти так же, как и государство могут защитить или, наоборот, нарушить наши права человека, а значит требуют какого-то регулирования. Но так как обязательства обеспечивать и защищать права человека лежат именно на государстве, то и регулирование деятельности IT-корпораций, провайдеров и другого бизнеса, обеспечивающего нам доступ в интернет, является обязанностью государства.

Возьмем для примера всем знакомые предложения (которые порой выглядят как ультиматум) веб-сайтов своим пользователям принять политику cookies. Как известно, cookies позволяют сайту отслеживать браузерные предпочтения анонимизированных, но вполне конкретных пользователей, собирать статистику и выстраивать таким образом маркетинговые стратегии. При

этом политики cookies могут нарушать право пользователей на приватность и препятствовать им в доступе к информации. Именно поэтому вступивший в силу в Евросоюзе в 2018 году Общий регламент защиты персональных данных (GDPR) обязал веб-сайты при использовании cookies запрашивать у пользователей согласие на добровольную подписку на информационное обеспечение (opt-in).

Отсутствие внешнего регулирования интернета и новых цифровых технологий также чревато такими нарушениями, как дискриминация, киберпреступность, вредоносное использование искусственного интеллекта и другие. Так, BBC в своей публикации о возможных угрозах искусственного интеллекта («ИИ») приводит такие примеры:

- «Такая программа, как AlphaGo – ИИ, разработанный компанией Google DeepMind, способный обыграть человека в игру го – может быть использована хакерами для нахождения шаблонов данных и уязвимости кодировки.
- Некий отдельно взятый злоумышленник может купить дрон, оснастить его программой распознавания лиц и с помощью него напасть на какого-то конкретного человека.
- Боты могут быть автоматизированы на производство фейковых видеоклипов с целью политических манипуляций.
- Хакеры могут использовать синтезированную речь для того, чтобы выдать себя за кого-то».

Новые технологии могут представлять угрозу даже для права на жизнь – вспомним использование вооруженных беспилотных летательных аппаратов.

В 2011 году ООН были приняты Руководящие принципы предпринимательской деятельности в аспекте прав человека, которые применительно к новым технологиям оговаривают такие обязательства бизнеса и государств, как:

- Ответственное ведение бизнеса при разработке, применении, торговле и использовании цифровых технологий;
- Сбалансированное применение государством механизмов регулирования, поощрения и обеспечения социальной ответственности бизнеса для того, чтобы с одной стороны бизнес соблюдал стандарты прав человека и

практиковал подотчетность перед обществом, а с другой мог беспрепятственно развиваться потенциал цифровых технологий в решении насущных проблем человечества;

- Разработка и применение четких алгоритмов действий как государства, так и бизнеса, по восстановлению нарушенных прав человека.

Что касается именно интернета, то тогда же, в 2011 году, Специальный докладчик ООН по свободе слова, представляя Генеральной Ассамблее свой доклад, так сказал об ответственности IT-корпораций за права человека интернет-пользователей:

«Хотя основную ответственность за права человека несут государства, корпорации также обязаны соблюдать права человека, а это значит, что они должны проявлять должную осмотрительность во избежание нарушения прав человека».

Сложность в том, что в интернете нет границ, а значит, нет ни международной, ни национальной юрисдикции, и поэтому государствам приходится договариваться и между собой, и с бизнесом, что позволяет сохранять баланс интересов и тех, и других, но совсем не исключает нарушений прав человека. Недемократические страны, например, заинтересованы в «собственном», суверенном интернете, как, например, это уже сделал Китай и собираются сделать Россия, Иран, Пакистан, а также некоторые другие страны. Казахстан тоже был замечен в таком стремлении.

Сегодня угроза цифровым правам исходит от самих государств. ООН называет такие распространенные нарушения государствами прав человека в интернете, как цензура, то есть фильтрация или ограничение доступа к контенту, криминализация легального выражения мнений, блокировки интернета, а также отсутствие надлежащей защиты права на тайну частной жизни (приватность) и защиту персональных данных.

Американская организация Freedom House в своем докладе «Свобода в Сети» в 2021 году отмечает, что с годами уровень свободы интернета в мире продолжает падать. В 2020 году власти как минимум 20 стран ограничивали доступ своих граждан к интернету, а в 21 стране ограничениям подвергались социальные сети. Власти по меньшей мере 45 государств, по словам экспертов,

используют изощренные методы слежки и получения личной информации пользователей Сети.

Что касается отношений государств и IT-гигантов, в докладе говорится, что правительства 48 государств, включая Казахстан, ввели новые правила для технологических компаний в отношении контента и личных данных пользователей.

Интернет в Казахстане был назван «несвободным». В тройку государств с наиболее свободным интернетом вошли Исландия, Эстония и Канада.

В сфере новых цифровых технологий самую распространенную угрозу правам человека представляет использование государствами систем контроля в виде цифровой идентификации личности (по биометрическим данным) и технологий слежки.

Для предупреждения подобных нарушений мировое правозащитное сообщество настаивает, чтобы любое регулирование интернета и цифровых технологий было основано на принципах прав человека, чтобы государства не ограничивали доступ к интернету, гарантировали цифровую безопасность и сохранность персональных данных, и не дали случиться тотальному цифровому контролю.

### **Международные и региональные договоренности в сфере цифровых прав**

В конце апреля 2022 года в Вашингтоне (США) была подписана «Декларация о будущем интернета», инициированная США и поддержанная сразу 60 странами, среди которых все страны-члены ЕС, а также Великобритания, Канада, Грузия, Украина и многие другие.

Этой Декларацией ее участники подтвердили приверженность правам человека во всей цифровой экосистеме и выразили намерение поддерживать и продвигать демократические процессы и активное участие в них граждан, защищать приватность, противостоять попыткам фрагментировать глобальный интернет и развивать свободную и состязательную глобальную экономику.

В сентябре 2023 года ожидается проведение Саммита будущего ООН, где планируется утвердить Глобальный цифровой договор с участием всех заинтересованных сторон: правительств, системы

ООН, бизнеса, гражданского общества, низовых организаций, научных кругов и отдельных групп населения, например, молодежи.

В отличие от вышеупомянутой Декларации, Глобальный цифровой договор будет оговаривать использование цифровых технологий в целом и «обозначит общие принципы открытого, свободного и безопасного цифрового будущего для всех». На утверждение, в частности, будут вынесены следующие задачи:

- обеспечение всеобщего подключения к интернету и охвата цифровыми технологиями;
- недопущение фрагментации интернета;
- предоставление людям вариантов использования их данных;
- применение прав человека в интернете;
- продвижение надежного интернета путем введения критериев ответственности за дискриминацию и распространение недостоверной информации»;
- регулирование искусственного интеллекта так, чтобы он соответствовал общим глобальным ценностям.

На региональном уровне тоже разработано много директив и регламентов. В Европе среди основных:

- Регламент 2015/2020 Европейского союза и Европейского парламента об установлении мер относительно открытого доступа в интернет (2015), который утвердил принцип «сетового нейтралитета», «запрещающего провайдерам телекоммуникационных услуг при распределении трафика отдавать предпочтение определенным классам приложений и услуг, а также ограничивать доступ к другим» через замедление или блокировку.
- Общий Регламент о защите персональных данных (General Data Protection Regulation или GDPR) (2018).
- Закон о цифровых услугах (Digital Markets Act или DMA) (2022), которым впервые налагаются ограничения на деятельность больших интернет-корпораций или монополий, таких как Google, Meta, Microsoft, обязывающие их, под угрозой крупных штрафов, а при повторном нарушении запрета на деятельность в ЕС, соответствовать требованиям относительно размещаемого на их платформах контента, сбора и передачи персональных данных пользователей и другого.

На примере Европы мы видим, как государства все больше активизируются в контроле бизнеса, обеспечивающего возможность людям пользоваться интернетом. Но остается вопрос: а кто будет контролировать государство? Это – задача остальных заинтересованных сторон: межправительственных организаций и гражданского общества. Поэтому в регулировании интернета так важен мультистейкхолдерный подход, то есть подход с учетом пожеланий и интересов всех вовлеченных сторон, а не только бизнеса или государств.

На глобальном уровне с 2006 года существует площадка для такого мультистейкхолдерного обсуждения – Форум управления интернетом (IGF), – где различные группы заинтересованных сторон обсуждают вопросы государственной политики в отношении интернета. По предложению Генерального секретаря ООН разработана Дорожная карта по цифровому сотрудничеству, и права человека – всегда одна из центральных тем для обсуждения на IGF.

На уровне страновых инициатив, в мире пока только в одной стране – Бразилии – был принят так называемый «закон об интернете». Называется он **«MARCO CIVIL DA INTERNET»** или кратко **«MARCO CIVIL»**. Его еще называют бразильской «интернет-конституцией». Этот закон определяет «порядок использования интернета в Бразилии, который основывается на таком фундаментальном праве как свобода выражения мнений, а также зиждется на следующих основополагающих положениях: необходимость учета трансграничного характера интернета и его глобального охвата населения всего мира; уважения прав человека; развития личности и осуществления гражданских прав в цифровой среде; плюрализме и многообразии; открытости и взаимодействия; свободы предпринимательства, конкуренции и защите прав потребителей; учета социального предназначения интернета».

### Ситуация с цифровыми правами в Казахстане

Главное, что нужно знать о регулировании государством интернета в Казахстане, – интернет отнесен к СМИ. Это значит, что и на сайты, и на социальные сети распространяются все те требования, которые государство налагает на печатные медиа. Это включает законодательные требования по авторским

правам, по рекламе, по распространению несоответствующей действительности информации (слухов или фейков), по защите чести и репутации, например, Первого президента, и многие другие.

За нарушения доступ к сайтам может быть ограничен, при этом не только по решению суда, но и «уполномоченного органа». Список (реестр) сайтов, доступ к которым был ограничен, актуализируется нерегулярно, и посмотреть, какие именно сайты и на каком основании заблокированы, не всегда возможно. Многие сайты остаются заблокированными годами, часто их зарубежные владельцы порой даже не подозревают, что их сайт в Казахстане заблокирован.

Казахстан неоднократно выказывал намерение «национализировать» интернет, что означает попытки обязать иностранные интернет-платформы регистрироваться в Казахстане; локализовать хранение персональных данных (обязать собственников или операторов персональных данных хранить эти данные на серверах исключительно внутри Казахстана); установить, подобно Китаю, **firewall**, в том числе внедрив технологию **man-in-the-middle**, известную в Казахстане как «национальный сертификат безопасности», когда государство выступает посредником между пользователем и иностранным сайтом – пожарной стеной (firewall), – пресекая (или отсеивая) вредоносную для пользователя, по мнению государства, информацию. При этом есть риск попадания госоргану-посреднику конфиденциальной информации, например, с персональными или банковскими данными пользователей, паролями и другой. В январе 2022 года, во время объявленного чрезвычайного положения, интернет в Казахстане вовсе был отключён на несколько дней.

Обеспокоенность правозащитников вызывает требование государства об обязательном теперь сборе биометрических данных граждан (и не только) для биометрической аутентификации личности, широкое использование неизбежной слежки (видеонаблюдение и видеомониторинг).

Вместе с этим, в Казахстане довольно хорошо развиты инструменты «электронного участия» граждан в работе государства. Казахстан заявил, что взял курс на «цифровое государство».

В Казахстане правозащитники активно защищают цифровые права. Группа экспертов по цифровым правам, члены которой стали авторами этого пособия, постоянно мониторит ландшафт цифровых прав и свобод в Казахстане, взаимодействует с государством при разработке законов, связанных с цифровыми технологиями и интернетом, отслеживает случаи блокировок веб-сайтов и добивается снятия ограничений, выступает с публичными заявлениями, проводит тренинги по цифровым правам, то есть делает все, чтобы цифровые права человека не нарушались.



**СВОБОДА**

ВЫРАЖЕНИЯ  
МНЕНИЯ ОНЛАЙН



*Гульмира Биржанова*

## СВОБОДА ВЫРАЖЕНИЯ МНЕНИЯ ОНЛАЙН

«Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ» – гласит Всеобщая декларация прав человека, ст. 19<sup>1</sup>. Те же принципы отражены в МПГПП (Международном Пакте о гражданских и политических правах)<sup>2</sup>.

Принципы обеспечения прав и свобод человека онлайн были зафиксированы на 17-й сессии Совета ООН по правам человека (2011г.), где Специальный докладчик ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение представил доклад о роли Интернета для свободы выражения мнений. На сессии была принята совместная декларация Специальных докладчиков по правам человека о свободе выражения мнений в Интернете. В 2012 году была принята резолюция Совета ООН по правам человека, в которой утверждается, что права человека, в частности право на свободу выражения мнений, должны также защищаться и в онлайн-сфере<sup>3</sup>.

### Международные стандарты в области свободы выражения мнения

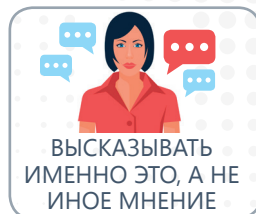
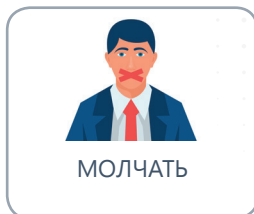
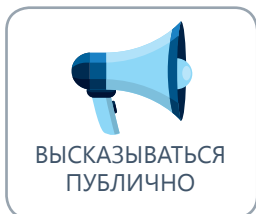
Свобода выражения мнения – базовое право, без которого невозможна реализация других фундаментальных прав человека (право на свободу собраний и объединений, право на свободу мысли, совести и религии, убеждений, независимые выборы и т.д.)

<sup>1</sup> [https://www.un.org/ru/documents/decl\\_conv/declarations/declhr.shtml](https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml)

<sup>2</sup> [https://www.un.org/ru/documents/decl\\_conv/conventions/pactpol.shtml](https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml)

<sup>3</sup> <https://www.ohchr.org/ru/disabilities/human-rights-council-resolutions>

## СВОБОДА ПРИДЕРЖИВАТЬСЯ СВОЕГО МНЕНИЯ



### Международные принципы в области свободы выражения мнения

- Тема высказывания. Если спорное высказывание посвящено политическим вопросам или вопросам общественной значимости, то оно имеет более высокую степень защиты в рамках ст. 19 Пакта.
- Субъект, о котором говорят. Принцип повышенной терпимости публичных фигур: «...пределы допустимой критики в отношении политиков как таковых шире, чем в отношении частного лица». Поскольку политики и общественные деятели сознательно выставляют себя на суд публики, они должны быть готовы к более пристальному вниманию со стороны прессы и общественности к каждому своему слову и делу.
- Общественный интерес — это не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правому государству и гражданскому обществу, общественной безопасности, окружающей среде. Следует различать общественный интерес и общественное любопытство.

### Баланс между правом на частную жизнь и свободу слова

#### ПРАВО НА СВОБОДУ СЛОВА



ПРАВО НА «ЧАСТНУЮ ЖИЗНЬ» =  
НЕПРИКОСНОВЕННОСТЬ + ОХРАНА ПЕРСОНАЛЬНЫХ ДАННЫХ

## В каких случаях допустимы ограничения свободы слова

- Должны быть установлены законом и являться необходимыми.
- Должны применяться для уважения прав и репутации других лиц.
- Для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

## Национальное законодательство

СТАТЬЯ 20 Конституции РК гарантирует право на получение и распространение информации любым не запрещенным законом способом. В этой же статье говорится о том, что перечень сведений, составляющих государственные секреты, определяется законом<sup>4</sup>.

СТАТЬЯ 2 Закона о СМИ также гласит, что свобода слова, творчества, выражения в печатной и иной форме своих взглядов и убеждений, получение и распространения информации любым не запрещенным законом способом гарантируются Конституцией РК. Цензура запрещается<sup>5</sup>.

В 2009 году в Казахстане все интернет-ресурсы приравнили к СМИ: «средство массовой информации — периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная запись и иная форма периодического или непрерывного публичного распространения массовой информации, включая интернет-ресурсы». Соответственно, социальные сети в рамках законодательства тоже являются СМИ.

## ПРАВОВЫЕ РИСКИ



<sup>4</sup> <https://adilet.zan.kz/rus/docs/K950001000>

<sup>5</sup> <https://adilet.zan.kz/rus/docs/Z990000451>

Некоторые пользователи социальных сетей уверены, что, сделав свой профиль закрытым, они могут публиковать всё, что угодно. Однако это далеко не так. Всё, что вы публикуете в интернете, — публично, поэтому не забывайте о приватности своего блога или аккаунта. Любая скрытая информация может стать общей и доступной, а если её признают противоправной, вас могут привлечь к ответственности.

Если вы делаете публичное высказывание, касающееся большой группы людей, которую можно описать в терминах национальности, гражданства, религии, языка, постарайтесь отнестись к нему внимательнее.

Воздержитесь от публикации сообщений, которые могут быть неправильно истолкованы (даже если вы их публикуете от своего лица) - призывающие к разжиганию межнациональной розни, свержению политического строя, напрямую участвовать в конфликтах, а также распространению непроверенной информации.

Не позволяйте себе публиковать непроверенную информацию, поскольку в Казахстане с 2014 года действует норма уголовного кодекса, которая устанавливает ответственность за распространение заведомо ложной информации и предусматривает наказание до 10 лет лишения свободы<sup>6</sup>.

Прежде чем поделиться информацией, проверьте её на достоверность. Если нет уверенности и доверия к источнику, от репоста или рассылки лучше отказаться. Помните, что репост – это распространение информации, и репост без комментариев тоже является публикацией.

Если под постом появились комментарии, которые покажутся подсудными, несут ли за них ответственность? По закону – нет. Но на практике известны случаи, когда обвинение приписывало комментарии самому автору поста. И часто суды связывают комментарии со статьей или публикацией.

Что касается статей распространения заведомо ложной информации, возбуждения розни и призывов к терроризму, то это статьи публичного обвинения. Правоохранительные органы сами могут начать досудебное расследование – на основании мониторинга соцсетей, а также любой заинтересованный гражданин может заявить о преступлении.

<sup>6</sup> [https://online.zakon.kz/m/document?doc\\_id=31575252](https://online.zakon.kz/m/document?doc_id=31575252)

## **Перечень запрещенной информации**

(выдержки из Закона о СМИ и Закона о связи)

- Пропаганда или агитация культа жестокости и насилия, социального, расового, национального, религиозного, сословного и родового превосходства,
- Пропаганда или агитация насильственного изменения конституционного строя,
- Нарушения целостности РК, подрыва безопасности государства, войны,
- Пропаганда экстремизма или терроризма,
- Публикация материалов и распространение информации, направленной на разжигание межнациональной и межконфессиональной вражды,
- Запрещается размещать информацию о вакансиях для приема на работу, содержащую требования дискриминационного характера в сфере труда.
- Дача разрешения на публикацию в СМИ информации экстремистских материалов,

## **Какие действия можно предпринять, если начато уголовное преследование за пост или комментарий?**

Если пришла досудебная претензия или поступило заявление с требованием привлечь к ответственности от другого пользователя, необходимо сразу же поставить об этом в известность как много больше лиц и обязательно создать общественный резонанс.

## **Какие доказательства будут надежными?**

- Видео или аудиозапись рассказа
- Фотографии
- Документы (не обязательно иметь оригиналы документов, подойдут их копии)
- фотографии или даже скриншоты сайтов
- Судебные решения и приговоры

Если уже заведено уголовное дело по статьям 174 или 274 УК РК, нужен квалифицированный адвокат, желательно специализирующегося на подобных делах.

Необходимо также привлечь к проведению филологической экспертизы стороннего независимого эксперта. Независимый анализ спорной фразы — важный документ не только для суда первой инстанции. В случае обвинительного приговора в казахстанской системе отправления правосудия экспертиза пригодится при обращении в международную инстанцию.

### **Распространение информации о детях в сети**

У всех детей, как и у взрослых, есть право на собственное изображение и защиту персональных данных. При проведении интервью, фото и видеосъемки с детьми необходимо согласовать действия с родителями или законными представителями. Поскольку в соответствии с Законом «О браке и семье» (ст.71) родители являются законными представителями своего ребенка и выступают в защиту его прав и интересов в отношениях с любыми физическими и юридическими лицами, в том числе в суде, без специальных полномочий.

Дети, пострадавшие в результате противоправных действий (бездействия) и подозреваемые и (или) обвиняемые в совершении административных правонарушений.

Нельзя распространять в СМИ или сетях телекоммуникаций персональные и биометрические данные такого ребенка, включая информацию об его родителях и иных законных представителях, иной информации, позволяющей установить личность.

### **Можно распространять информацию:**

- если несовершеннолетний признан судом виновным в совершении тяжких и (или) особо тяжких преступлений, включая информацию о его родителях и иных законных представителях;
- если есть согласие несовершеннолетнего, достигшего 14-летнего возраста, пострадавшего в результате противоправных действий (бездействия), и его законных представителей;
- если есть согласие законных представителей несовершеннолетнего, не достигшего 14-летнего возраста, пострадавшего в результате противоправных действий (бездействия);

- если есть согласие несовершеннолетнего, достигшего 16-тилетнего возраста, совершившего административные и (или) уголовные правонарушения, и его законных представителей;
- если речь идет о распространении в СМИ информации, полученной от органов, ведущих уголовный процесс (в целях содействия расследованию преступления, установлению лиц, причастных к совершению преступления, розыску пропавших несовершеннолетних в объеме, необходимом для достижения указанных целей);
- если есть согласие одного законного представителя несовершеннолетнего пострадавшего лица, в случае если второй законный представитель находится за пределами Республики Казахстан и его согласие получить не представляется возможным;
- если законный представитель является подозреваемым или обвиняемым в совершении противоправных действий в отношении несовершеннолетнего, достигшего 14-тилетнего возраста и пострадавшего в результате противоправных действий, или его законных представителей;

За нарушение закона предусмотрена административная ответственность<sup>7</sup>.

## ГЛОССАРИЙ

**Публичное лицо** – это физическое лицо, которое наделено значимыми публичными функциями.

**Общественный интерес** – это не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правовому государству и гражданскому обществу, общественной безопасности, окружающей среде.

**Заведомо ложная информация** – информация, создающая опасность нарушения общественного порядка или причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

<sup>7</sup> <https://adilet.zan.kz/rus/docs/Z990000451>

**Рознь** – умышленные действия, направленные на разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни, на оскорбление национальной чести и достоинства либо религиозных чувств граждан, а равно пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, сословной, национальной, родовой или расовой принадлежности.

**Пропаганда** – под пропагандой в средствах массовой информации понимается распространение взглядов, фактов, аргументов и иной информации, в том числе намеренно искаженной, для формирования положительного общественного мнения о запрещенной законодательством Республики Казахстан информации и (или) побуждения к совершению противоправного действия или бездействию неограниченного круга лиц.

**Цензура** – предварительное согласование сообщений и материалов средствами массовой информации с государственными органами, должностными лицами и иными организациями по их требованию или по иным основаниям с целью ограничения или наложения запрета на распространение сообщений и материалов либо их отдельных частей;

**Экстремизм** – какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них, и преследуемые в уголовном порядке в соответствии с национальным законодательством.

### **Творческое задание**

Найдите посты, статьи, сюжеты, где, на ваш взгляд, есть признаки "hate speech". Обсудите в группе эти примеры.

**ДОСТУП**

К ИНФОРМАЦИИ



*Диана Окремова*

## ДОСТУП К ИНФОРМАЦИИ

Доступ к информации – одно из основных прав человека, которое в последние годы все больше реализуется онлайн. Свободный доступ к информации влияет на качество государственного управления, прозрачность, подотчетность, активность гражданского общества, помогает снижать уровень коррупции. Благодаря развитию онлайн инструментов все больший объем информации становится доступен в сети, обеспечивая гражданам возможность анализировать, проводить адвокационные кампании, участвовать в процессах принятия государственных решений.

### Международные стандарты

Первый закон о праве на доступ к информации появился в 1766 году в Швеции и почти 200 лет был единственным подобным документом в мире. Он позволял национальному парламенту получать доступ к информации от короля. В 1951 году закон о доступе к информации стал действовать в Финляндии. Сегодня более 100 стран приняли нормы национального права, регулирующие процессы в этой сфере.

Право на информацию (Right of Access to information, RTI) является одним из базовых прав человека. Оно описано в международном законодательстве как право, которое относится в свободе самовыражения, необходимое для укрепления демократии и общественного участия; как антикоррупционный инструмент, а также как важный инструмент защиты окружающей среды. Основными преимуществами реализации этого права являются улучшение качества государственного управления, повышение инвестиционного климата, снижение коррупции, активизация гражданского общества и усиление его роли в принятии решений.

### Базовые нормы доступа к информации содержатся в:

- ст. 10 Всеобщей декларации прав человека,
- ст. 19 Международного пакта о гражданских и политических правах (МПГПП)

- ст. 13 Конвенции ООН против коррупции,
- в Орхусской конвенции,
- в документах ООН, ОБСЕ, ЮНЕСКО, Конвенции Совета Европы о доступе к официальным документам, решениях Европейского суда по правам человека, резолюциях Комитета и Парламентской ассамблеи Совета Европы.

Главным принципом считается принцип максимальной открытости информации, от которого можно отступить в очень ограниченных случаях, и они должны быть четко и узко сформулированы.

В директивном замечании Комитета ООН по правам человека сказано, что *«ст. 19 Пакта гарантирует право на информацию, находящуюся в распоряжении государственных органов. Он требует, чтобы государства в приоритетном порядке распространяли информацию, имеющую общественный интерес, и что доступ к ней должен быть "легким, быстрым, эффективным и практическим"»*. В замечании также сказано, что государства должны учредить "необходимые процедуры": например, законодательство для реализации права на информацию; плата за доступ к информации должна быть ограничена в размерах, отвечать на запросы следует своевременно, органы власти должны обосновывать отказы в предоставлении, а государствам следует создать механизмы обжалования отказов.

Конвенция ООН против коррупции требует, чтобы государства принимали надлежащие меры для обеспечения населения эффективным доступом к информации, и обязывает защищать информаторов (whistle-blower).

Выполнение стандартов накладывает два обязательства на правительства и государственные органы. Во-первых, обязанность обнародовать ключевую информацию о мероприятиях, осуществляемых государственными органами; во-вторых, обязанность отвечать на запросы людей и предоставлять доступ к документам.

### **Основные принципы базовых законов о доступе к информации следующие:**

- **Право на доступ** – право физического лица, организации или юридического лица на возможность запрашивать

информацию у государственных органов без обязанности правового обоснования своего к ней интереса;

- **Обязанность предоставлять информацию** – обязанность государственных органов отвечать на запросы и предоставлять информацию. Это включает механизмы работы с запросами и установление предельных сроков ответа на запросы;
- **Исключения** позволяют не раскрывать определенные категории информации. Обычно для этого требуется, чтобы до сокрытия информации было показано, какой вред ее раскрытие может нанести;
- **Внутреннее обжалование** – механизмы, позволяющие заявителю оспаривать отказы в предоставлении информации;
- **Внешнее обжалование и надзор** – рассмотрение жалоб независимым органом;
- **Проактивная публикация** – требование к органам власти проактивно публиковать информацию о своей деятельности;
- **Санкции** – наказание для должностных лиц за незаконное уничтожение или изменение информации либо за незаконный отказ в ее предоставлении.

Надо отметить, что в последние годы проактивный доступ к информации обеспечивается такими способами как открытые данные и электронные правительства.

Важно знать, что право на доступ к информации, как и право на свободу выражения мнений, не является абсолютным и может быть ограничено. Так, п. 3 ст. 19 Международного пакта о гражданских и политических правах говорит, что ограничения должны быть установлены законом и являться необходимыми: а) для уважения прав и репутации других лиц; б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения. Это можно использовать в качестве теста при определении законности и обоснованности ограничения или нарушения права на свободу информации.

Если национальные законы не соответствуют указанным правилам, то они противоречат международным нормам, и в спорных моментах должны применяться международные нормы.

Существуют различные рейтинги, в которых оценивается ситуация с доступом к информации в странах. Наиболее

известные – Карта глобального права на информацию<sup>8</sup> и Обзор открытости бюджета<sup>9</sup>. Также действуют международные партнерства, такие как OGP (Open Government Partnership), GRECO (Group of States against Corruption), стимулирующие государства внедрять прогрессивные стандарты доступа к информации.

В 2015 году предложением ЮНЕСКО 28 сентября был назначен «Международным днем всеобщего доступа к информации».

### Казахстанская практика

Право на доступ к информации закреплено в различных национальных документах:

- в ст. 20 Конституции («Каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом. Перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом»);
- в Законе о доступе к информации<sup>10</sup>;
- в Законе о СМИ<sup>11</sup>;
- в Экологическом кодексе (глава 21)<sup>12</sup>;
- в Бюджетном кодексе (принцип транспарентности, п. 4 Ст. 4)<sup>13</sup>
- в Законе об архивах<sup>14</sup>
- Закон о недрах и недропользовании (ст. 7)<sup>15</sup> и др.

### К прогрессивным пунктам закона о доступе к информации можно отнести следующие:

- Служебная информация теперь не относится к информации с ограниченным доступом, что формально делает доступным большой массив документов госорганов;
- Квазигосударственные органы (такие как «Самрук-Казына», КТЖ и другие с госучастием) относятся к обладателям

<sup>8</sup> <https://www.rti-rating.org/>

<sup>9</sup> <https://www.internationalbudget.org/open-budget-survey>

<sup>10</sup> <http://adilet.zan.kz/rus/docs/Z1500000401/z150401.htm>

<sup>11</sup> [http://adilet.zan.kz/rus/docs/Z990000451\\_](http://adilet.zan.kz/rus/docs/Z990000451_)

<sup>12</sup> <http://adilet.zan.kz/rus/docs/K070000212>

<sup>13</sup> <http://adilet.zan.kz/rus/docs/K080000095>

<sup>14</sup> <http://adilet.zan.kz/rus/docs/Z980000326>

<sup>15</sup> <http://adilet.zan.kz/rus/docs/K1700000125>

информации и обязаны предоставлять ее наряду с госорганами;

- Четко регламентируется порядок обращений на сайте «электронное правительство». Граждане могут получать информацию через e-gov, что значительно упрощает процедуру и экономит время.

Закон делит информацию на три категории: общедоступную информацию, информацию, доступ к которой не может быть ограничен, и информацию с ограниченным доступом. К последней относятся государственные секреты, тайны (личная, банковская, усыновления, налоговая, врачебная, коммерческая), служебная информация с пометкой «Для служебного пользования»<sup>16</sup> (далее – ДСП). Последний пункт вызывает много нареканий, споров и несогласий.

Так, в «Правилах отнесения сведений к служебной информации ограниченного распространения и работы с ней» устанавливается право руководителей государственных органов самостоятельно относить те или иные сведения к категории «Для служебного пользования». При этом Правила устанавливают возможность широкого толкования критериев информации ограниченного распространения и, более того, список критериев не является закрытым, давая возможность ограничивать доступ к информации, если они, по мнению исполнителя, могут быть использованы в ущерб интересам государственного органа. Эти нормы, в свою очередь, дают возможность для злоупотреблений ограничениями и создают потенциал для незаконного сокрытия общественно значимой информации.

Кроме того, закон не предусматривает единый формат опубликования информации, поэтому этот вопрос остается на совести каждого госоргана. К примеру, на интернет-ресурсах раскрывается информация общего характера, но практически не раскрывается информация о проведении проверок. Или размещается план проверок, но отсутствуют результаты её проведения. Сведения об оказываемых государственных услугах предоставляются частично, с различной степенью детализации, обычно не по всем услугам и не в простом и понятном виде.

<sup>16</sup> <http://adilet.zan.kz/rus/docs/P1500001196>

Во время пандемии практика показала, что государственные органы не готовы в полной мере справляться с новыми вызовами. Так, значительно увеличилось количество жалоб от журналистов по предоставлению информации. В связи с переходом на онлайн формат возникли проблемы с участием СМИ в совещаниях, судебных онлайн-процессах, да и в целом с грамотной организацией оперативного информирования общественности о ситуации.

В прошлом году группа правозащитных организаций и граждан обратилась к президенту и парламенту с требованием пересмотреть действующие правила отнесения информации к категории «для служебного пользования»

Эксперты отметили, что с момента введения карантина гражданское общество столкнулось с тем, что государственные органы без видимых причин все чаще относят информацию к категории ДСП. При этом, как показывает практика, оспорить действия чиновников невозможно, поскольку на соответствующих приказах также стоит гриф ДСП. Так, была засекречена информации о том, какие СМИ получают деньги по линии государственного информационного заказа; о том, каков размер зарплаты депутатов мажилиса парламента.

Что касается бюджетной информации в целом, то здесь по-прежнему нет единых требований для опубликования. Основные сведения об использовании бюджета можно найти на сайте государственных закупок<sup>17</sup>, который в период пандемии стал главным источником бюджетных новостей. Активисты и журналисты публиковали сведения окупаемых чиновниками услугах, предавая огласке сомнительные закупки и обращая на них внимание Антикоррупционного агентства.

Данные о бюджете также можно найти на портале e-gov.kz (открытые бюджеты), на сайтах Агентства по статистике, Счетного комитета, Министерства финансов. По статистике в разделе «Открытые бюджеты» портала «Открытое правительство» опубликовано более 13 500 проектов бюджетных программ, однако сложно сделать вывод о степени вовлеченности граждан в процесс обсуждения проектов бюджетных программ и отчетов о реализации бюджетных средств, поскольку статистика посещения отсутствует. Кроме того, информация обновляется

<sup>17</sup> [www.goszakup.gov.kz](http://www.goszakup.gov.kz)

нерегулярно и бессистемно. Так, например, информация о бюджете Конституционного совета последний раз обновлялась три года назад. По администрации президента и канцелярии первого президента данные вообще отсутствуют. При этом информацию о расходах этих ведомств можно найти на сайте госзакупок.

В последнее время появились общественные инициативы, предоставляющие населению бюджетную информацию в простом и доступном виде<sup>18</sup>.

В конце прошлого были приняты поправки в закон о Доступе к информации, которые коснулись нескольких моментов. Во-первых, четко обозначен уполномоченный орган в области доступа к информации (им стало Министерство информации), описаны его функции, полномочия и ответственность. Во-вторых, даны определения понятиям «интернет-портал открытого диалога» и «блог-платформа первых руководителей». В-третьих, перечислены компетенции правительства, уполномоченных органов в сфере информации и информатизации.

Также детализирована информация, которая должна размещаться на интернет-ресурсах обладателей информации. В частности, определены списки категорий информации, которая размещается на сайтах судов, акиматов, министерств, квазигосударственных органов. К обладателям информации теперь отнесены также исполнители функций центральных и (или) местных исполнительных органов.

В 2020 году Казахстан впервые набрал 38 баллов в Индексе восприятия коррупции Transparency International, поднявшись на 19 позиций<sup>19</sup>. Вместе с тем, эксперты отметили, что «власти Казахстана допускали нарушения демократических свобод, связанных с прозрачностью и доступом к финансовой информации о расходах на здравоохранение, необоснованными ограничениями деятельности журналистов, правозащитников и представителей гражданского общества».

<sup>18</sup> [www.publicbudget.kz](http://www.publicbudget.kz), <http://openbudget.kz/>, <http://nedra.echo.kz/>

<sup>19</sup> [http://tikazakhstan.org/v-indekse-vospriyatiya-korrupsii-kazahstan-podnyalsya-na-19-pozitsij-nabrav-vpervye-38-ballov/?fbclid=IwAR27ybKY3\\_MIFsDK0kZxZQmndAhTctv08i7VxyQD-HmehlLiwcNduj3iUHs](http://tikazakhstan.org/v-indekse-vospriyatiya-korrupsii-kazahstan-podnyalsya-na-19-pozitsij-nabrav-vpervye-38-ballov/?fbclid=IwAR27ybKY3_MIFsDK0kZxZQmndAhTctv08i7VxyQD-HmehlLiwcNduj3iUHs)

## АЛГОРИТМ ДЕЙСТВИЙ

Если вы решили реализовать свое право на доступ к информации, в первую очередь необходимо изучить одноименный закон.

Итак, что такое информация согласно закону? Это – сведения, зафиксированные на любом носителе и имеющие реквизиты, позволяющие их идентифицировать. То есть это любая информация, которая уже есть в организации, которую не нужно создавать специально.

Запрашивая информацию, вы являетесь ее пользователем. А организации, ее предоставляющие, называются обладателями информации. Запрашивать информацию можно в государственных органах, парламенте, квазигосударственных органах, у монополистов и доминантов рынка. Также вы можете запрашивать сведения у частных фирм, только о бюджетных расходах.

Например, если компания выигрывает тендер на ремонт дорог, вы имеете право знать подробности, и предоставить их должна как фирма, так и госорган, проводивший тендер.

Каким образом вы можете получить информацию? Существует несколько способов, среди которых – размещение в прессе, в помещениях госорганов, на интернет-ресурсах. Сюда также входят публичные отчеты первых руководителей, заседания коллегий госорганов. Но наиболее действенный способ – это запрос. Он может быть, как устным, так и письменным. Здесь очень помогут инструменты портала электронного правительства. Для этого нужно зарегистрироваться на сайте e-gov.kz и получить электронно-цифровую подпись. После этого вы можете отправлять запросы через личный кабинет, либо на блогах первых руководителей госорганов.

Ответ на письменный запрос должна предоставляться в течение 15 дней. Если запрашиваемая информация входит в компетенцию нескольких обладателей информации, срок рассмотрения может быть продлен еще на 15 дней. Об этом вам должны сообщить в течение трех рабочих дней.

Если же ваш запрос требует ответа другого органа, его перенаправят туда, уведомив вас об этом.

Важно знать, что ответ на письменный запрос предоставляется по вашему выбору в бумажной или электронной формах на языке обращения.

В законе есть также перечень информации, доступ к которой не подлежит ограничению. Сюда входят сведения о чрезвычайных ситуациях, угрожающих безопасности и здоровью граждан, о состоянии экологии и другая. Важно, что сюда также относится информация о формировании и расходовании средств из республиканского и местного бюджетов. Это значит, что бюджетные траты всегда должны быть максимально прозрачны и доступны гражданам.

К сожалению, в некоторых случаях вам могут в информации отказать. Например, если госорган не может установить содержание запроса, если еще не принято решение по результатам проверок или вы просите дать правовую оценку актов. Мотивированный ответ об отказе в информации вы должны получить в течение пяти рабочих дней.

Если вам отказали в информации, на ваш взгляд, незаконно, вы можете обжаловать это решение. Есть несколько способов: написать жалобу вышестоящему лицу или в вышестоящий орган, либо обратиться в суд.

Санкции за нарушения предусмотрены в ст. 456-1 «Незаконное ограничение права на доступ к информации» КОАП РК<sup>20</sup> Ответственность может наступить за:

- Неправомерный отказ в предоставлении информации либо предоставление заведомо ложной информации в случаях, когда такая информация подлежит предоставлению по запросу пользователя информации;
- Размещение заведомо ложной информации в средствах массовой информации, на интернет-ресурсе обладателя информации, на интернет-портале открытых данных или иными способами, предусмотренными законодательством Республики Казахстан;
- Неправомерное отнесение информации, не являющейся информацией с ограниченным доступом, к информации с ограниченным доступом.

<sup>20</sup> <http://adilet.zan.kz/rus/docs/K1400000235>

Если суд признает, что чиновник нарушил закон о доступе к информации, он может быть оштрафован на сумму от 30 до 100 МРП.

### Полезные ссылки

Агентство по статистике [www.stat.gov.kz](http://www.stat.gov.kz)

Комитет правовой статистики <http://pravstat.prokuror.kz>

Комитет государственных доходов [www.kgd.gov.kz](http://www.kgd.gov.kz)

Электронное правительство [www.egov.kz](http://www.egov.kz)

Портал госзакупок [www.goszakup.gov.kz](http://www.goszakup.gov.kz)

Интерактивная карта бюджетов [www.publicbudget.kz](http://www.publicbudget.kz)

Платежи недропользователей на социально-инфраструктурные проекты <https://nedra.echo.kz/>

Отчеты международных организаций

Рейтинги всемирного банка

Рейтинги международных организаций (Freedom house, Transparency International)

Профильные ассоциации и профсоюзы

Исследовательские агентства

### Творческое задание

Составьте и отправьте запрос на тему, связанную с расходованием бюджетных средств, в местный акимат или министерство, проанализируйте ответ. В случае отказа – составьте жалобу и также проанализируйте ответ.

**АВТОРСКОЕ**

ПРАВО В  
ИНТЕРНЕТЕ



*Ольга Диденко*

## АВТОРСКОЕ ПРАВО В ИНТЕРНЕТЕ

### Мифы и реалии авторского права

Широкое распространение интернета, социальных сетей, мессенджеров в нашей жизни повлияли на то, как быстро и легко чужие тексты, фотографии и аудиовизуальные материалы могут быть использованы без разрешения правообладателей для иллюстраций материалов в СМИ, собственных постов и блогов, интернет-изданий, выпуска газет, сайтов, программ и любого другого контента. Такая быстрота и легкость воспроизведения порождает многочисленные мифы о соблюдении авторских прав в интернет-пространстве. Самые распространенные из них:

**Миф 1.** Все, что есть в интернете в открытом доступе, можно брать и публиковать

**Миф 2.** Только высокохудожественные фотографии защищены авторским правом

**Миф 3.** Только те фотографии, на которых изображены люди, защищены авторским правом

**Миф 4.** Если текст, фотография или аудиовизуальный материал опубликованы в открытом аккаунте, то разрешение на их републикацию не требуется

**Миф 5.** Даже если я нарушу чьи-то права, ничего за это не будет (никто не пойдет разбираться в суд, никто не узнает и т.д.)

Это очень опасные мифы и наиболее опасны они для журналистов и всех, кто работает в медиа. Почему? Для этого есть две причины: во-первых, журналисты и все, кто работают в медиа, сами создают авторский контент и могут сталкиваться с нарушением авторских прав, во-вторых, редакции СМИ могут использовать произведения других авторов для различных целей, связанных с подготовкой и выпуском продукции СМИ и, таким образом, могут нарушать права других авторов.

## Авторское право и его место в ряду дисциплин для будущих журналистов

Концепция авторских прав базируется на очень простой идее: если человек создает уникальное и оригинальное произведение, вне зависимости от формы и способа выражения, он – **автор**, и его права на использование этого произведения надежно защищены. Эта защита не зависит от того, зарегистрировали вы свое авторское право или нет. Созданные произведения чаще всего называются **объектами авторского права** (ОАП) или **интеллектуальной собственностью** (ИС). Какие это могут быть произведения? Литературные, научные и художественные произведения, как-то: произведения письменные, музыкальные, драматические и кинематографические, произведения живописи, графики и скульптуры<sup>21</sup>.

Автору гарантируется защита как **неимущественных авторских прав**: право на указание авторства, прав на использование псевдонима, право на обнародование. Автор также может защищать свои авторские права всеми доступными способами, защищать свою репутацию как автора, если его произведение искажено, извращено или изменено таким образом, что это наносит ущерб.

Ему гарантируется, что, создавая литературные и художественные произведения, он сможет их распространять и получать от этого доход (**авторское вознаграждение**). Быть автором должно быть выгодно с экономической точки зрения. Автору гарантируется, что не только он, но и его наследники будут получать выгоду от распространения его произведений до его смерти и после 50 лет<sup>22</sup> после его смерти... Это называется **авторское вознаграждение за каждый случай использования ОАП**. Но существуют **исключения для правомерного использования авторских произведений в определенных случаях**.

<sup>21</sup> Статья 1 Всемирной Конвенции об авторском праве (Женева), пересмотренной в Париже 24 июля 1971 года. Текст конвенции на русском языке доступен по ссылке: [https://www.un.org/ru/documents/decl\\_conv/conventions/pdf/copyright.pdf](https://www.un.org/ru/documents/decl_conv/conventions/pdf/copyright.pdf)

<sup>22</sup> В некоторых юрисдикциях этот срок составляет 70 лет.

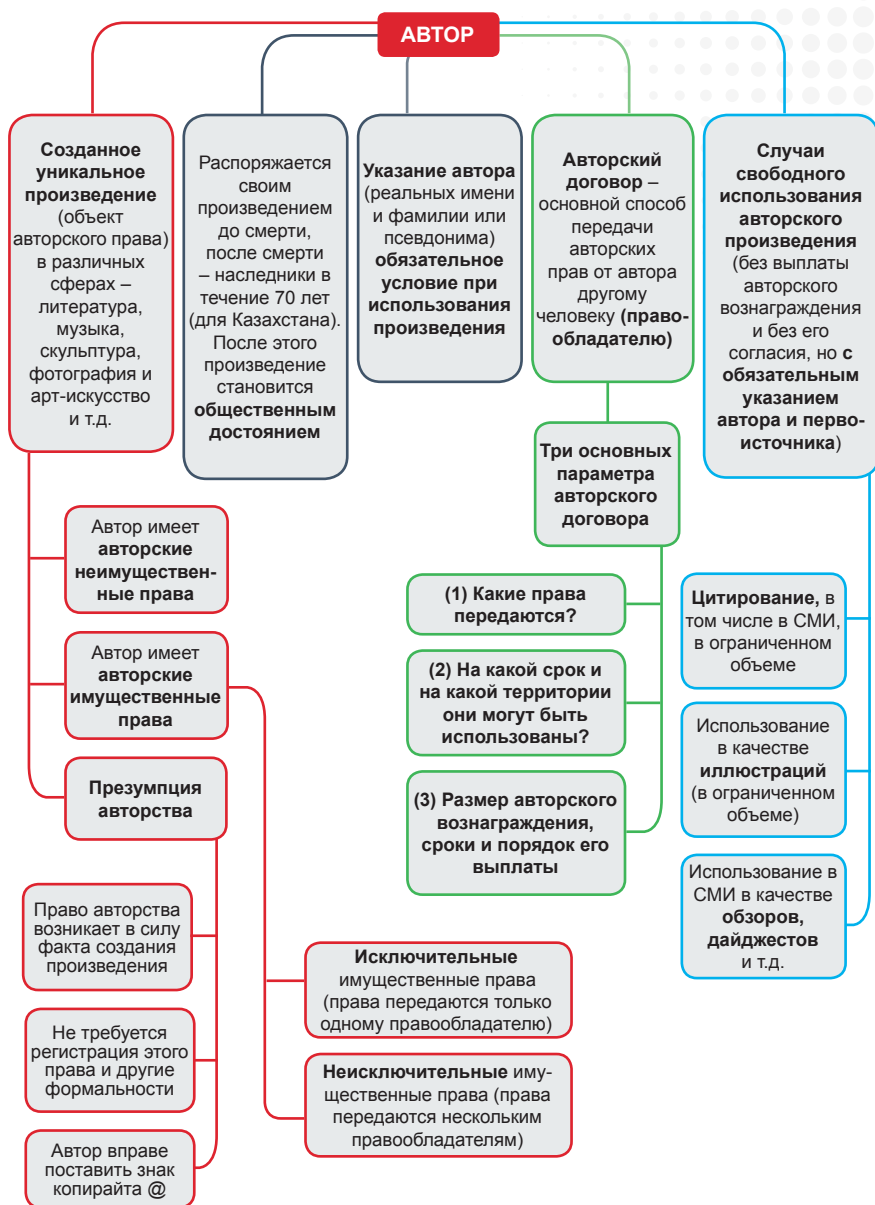


Рисунок 1. Как «работает» авторское право?

Автору гарантируется, что только он вправе определять, как и где он хотел бы использовать свое произведение. Это называется **неимущественные авторские права**. Любое незаконное использование авторских прав – как имущественных, так и неимущественных – должно пресекаться и наказываться, как в виде денежной компенсации, так и других санкций.

Так работает система авторского права в мире, так же работает она у нас, поскольку **Республика Казахстан ратифицировала основные международные документы** – Бернскую Конвенцию об охране литературных и художественных произведений<sup>23</sup>, Всемирную Конвенцию об авторском праве<sup>24</sup> и многие другие. Это означает, что казахстанские авторы могут защищать свои права по международным стандартам.

Основной закон, который регулирует права автора и все вопросы, связанные с авторскими правами в Казахстане, – **Закон РК «Об авторском праве и смежных правах»**<sup>25</sup>. Ниже в схеме указаны основные понятия – автор, объект авторского права, презумпция авторства, авторские неимущественные и имущественные права, исключительные и неисключительные имущественные права, авторский договор и три основных его элемента – (1) перечень прав, которые передаются по данному договору, (2) указание срока и территории и (3) размер авторского вознаграждения, сроки и порядок выплаты. Это **общее правило** концепции авторского права – автор должен получать вознаграждение за каждый случай использования его произведения. Однако **есть исключения из этого правила** – и они также указаны в данной схеме:

Бернская конвенция об охране литературных и художественных произведений не относит «новости дня» и «простую пресс-

<sup>23</sup> О присоединении Республики Казахстан к Бернской конвенции об охране литературных и художественных произведений. Закон Республики Казахстан от 10 ноября 1998 г., N 297. Текст закона доступен по ссылке: [https://adilet.zan.kz/rus/docs/Z980000297\\_](https://adilet.zan.kz/rus/docs/Z980000297_)

<sup>24</sup> О присоединении Республики Казахстан к Договору Всемирной организации интеллектуальной собственности по авторскому праву. Закон Республики Казахстан от 16 апреля 2004 года N 547. Текст закона доступен по ссылке: [https://adilet.zan.kz/rus/docs/Z040000547\\_](https://adilet.zan.kz/rus/docs/Z040000547_)

<sup>25</sup> Об авторском праве и смежных правах. Закон Республики Казахстан от 10 июня 1996 года № 6-І. Текст документа доступен по ссылке: [https://adilet.zan.kz/rus/docs/Z960000006\\_](https://adilet.zan.kz/rus/docs/Z960000006_)

информацию» к объектам авторского права<sup>26</sup>. Наш закон детализирует – «**сообщения о событиях и фактах, имеющие информационный характер, не относятся к объектам авторского права**»<sup>27</sup>. Означает ли это, что авторское право не имеет никакого отношения к СМИ, журналистами, фотографам и другим медиаспециалистам? Совсем нет. Напротив, связь между журналистикой и авторским правом – прямая и очевидная.

*Во-первых*, журналисты и фотографы тоже являются авторами. Как следует из вышеуказанных положений, только ленты новостей, новостные программы и сюжеты, краткие новости, пресс-релизы, пресс-анонсы, бегущая строка на телевидении с новостями, любая форма подачи только новостей, событий дня – это не объект защиты со стороны авторского права. Все остальное – **журналистские статьи, публикации, сюжеты, программы, фильмы, интервью, расследования, все журналистское творчество, творчество фотографов, операторов, звуко-режиссеров на телевидении, сценаристов и т.д. – это все защищается авторским правом.**

*Во-вторых*, средства массовой информации признаются **составными произведениями**<sup>28</sup>. Это значит, что журналисту и, например, фотографу как авторам текста и фотографий принадлежат личные неимущественные авторские права – это права на указание имя автора или псевдонима, право не подписывать свое произведение, если искажен его смысл и т.д. Журналист или фотограф, работающие по договору с редакцией, передают издателю или вещателю (или собственнику СМИ) свои авторские имущественные права – право на публикацию их текстов и фотографий за авторское вознаграждение (гонорар, заработная плата). Издателю, выпускающему в свет газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Издатель вправе при любом использовании таких изданий указывать свое наименование либо требовать такого указания<sup>29</sup>.

*В-третьих*, у авторов, сценаристов, операторов и других создателей аудиовизуальных материалов, работающих на телеканалах и радиостанциях, возникают смежные права. Аудиовизуальный материал считается составным произведением

<sup>26</sup> Пункт 8 статьи 2 Бернской конвенции об охране литературных и художественных произведений

<sup>27</sup> Подпункт 4 статьи 8 Закона РК «Об авторском праве и смежных правах»

<sup>28</sup> Пункт 2 статьи 11 Закона РК «Об авторском праве и смежных правах»

<sup>29</sup> Здесь же

и, соответственно, каждый имеет право на свою долю авторского вознаграждения. Все, кто работает на телевидении и радио, соответственно, также как журналисты в редакции газеты, передают свои имущественные права телеканалу или продакш-студии, получают взамен гонорар. Но личные немущественные права передать нельзя, поэтому мы всегда видим титры с фамилиями и именами всех, кто создавал какой-то аудиовизуальный продукт.

Авторские права журналистов и фотографов, как и других соавторов, могут нарушаться. Если вы увидели, что статья из вашего СМИ была перепечатана без разрешения и указания автора – это нарушение авторского права, автор не получил вознаграждение, не было согласия и т.д. Такое использование уже опубликованных текстов должно быть пресечено и денежная компенсация должна последовать.

### **Особенности использования авторских произведений в СМИ и в интернете (социальные сети, блоги)**

Является ли Интернет зоной, где не работают авторские права? Конечно, нет. Но Интернет способствует многократному увеличению информационного потока и скорости потребления информации, а, значит, риски нарушения авторских прав возрастают. Для того, чтобы предотвратить нарушения авторских прав, правообладатели публикуют **Правила пользования Интернет-ресурсом**<sup>30</sup> или **Правила использования материалов сайта**<sup>31</sup> или **Информация об ограничениях использования материалов**<sup>32</sup>, в которых устанавливают определенные ограничения как правообладатели. Это может быть указание допустимого объема цитирования (не больше 1/3 текста или первый абзац, например), условия воспроизведения текстов и фотографий из других источников, републикация комментариев и блогов и т.д. Несмотря на это, нарушение авторских прав со стороны СМИ довольно частое явление. Ниже представлены основные нарушения авторских прав уже со стороны редакций СМИ.

<sup>30</sup> Например, Правила пользования интернет-ресурсом Информбюро.kz

<sup>31</sup> Условия использования материалов, размещенных на медиа-портале Caravan.kz <https://www.caravan.kz/info/soglashenie-ob-ispolzovanii-376773>

<sup>32</sup> Например, Правила ограничения использования материалов новостного сайта Tengrinews.kz <https://tengrinews.kz/page/information/>



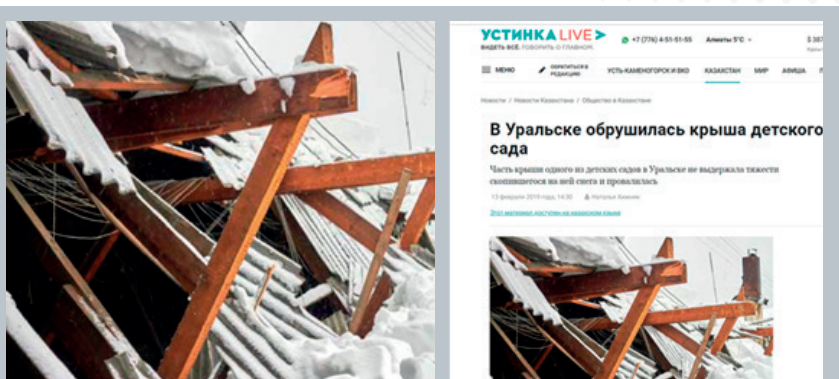
Рисунок 2.

*Классификация нарушений авторских прав со стороны редакций СМИ*

Незаконное использование фотографий из поисковых систем или других сайтов для иллюстраций текстов на сайтах СМИ и сетевых изданий - очень частое нарушение со стороны редакций СМИ. Контент-редакторы иллюстрируют тексты фотографиями, которые они находят в поисковых системах. И хотя поисковые системы предупреждают о необходимости соблюдения авторских прав, чаще всего эти предупреждения игнорируются. Если такая фотография опубликована без разрешения автора и без выплаты ему вознаграждения, а также без указания авторства, это является нарушением авторским прав, может последовать иск и требование о компенсации.

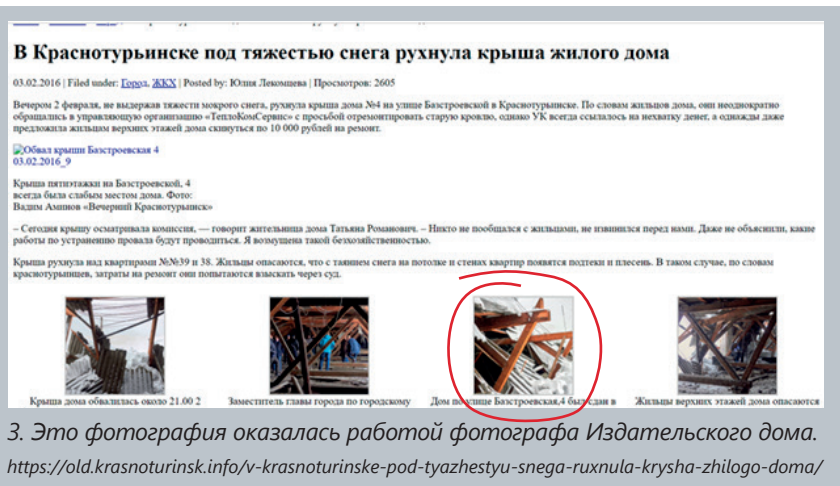
**ПРИМЕР 1.**

В одной из редакций проиллюстрировали материал такой фотографией, которую взяли из поисковой системы. При публикации фотографии не был указан автор, редакция не придавала никакого значения этому вопросу. После публикации редакция получила претензию и требование выплаты компенсации за незаконное использование фотографий без разрешения правообладателя, Издательского дома, который являлся правообладателем.



1. Эта фотография была найдена в интернете с помощью поиска

2. Это фото использовали для иллюстрации новости на сайте газеты



3. Это фотография оказалась работой фотографа Издательского дома.  
<https://old.krasnoturinsk.info/v-krasnoturinske-pod-tyazhestyu-snega-ruxnula-krysha-zhilogo-doma/>

**ПРИМЕР 2.**

Плагиат также недопустим в журналистике, в издательском деле, в академической среде. Некоторые редакции полностью используют тексты и фотографии других редакций, без получения какого-либо разрешения и указания авторов и первоисточников. Редакция информагентства, которая пострадала от плагиата со стороны другого СМИ, обратилась в суд за защитой свои нарушенных прав как правообладатель.



1. Материалы сайта KyzylordaNewz.kz, опубликованные 13.02.2020. Это полностью авторский контент журналиста и фотографа сайта



2. Этот текст и фотографии в одной из газет от 14.02.2020 года, полностью идентичны, только без указания авторов



3. Еще один образец плагиата, статья и фотография на сайте от 12.02.2020



4. Та же статья и фотография, идентичные на 100%, в газете от 14.02.2020 года, без указания авторов

Другие распространенные нарушения авторских прав в Интернете – это **использование текстов, фотографий, видео из открытых аккаунтов в социальных сетях без согласования с владельцем**. Несмотря на то, что это могут быть открытые аккаунты, ре-публикация такого контента в других СМИ требует получения разрешения владельца и указания первоисточника.

### **Как предотвратить нарушения авторских прав правообладателей со стороны редакций СМИ?**

Для того, чтобы предотвратить нарушения авторских прав со стороны редакций СМИ, можно порекомендовать следующие действия:



#### ***Для журналистов, фотографов, других медиаспециалистов как авторов текстов, фотографий***

- Всегда указывать в трудовом или ином договоре положения относительно авторских прав - указание имени или псевдонима, другой важной информации, например, может ли автор-журналист или фотограф распространять свои работы другим способом и т.д.
- Всегда отслеживайте факты незаконного использования ваших авторских текстов и фотографий, других материалов, и ставьте свою редакцию СМИ в известность об этом.



#### ***Для редакций СМИ и сетевых изданий, информагентств***

- Пользуйтесь услугами фотобанков или собственных фотографов, не используйте для иллюстрации фотографии из интернета. То же самое касается текстов и аудиовизуальных материалов.
- Помните про возможности цитирования, иллюстраций и публикаций обзоров и дайджестов, если необходимо использовать уже опубликованные тексты, фотографии или аудиовизуальные материалы
- Обновите свои правила использования материалов сайта или сетевого издания для того, чтобы избежать нарушения ваших прав как правообладателей



#### ***Тексты, фото и другие материалы из социальных сетей и других источников в Интернете***

- Разработайте алгоритм действий в случаях использования текстов, фото, аудио и видео из открытых аккаунтов в социальных сетях
- Обязательно необходимо получать разрешение авторов этих материалов на републикацию, указывать первоисточник и давать гиперссылку на него
- Откажитесь от публикации контента или замените его, если это правило (указано выше) выполнить невозможно

На практике журналист и редакция СМИ может столкнуться со смежными проблемами, например, претензиями на нарушение право на собственное изображение или нарушением оборота персональных данных и т.д. Здесь необходимо четко разграничить, как и почему авторские права в журналистике отличаются от других прав и как предусмотреть защиту авторских прав как для самих журналистов, фотографов прессы и других медиаспециалистов, и одновременно – предупредить нарушение авторских прав других лиц со стороны редакций СМИ.

## ГЛОССАРИЙ

**Автор** - Любой человек, кто создал уникальное и оригинальное произведение – письменное, устное, в других формах, в различных сферах – литература, музыка, искусство и т.д.

**Объект авторского права** - Само произведение, уникальное и оригинальное, которое имеет своего автора или соавторов – книги, энциклопедии, газеты и журналы, скульптуры и картины, телепрограммы, фильмы, музыкальные произведения и т.д.

**Презумпция авторства** - Правовое положение, которое закреплено в международных стандартах и законе – возникновение авторства базируется на факте создания произведения.

**Знак копирайта @** - Регистрация и иные разрешения автору не нужны, для того, чтобы начать реализацию своих авторских прав. Факт авторства подтверждается знаком @, однако если его нет – это не означает, что у произведения нет автора.

**Срок охраны авторских прав** - Авторские права охраняются законом в течение всей жизни автора и после его смерти в течение 50-70 лет (в Казахстане 70 лет) эти права реализуются через наследников. После истечения этого срока произведение признается общественным достоянием.

**Авторские права** - Возможности для автора или соавторов распространять свое произведение и получать доход. Категории прав:

- **личные неимущественные права** авторов (право на имя, право публиковать свою работу под псевдонимом и т.д.)
- **имущественные права авторов** (используются для получения дохода от распространения своего произведения право

производить и распространять, публично показывать произведение, право на переработку произведения, право на перевод и т.д.)

Имущественные права, в свою очередь, могут быть исключительные (возможность использования произведения только одним правообладателем) и неисключительными (несколько правообладателей могут использовать произведение одновременно)

**Правообладатель** - Автор или лицо, которому временно, по авторскому договору, переданы имущественные авторские права на использование, распространение и т.д. произведения

**Авторский договор** - Письменный договор автора с другим лицом или лицами, которому или которым автор уступает авторские права получать доход от своего произведения на определенных условиях. В договоре обязательно указываются – срок и территория действия, какие именно права передаются и за какое вознаграждение и как оно будет уплачиваться.

**Смежные права** - Возникают у исполнителя, производителя фонограммы, сотрудников организации эфирного и кабельного вещания и т.д.

## ПОЛЕЗНЫЕ ССЫЛКИ

1. **WIPO** – Всемирная организация интеллектуальной собственности (ВОИС), была учреждена в 1967 году. Сейчас это - глобальный форум, занимающийся вопросами политики, укрепления сотрудничества, предоставления услуг и информации в области интеллектуальной собственности. ВОИС является самофинансируемым учреждением системы Организации Объединенных Наций и насчитывает 193 государства-члена. Официальный сайт организации <https://www.wipo.int/about-wipo/ru/>
2. **Бернская конвенция по охране литературных и художественных произведений** (1886 год), с изменениями от 28 сентября 1979 г, на русском языке <https://wipolex.wipo.int/ru/text/283697>
3. **Всемирная конвенция об авторском праве** от 6 сентября 1952 г, на английской языке <https://wipolex.wipo.int/ru/text/172836>

4. Пекинский договор по аудиовизуальным исполнениям (2012 год), на русском языке <https://wipolex.wipo.int/ru/text/295841>
5. Закон Республики Казахстан от 10 июня 1996 года № 6-І «Об авторском праве и смежных правах». [https://adilet.zan.kz/rus/docs/Z960000006\\_](https://adilet.zan.kz/rus/docs/Z960000006_)
6. Закон Республики Казахстан от 23 июля 1999 года № 451-І «О средствах массовой информации» [https://adilet.zan.kz/rus/docs/Z990000451\\_](https://adilet.zan.kz/rus/docs/Z990000451_)
7. Закон Республики Казахстан от 18 января 2012 года № 545-ІV «О телерадиовещании» <https://adilet.zan.kz/rus/docs/Z1200000545>
8. Подборка судебных дел по защите интеллектуальной собственности (российская практика) <http://mediapravo.org/materials/problems> Тема №2. Интеллектуальная собственность

### Творческое задание

Студенты должны найти и проанализировать Правила использования материалов (или другие аналогичные документы) пяти (или десяти) крупнейших новостных порталов Казахстана и составить общую таблицу, в которой были бы отражены следующие критерии:

1. Название документа и гиперссылка
2. Кто является правообладателем, название
3. Какие ограничения установлены для использования текстов этого сайта?
4. Какие ограничения установлены для использования фотографий и других изображений?
5. Какие ограничения установлены для использования аудиовизуальных материалов, графики?
6. Дополнительные ограничения по использованию авторских прав

# ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ



*Дана Мухамеджанова*

## ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Несмотря на то, что универсального определения права на неприкосновенность частной жизни не существует, можно отметить множество попыток ученых, судей и практиков данной области сформулировать и дать исчерпывающее определение данной категории прав человека.

При формировании концепции неприкосновенности и уважении частной жизни в первую очередь подчеркивалась важность жилища, частной собственности, тайны переписки, телесной неприкосновенности и семейных тайнах, изъятиях и обысков<sup>33</sup>. Однако несмотря на то, что право на частную жизнь предусматривает некоторый информационный контроль, не все вопросы информационного контроля относятся к приватности отдельных лиц<sup>34</sup>. Далее акцент сместился на защиту права на неприкосновенность частной жизни в общественных местах, определения границ вторжения от государства.<sup>35</sup> Сфера охвата границ и пределов вторжения либо ограничения приватности имеет значительную разницу в различных конституционных системах зарубежных государств.

Право на неприкосновенность частной жизни носит в себе позитивный и негативный характер. Негативные обязательства влекут за собой защиту отдельных лиц от нежелательного вмешательства в личную жизнь как со стороны государства, так и со стороны частных лиц. Позитивное обязательство права на неприкосновенность частной жизни влечет за собой обязательство государств обеспечить необходимую и адекватную защиту неприкосновенности частной жизни, устранить

<sup>33</sup> Schulhofer S. J. Fifth Amendment at Justice: A Reply // University of Chicago Law Review. 1987. (54). С. 950.

<sup>34</sup> Hert P. J. A. de, Gutwirth S. Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action // Reinventing data protection? 2009. С. 3–45.

<sup>35</sup> Nowak J. E., Rotunda R. D., Young J. N. Constitutional Law / J. E. Nowak, R. D. Rotunda, J. N. Young, West, 1986.

препятствия для автономного формирования индивидуальной свободы<sup>36</sup>.

Подчеркивая важность частной жизни, следует отметить, что в разное время и в различных обществах всегда было стремление к приватности, об этом свидетельствуют такие природные инстинкты как человека, так и животных, на территориальное отделение и собственное пространство для уединения. Для кого-то приватность является неким психологическим состоянием, состоянием возможности изоляции от других, нежеланием делиться чем-то личным, либо сокрытие каких-то отношений, таинство информации для небольшого круга людей, например, только семьи. Также это выражено контролем над информацией о самом себе или способностью индивида передавать ровно ту часть информации о себе, которой он готов поделиться, возможностью знать о тайне своего происхождения, ознакомиться с личными делами того, кому они принадлежат, получать доступ к ним. Существует также мнение авторов о частной жизни, которое определяет «требование отдельных лиц, групп или учреждений самим определять, когда, как и в какой степени информация о них будет передана другим».<sup>37</sup>

Несмотря на сложность определения понятия неприкосновенности частной жизни для наилучшего понимания, следует выделить наиболее распространенные виды концепций приватности:

- Право быть оставленным в покое,
- Приватность как индивидуальная автономия,
- Ограниченный доступ к информации о себе,
- Секретность,
- Минимизация бремени,
- Контроль над личной информацией.<sup>38</sup>

<sup>36</sup> How far may Colombia's Constitutional Court go to protect IDP rights? | Forced Migration Review // [www.fmreview.org](http://www.fmreview.org) [Электронный ресурс]. URL: <https://www.fmreview.org/brookings/cepedaespinoza> (дата обращения: 13.07.2021).

<sup>37</sup> Irwin R., Kramer . The Birth of Privacy Law: A Century Since Warren and Brandeis. 1990. С.

<sup>38</sup> Reynolds O. M., Westin A. F. Review of PRIVACY AND FREEDOM // Administrative Law Review. 1969. № 1 (22). С. 101–106.

Алан Вестин упоминал еще в 1967 году о рисках технологического развития для частной жизни, возможности следить не только за активностью, но и за мыслями при помощи прослушивающих устройств, записи телефонных разговоров, полиграфических тестов и др.<sup>39</sup>

Сотни миллионов людей ежедневно посещают большое количество интернет - сайтов, предоставляют персональную информацию в государственные институты, совершают сделки и выполняют иные действия, при которых используются или затрагиваются их персональные данные, и зачастую не задумываясь о том, что происходит с данными в последующем.

Наиболее важным положением в области прав человека является Всеобщая декларация прав человека. В статье 12 установлено: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств», что закрепляет право человека на приватность его частной жизни и подразумеваемое право на защиту от посягательств на персональные данные.

В свою очередь право на неприкосновенность частной жизни определено в статье 17 Международного пакта о гражданских и политических правах, который также является одним из важнейших международных документов обеспечения и защиты прав человека. Однако несмотря на наличие правового регулирования сферы персональных данных как на международном, так и на национальных уровнях и внедрения новых механизмов защиты персональных данных (развития кибербезопасности), на практике все же имеют место утечки, перепродажа, использование персональных данных и иные действия злоумышленников, совершаемые в противоправных целях. При этом многие владельцы персональных данных часто не подозревают о совершении правонарушений с использованием их персональных данных, так как базы хранения таких данных не обеспечиваются достаточной киберзащитой от посягательств третьих лиц, соответственно, не обладают возможностями своевременно и оперативно реагировать на атаки со стороны.

<sup>39</sup> См. там же, стр. 101.

Более того, в силу трансграничности и анонимности совершаемых правонарушений с использованием персональных данных, наличия сложностей в определении местонахождения субъекта, в оценке реального объема ущерба, нанесенного в результате совершенного правонарушения, подобные посягательства остаются за пределами правовой ответственности.

Остановимся на некоторых концепциях частной жизни, которые могут дать более развернутое понятие приватности, несмотря на ограниченность его определения и закрепления в юридической терминологии:

### **Право быть оставленным в покое<sup>40</sup>**

Первая успешная попытка сформулировать сущность понятия частной жизни была сделана знаменитыми американскими авторами, адвокатом Самюэлем Уорреном и судьей Верховного Суда Луисом Д. Брандэйсом в 1890 году в журнале «Harvard Law Review»<sup>41</sup>. Статья, изданная в прошлом веке, не потеряла свою актуальность и сегодня, наоборот, огромное количество научных трудов, изданий базируется на идеях классификации категории приватности как «права быть оставленным в покое», «the right to be alone».

Критический подход к приватности представил Джон Милс (John L. Mills). Он указал, что повсеместный сбор данных создает возможность наблюдения за гражданами в условиях тоталитарного режима, в котором зафиксированы любые действия, предпочтения, привычки, сформированные на основании анализа данных и алгоритмов искусственного интеллекта, изучение системы поисковиков, запросов, взаимодействий с другими пользователями. В последующем предоставляется возможность предсказывать и влиять на мнение и настроение людей. Различие между частной и общественной сферами может быть уничтожено, так как десятки умных устройств регистрируют активность в домах или автомобилях и подключаются к корпоративным или государственным

<sup>40</sup> Cooley T. M., Haggard D. A. A treatise on the law of torts or the wrongs which arise independently of contract // Berkeley Law [Электронный ресурс]. URL: <https://lawcat.berkeley.edu/record/388726?ln=en> (дата обращения: 16.07.2021).

<sup>41</sup> Vol. 4, No. 5, Dec. 15, 1890 of Harvard Law Review on JSTOR // [www.jstor.org](http://www.jstor.org) [Электронный ресурс]. URL: <https://www.jstor.org/stable/i256795> (дата обращения: 16.07.2021).

компьютерам в любом месте. Для предотвращения подобных сценариев потребуются важные гарантии конфиденциальности. Дэвид Коль (David Cole) рассматривает процесс наблюдения за гражданами как правительственными органами, так и частными субъектами. Он сравнивает эффект наблюдения с попыткой установить социальный контроль над обществом и средством манипуляций.

### **Телесная целостность**

Сфера телесной приватности, включает в себя приватность:

- 1) тела;**
- 2) ума;**
- 3) дома;**
- 4) интимного поведения;**
- 5) тайны переписки;**
- 6) семейной жизни.**

Примечательно дело бывшего Президента Франции Франсуа Миттерана. После его смерти в книге "Большой секрет" ("Le Grand Secret") доктор Гюблер поделился с общественностью информацией о заболевании, а именно раке простаты покойного Миттерана. В книге содержатся сведения о состоянии здоровья, которая, по мнению семьи экс-президента, составляла профессиональную врачебную тайну и подробности борьбы с болезнью. Уголовный суд Парижа признал нарушение профессиональной тайны, запрет на распространение книги, а также назначил сумму возмещение ущерба.

По части обращения семьи экс-президента о нарушении ст. 8 ЕКПЧ, включающей разглашение сведений о его частной жизни после смерти суд ЕСПЧ подсчитал, что описанное состояние здоровья и подробности лечения не представляют собой вмешательство в частную жизнь Миттерана, потому как претендовать на защиту он мог только будучи живым.<sup>42</sup> В таких случаях возникло немало спорных моментов, потому что в случае смерти лица право защищать частную жизнь передается его близким родственникам.

<sup>42</sup> Компания «Плон» против Франции. Editions Plon v. France | Global Health & Human Rights Database [Электронный ресурс]. URL: <https://www.globalhealthrights.org/plon-societe-v-france/>

Более того, право на неприкосновенность частной жизни существует даже тогда, когда человек находится в публичном пространстве, как это было в деле Пэк против Великобритании (Peck v United Kingdom). Пэк, решивший свести счеты с жизнью в общественном месте, достав нож, пытался перерезать себе вены, тем самым попал в объективы камер видеонаблюдения. В последующем акт суицида удалось предотвратить правоохранительным органам, однако запечатленный видеоматериал был передан для публикации телеканалам Великобритании в качестве статистики предотвращения преступлений и для поддержания общественного порядка при помощи видеонаблюдения. В последующем Пэк был вынужден обратиться в ЕСПЧ по части нарушения статьи 8 о защите своей частной жизни. В решении суда была отмечена важность поддержания общественного порядка, однако СМИ и телевизионным каналам было необходимо принять меры, соответствующие принципам необходимости и пропорциональности, а именно при публикации материала, представляющего общественный интерес, замаскировать лицо гражданина так, чтобы его невозможно было идентифицировать и распознать по каким-либо характеристикам<sup>43</sup>.

Другими аспектами жизни человека, которые считаются частью частной жизни, являются, например, личная идентичность, включая имя, сексуальные действия, религию, этническую идентичность (RB v Hungary), а также сбор и использование персональных данных государством (Захаров против России), включая медицинские записи.

### **Личная автономия и идентификация личности**

Во многих демократических обществах существует фундаментальная вера в уникальность личности, поощрение достоинства и ценности человека (Westin 1967, стр. 33)<sup>44</sup>. Чтобы защитить личную автономию и чувство человеческого достоинства<sup>45</sup>, необходимо иметь личное пространство, свободное от вмешательства извне. Также это означает право

---

<sup>43</sup>

<sup>44</sup> См. 7. Стр. 33

<sup>45</sup> D. Kretzmer and E. Klein The Concept of Human Dignity in Human Rights Discourse Brill Nijhoff, 2002. <http://www.gbv.de/dms/spk/sbb/toc/345530985.pdf>

личности на самоопределение<sup>46</sup>, возможность быть наедине со своими мыслями и чувствами. Концепция защиты приватности также имеет значение в юридической терминологии как «право на информационное самоопределение» («informationelle Selbstbestimmung»), провозглашенное Конституционным судом Германии (Bundesverfassungsgericht)<sup>47</sup> в его исторически важном решении о переписи населения<sup>48</sup>. В декабре 1983 года Федеральный конституционный суд Германии объявил неконституционными некоторые положения Закона о переписи населения (Volkszählungsurteil). Суд постановил, что основное право гарантирует: «...способность физического лица определять раскрытие и использование его персональных данных»<sup>49</sup>.

Это было одна из первых и наиболее известных формулировок «права на информационное самоопределение», понимаемого Судом как «полномочия индивида решать самостоятельно, исходя из идеи самоопределения, в каких пределах информация о его частной жизни может быть доступна для сведения других, и индивид волен самостоятельно решать в какой степени он будет раскрывать аспекты своей личной жизни»<sup>50</sup>.

### Информационная приватность

Информационная приватность также включает персональные данные и тайну корреспонденции. Важность персональных данных как аспекта частной сферы является прямым результатом быстрого распространения цифровых технологий.

<sup>46</sup> Jacoby N. GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW VOLUME 35 2007 NUMBER 3 REDEFINING THE RIGHT TO BE LET ALONE: PRIVACY RIGHTS AND THE CONSTITUTIONALITY OF TECHNICAL SURVEILLANCE MEASURES IN GERMANY AND THE UNITED STATES. С. 467-468.

<sup>47</sup> Bundesverfassungsgericht 1 S. Bundesverfassungsgericht - Decisions - Decision on the constitutionality of the 1983 Census Act // [www.bundesverfassungsgericht.de](http://www.bundesverfassungsgericht.de) [Электронный ресурс]. URL: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215\\_1bvr020983en.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html), 68-69 (дата обращения: 15.07.2021).

<sup>48</sup> Rouvroy A., Pouillet Y. The Right to and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy // Reinventing Data Protection? 2009. С. 45–76.

<sup>49</sup> Там же. См. 12, 68-69

<sup>50</sup> Там же. См. 12, 68-69

21 мая 2013 года в Казахстане был принят Закон «О персональных данных и их защите». Главной целью закона является «обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных», однако необходимо отметить, что положение, касающееся накопления о хранении персональных данных, был внесено законодателем только 2 января 2021 года.

Компетенция уполномоченных органов в сфере защиты персональных данных закреплена в статье 27 Закона. Потому как защита персональных данных в Казахстане связана непосредственно с общей политикой, которая касается обеспечения безопасности сохранения режима, а также с наиболее серьезными проблемами, связанными с борьбой с терроризмом, религиозным экстремизмом.

Общий регламент защиты персональных данных (GDPR) Европейского союза определяет персональные данные как «любую информацию, относящуюся к идентифицированным или идентифицируемым физическим лицам, которые могут быть идентифицированы прямо или косвенно, в частности, посредством ссылки на идентификационный номер или один или несколько факторов, специфичных для их физических, психологических, генетических, психических, экономических, культурных, культурных и культурных или социальная идентичность».

### **Минимизация вреда**

Данная концепция приватности рассматривается как средство минимизации бремени нарушения. Потому как частная жизнь зачастую нарушается из-за вторжения извне. В случае если нарушения будут иметь системный характер, они вполне могут стать бременем, в особенности если повторяющийся характер наносит определенный урон или ущерб. Поэтому вторжения в нашу частную жизнь должны быть сведены к минимуму.

Право на неприкосновенность частной жизни предоставляет нам средства для защиты от этих нежелательных, обременительных вторжений. Примером, иллюстрирующим эту концепцию конфиденциальности, является нежелательная коммерческая электронная почта или «спам». Как в Нидерландах, так и в Соединенных Штатах, законодательство о конфиденциальности используется для защиты отдельных лиц от нежелательной коммерческой электронной почты.

## Цифровая приватность

Остановившаяся на последней, можно отметить, что интернет и цифровые технологии поспособствовали проявлению права на неприкосновенность частной жизни в новом ключе после разоблачений Эдварда Сноудена<sup>51</sup> и принято ряда резолюций Генеральной Ассамблеи и Совета по правам человека ООН 68/167, 69/166, 71/199, 28/16 и 34/7 от 23 марта 2017 года о праве на неприкосновенность частной жизни в цифровую эпоху<sup>52</sup>. Формат наблюдения, выявленный Сноуденом, определял целенаправленное, одновременно нецелесообразное вмешательство в приватность, включающее массовый сбор, хранение данных цифровых коммуникаций и метаданных.

Очевидно, что вопросы массовой слежки, сбора данных и применения цифрового наблюдения будут по-прежнему вызывать серьезную озабоченность, так как развитие цифровых технологий создает новые проблемы использования камер с функцией распознавания лиц, цифрового наблюдения, искусственного интеллекта, анализа больших данных и трансграничного потока передачи данных, распознавания речи и др.

В дополнение к росту электронных баз данных и информации, технологии становятся все более проникающими в связи с увеличением наблюдения в стиле Большого Брата за рабочими местами, частной собственностью, образовательными учреждениями, торговыми центрами, улицами и другими общественными местами.

Расширение частных компаний, корпораций приводит к увеличению рабочих мест, однако работники стали все чаще подвергаться контролю и мониторингу со стороны работодателей. Сторонники мониторинга утверждают, что использование систем видеонаблюдения и мониторинга учета действий сотрудника на рабочем месте предполагает эффективные средства контроля за качеством выполнения обязательств работников, способствуя тем самым увеличению производства и снижению

<sup>51</sup> Факт обнаружения иностранной цифровой слежки при помощи программ, выявленная Эдвардом Сноуденом бывшим агентом Агентства национальной безопасности США (АНБ).

<sup>52</sup> Резолюции Генеральной Ассамблеи и Совета по правам человека ООН о праве на неприкосновенность частной жизни в цифровую эпоху // Un.org [Электронный ресурс]. URL: [https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/CONF.157/24%20\(Pa&Lang=R](https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/CONF.157/24%20(Pa&Lang=R) (дата обращения: 15.07.2021).

трудозатрат. Работодатели не ограничены в получении доступа к корпоративной почте, а зачастую и частной электронной почте своих сотрудников, телекоммуникации, телефонные звонки, голосовая почта, истории поисковых запросов, просмотр веб-страниц и компьютерных файлов, которые хранятся в информационных системах компании также находятся в доступе.

## ГЛОССАРИЙ

**Информационная эра** - (англ. Information Age, также известная как эра компьютеров или информационная эпоха (электронная эпоха)) — концептуальная идея о том, что современный век будет характеризоваться широкими возможностями для отдельных лиц свободно передавать/принимать информацию, а также мгновенным доступом как к освоенным знаниям, так и к любой информации о планах, поставленных человечеством, что было бы трудно или невозможно в предыдущие эпохи развития человечества<sup>53</sup>.

**Информационно-коммуникационная технология** - совокупность методов, производственных процессов, программно-технических и лингвистических средств, интегрируемых с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей<sup>54</sup>.

**Цифровое наблюдение** – охватывает мониторинг, перехват, сбор, получение, анализ, использование, хранение, защиту, вмешательство, доступ или иные действия с информацией, которая включает, отражает, возникает из или рассказывает о коммуникациях человека в прошлом, настоящем или будущем<sup>55</sup>.

**Информационная безопасность** – защищенность информации от возможных угроз, направленных на нарушение ее конфиденциальности, целостности, доступности или на ее умышленное искажение. Система мер, методов и средств

<sup>53</sup> Джесси Рассел «Информационная эра». Интернет-источник: <http://dic.academic.ru/dic.nsf/ruwiki/1506872/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F>

<sup>54</sup> Глоссарий по информационному обществу / Под общ.ред. Ю.Е. Хохлова. — М.: Институт развития информационного общества, 2009. 61 с. — 160 с. Интернет ресурс: <http://www.iis.ru/docs/is.glossary.2009.pdf>

<sup>55</sup> См. там же

правового, организационного и технологического характера, обеспечивающих предотвращение умышленного или случайного нарушения конфиденциальности, целостности, доступности и искажения информации<sup>56</sup>.

**Неприкосновенность частной жизни** — (в юр. науке) ценность, обеспечиваемая правом на неприкосновенность частной жизни.

Право на неприкосновенность частной жизни включает:

- запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия;
- право контролировать информацию о себе;
- право на защиту чести и доброго имени;
- право на защиту персональных данных;
- право на тайну связи;
- право на неприкосновенность жилища;
- врачебную тайну, тайну усыновления, тайну исповеди и другие виды профессиональной тайны<sup>57</sup>.

**Конфиденциальность** - это комплекс мер по предотвращению утечки и разглашения той или иной информации. Сущность данного понятия также можно уяснить, ознакомившись с его переводом с разных языков. Это звучит примерно, как "тайна" или "доверие". Конфиденциальность можно считать необходимым условием для многих видов деятельности, среди которых медицинская, адвокатская, аудиторская и прочие<sup>58</sup>.

<sup>56</sup> См. там же

<sup>57</sup> Интернет-источник: <http://dic.academic.ru/dic.nsf/ruwiki/89877>

<sup>58</sup> Интернет-источник: BusinessMan.ru: <https://businessman.ru/new-konfidencialnost-eto-opredelenie-regulirovanie-oxrana-konfidencialnoj-informacii.html>

### Творческое задание

Ник Томилиан вел активную электронную переписку с близкими людьми посредством Messenger Microsoft Outlook, просматривал фильмы в рабочее время. При проведении дисциплинарного разбирательства Суды Италии установили, что использование заявителем сети Интернет в личных целях на рабочем месте является нарушением, в частности, принималось во внимание обстоятельство, что работодатель предварительно оценил содержание официальной корпоративной почтовой переписки сотрудника, а также личной переписки в Messenger Microsoft Outlook.

По обстоятельствам данного дела сотруднику было известно об установленной политике мониторинга переписки сотрудников и нецелевого использования интернет трафика.

На дисциплинарной комиссии было установлено, что использование ресурсов компании, предназначенных для использования в рабочих целях, является основанием для увольнения сотрудника. Также руководство компании подтверждает, что данный сотрудник и другие сотрудники компании неоднократно были уведовлены о политике мониторинга и контроля за электронными сообщениями компании.

Заявитель обжаловал свое увольнение в Суд. По утверждению заявителя Ника Томилиана, его увольнение было незаконным, на основании нарушения его права на уважение частной жизни. Заявитель утверждает, что внутригосударственные суды не выполнили своего обязательства по защите права на уважение личной жизни и тайны корреспонденции. В своем обращении он потребовал в суде принять решение об отмене незаконного увольнения и обязать работодателя восстановить его в должности, осуществить выплату компенсации в размере 40 000 евро за причиненный моральный и материальный вред, а также возместить судебные расходы и издержки. В рамках творческого задания необходимо выступить в виде модельного заседания

Европейского суда по правам человека (ЕСПЧ) в следующем порядке:

***A. Обстоятельства дела, позиция заявителей,***

***B. Материально-правовые аспекты,***

***C. Процессуальные аспекты,***

***D. Выводы и решение ЕСПЧ,***

***E. Практика ЕСПЧ.***

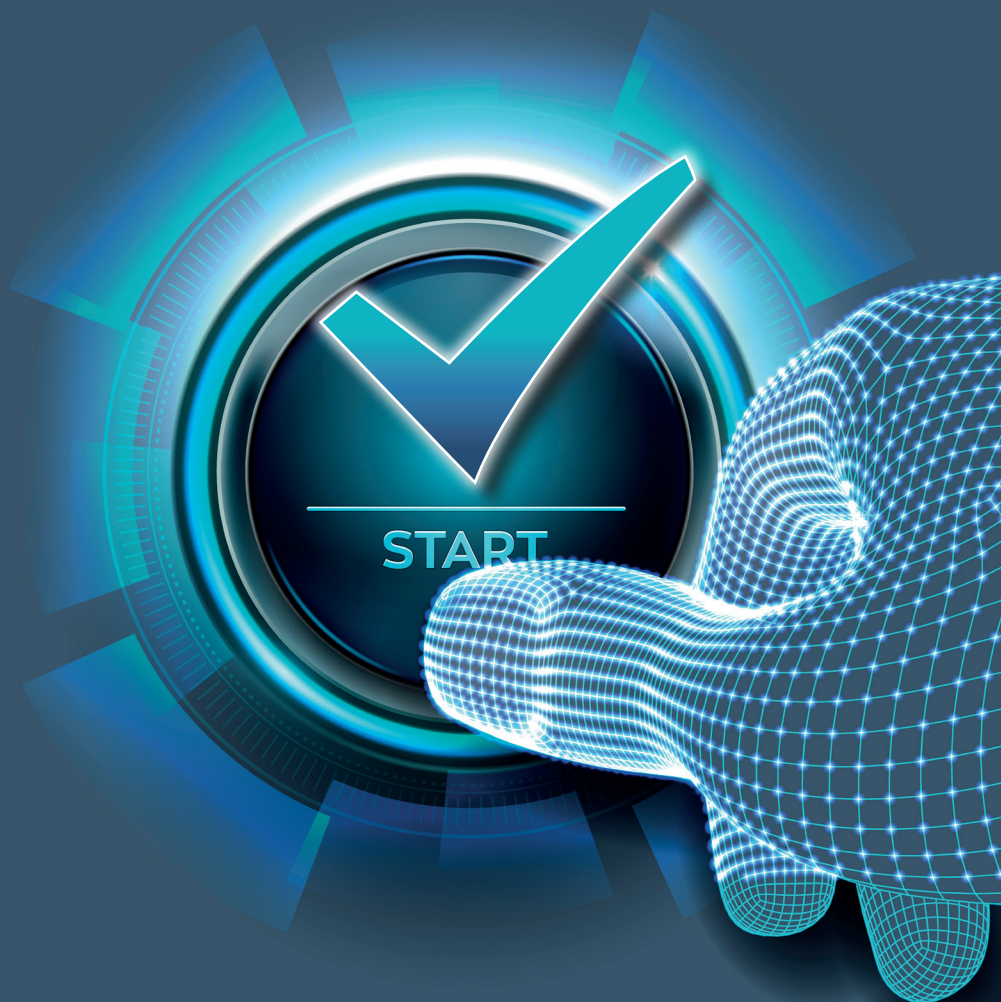
По итогам выступления сделать аналитический вывод, обоснованность принятого решения.

При решении задачи обязательно подкреплять свои доводы анализом других судебных решений ЕСПЧ (2-3 решения для сравнения).

Обратите внимание на подходы принятия решений судом, для своей работы используйте ключевые параметры пределов допустимости вмешательства со стороны государство или частного представителя, как варьировалась планка требований, исходя из теста проверки на "законность", "необходимость в демократическом обществе" и "пропорциональности".

Дополнительная информация для изучения: Интернет: прецедентная практика Европейского Суда по правам человека, далее по ссылке: [https://www.echr.coe.int/Documents/Research\\_report\\_Internet\\_RUS.pdf](https://www.echr.coe.int/Documents/Research_report_Internet_RUS.pdf)

# ЭЛЕКТРОННОЕ УЧАСТИЕ



*Данила Бектурганов*

## ЭЛЕКТРОННОЕ УЧАСТИЕ

### Определение и цели электронного участия

Электронное участие (E-Participation) – специфическая и относительно «молодая» форма общественного и политического участия граждан в делах государства. Можно утверждать, что Электронное участие – это традиционное политическое участие, то есть деятельность граждан, направленная на оказание влияния на процесс принятия решений и их осуществление, только реализуемая в цифровом пространстве с помощью информационных и коммуникационных технологий (ИКТ). Важно, что это добровольная деятельность обычных граждан, не связанных с официальным осуществлением политических или управленческих функций.

Исторически первым концептом взаимодействия государства и граждан в цифровой среде была концепция Электронного правительства<sup>59</sup> (e-Government). Бурное развитие интернета в 90-х годах, когда появились технологии высокоскоростного обмена данными и стала доступна соответствующая инфраструктура, сделало возможным перенос части функций государственных органов в электронную среду. На том этапе не планировалось никакого другого функционала, кроме предоставления государственных услуг онлайн – выдача разнообразных электронных документов и справок.

Появившаяся позднее – в 2000-х – концепция Электронного управления (e-Governance) уже предполагала активное участие граждан в управлении и развивала методы учета мнения граждан при принятии решений. Появившаяся в середине 2000-х концепция Электронного участия (e-Participation) является частью Электронного управления; более того, методы и технологии Электронного участия являются необходимым «механизмом» (или экосистемой) обеспечения реализации Электронного управления.

<sup>59</sup> Сравнительный анализ электронного правительства <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/English.pdf>

В этом контексте технологии и сервисы Электронного правительства играют уже вспомогательную роль, то есть роль базовой информационно-технологической платформы. Одним из наиболее показательных примеров реализации экосистемы Электронного управления является опыт Эстонской Республики (законодательная база и единая инфраструктура X-Road<sup>60</sup>, обеспечивающая межведомственное и межуровневое взаимодействие, в том числе с ресурсами Электронного участия)<sup>61</sup>. Эстонская Республика в настоящее время находится на лидирующей позиции в деле построения Электронной демократии (e-Democracy).

В документах ООН под электронным участием понимают «процесс вовлечения граждан в политику, принятие решений, разработку и оказание услуг в целях обеспечения участия, инклюзивности и целенаправленности, при помощи информационных и коммуникационных технологий»<sup>62</sup>. Определение участия как процесса наиболее полно отражает суть, поскольку реализация этого процесса требует, как «права на доступ к сети интернет», то есть доступности среды, в которой осуществляется электронное участие, так и «права на доступ к информации», которое подразумевает наличие в публичном доступе информации, позволяющей реализовать электронное участие; немаловажно и наличие нормативно-правовой базы, которая делает электронное участие легитимным. В документах ООН цель электронного участия определяется в «улучшении доступа к информации и общественным услугам, а также содействии в выработке политик для расширения прав и возможностей отдельных граждан и общества в целом»<sup>63</sup>.

Очевидно, что в прикладных целях более удобно определять электронное участие как «комплекс методов и инструментов, обеспечивающих электронное взаимодействие граждан и органов власти с целью учета мнения граждан в государственном и местном управлении при принятии политических решений, включая реагирование на обращения граждан по широкому кругу

<sup>60</sup> X-Road introduction (English) <https://www.youtube.com/watch?v=9PaHinkJlvA&t=35s>

<sup>61</sup> E-Estonia website <https://e-estonia.com/solutions/interoperability-services/x-road/>

<sup>62</sup> Обзор ООН по электронному правительству 2020 г. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>

<sup>63</sup> Департамент по экономическим и социальным вопросам ООН <https://publicadministration.un.org/ru/eparticipation>

проблем»<sup>64</sup>. Определение электронного участия на казахстанском портале электронного правительства: «Электронное участие – это процесс вовлечения граждан в политику, принятие решений, и разработку и предоставление услуг с помощью информационно-коммуникационных технологий».<sup>65</sup> Казахстан, как и многие другие страны, совершенствует национальный портал электронного правительства и увеличивает количество государственных услуг и сервисов, доступных онлайн.

### Законодательные основания

В настоящее время нет общепринятых международных стандартов, которые могли бы однозначно указывать на необходимость всем странам придерживаться общих правил при внедрении Электронной демократии. Однако из уже имеющихся документов можно извлечь основные принципы, на которых должно строиться электронное участие граждан в управлении государством.

- Конвенция о защите прав человека и основных свобод<sup>66</sup>, п.10, декларирует «Право каждого человека свободно выражать и придерживаться своего мнения, а также распространять информацию и идеи...»;
- МПГПП<sup>67</sup> в ст. 19 декларирует, что «Каждый человек имеет право беспрепятственно придерживаться своих мнений... имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию...»;
- МПГПП в ст. 25 декларирует, что «Каждый гражданин должен иметь... право и возможность... принимать участие в ведении государственных дел...»;
- МПЭСКП<sup>68</sup> в ст. 15 декларирует, что «Государства признают право каждого человека на пользование результатами научного прогресса и их практического применения»;

<sup>64</sup> Чугунов А.В. «Электронное участие в контексте трансформации концепции демократии», 2017 <https://www.acjournal.ru/jour/article/view/631/632>

<sup>65</sup> Электронное участие на портале eGov <https://egov.kz/cms/ru/eparticipation>

<sup>66</sup> Конвенция о защите прав человека <http://hrlibrary.umn.edu/russian/euro/Rz17euroco.html>

<sup>67</sup> МПГПП [https://www.un.org/ru/documents/decl\\_conv/conventions/pactpol.shtml](https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml)

<sup>68</sup> МПЭСКП [https://www.un.org/ru/documents/decl\\_conv/conventions/pactecon.shtml](https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml)

- Конвенция ООН об использовании электронных сообщений в международных договорах<sup>69</sup> в ст. 8 признает юридическую силу электронных сообщений. Поскольку Конституция РК в ст. 4 признает примат международного права, норма о юридической силе электронных сообщений распространяется и на казахстанскую юрисдикцию;
- В 2016 году Совет ООН по правам человека впервые принял резолюцию<sup>70</sup>, посвященную свободе слова в интернете, в которой, в том числе, подтверждает, что те же права, которые человек имеет в офлайн среде, должны также защищаться и в онлайн среде, в частности право на свободу выражения мнений.
- В национальном законодательстве РК есть несколько основных нормативно-правовых актов (НПА), которые позволяют реализовать электронное участие:
- Закон Республики Казахстан от 16 ноября 2015 № 401-V «О доступе к информации»<sup>71</sup>, ст. 10, содержит одно из определений доступа к информации как «доступ к информации, размещенной на соответствующих компонентах веб-портала «электронного правительства».
- Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»<sup>72</sup>, ст. 19, содержит определение видов услуг, оказываемых в электронной форме, а также регламентирует функционал «Электронного правительства» в ст. 21 – 31.
- Государственная программа «Цифровой Казахстан»<sup>73</sup>, утвержденная постановлением правительства РК от 12.12.2017 № 827. В программе описаны сервисы, которые планируется поддерживать при помощи функционала «электронного правительства», и отмечены проблемы, решение которых требует дополнительного внимания.

<sup>69</sup> Конвенция ООН [https://www.un.org/ru/documents/decl\\_conv/conventions/elect\\_com.shtml](https://www.un.org/ru/documents/decl_conv/conventions/elect_com.shtml)

<sup>70</sup> Резолюция ООН <https://undocs.org/A/HRC/32/L.20>

<sup>71</sup> Закон РК «О доступе к информации» <http://adilet.zan.kz/rus/docs/Z1500000401>

<sup>72</sup> Закон РК «Об информатизации» <http://adilet.zan.kz/rus/docs/Z1500000418>

<sup>73</sup> Программа «Цифровой Казахстан» <https://digitalkz.kz/napravleniya-programmy/>

- Административный Процедурно-Процессуальный Кодекс<sup>74</sup> (Кодекс Республики Казахстан от 29 июня 2020 года № 350-VI.) в п.1 ст. 22 определены права заявителя, подающего обращение в государственные органы.

### Компоненты электронного участия

Определяются следующие компоненты Электронного участия<sup>75</sup>:

Электронное информирование (предоставление информации в режиме онлайн): односторонняя связь, при которой правительство производит и поставляет информацию по разным онлайн-каналам для публичного использования гражданами. Это охватывает как «пассивный» доступ к информации по требованию граждан, так и «активные» меры правительства по распространению информации среди граждан.

Электронные консультации: двусторонняя связь, при которой граждане предоставляют обратную связь правительству с помощью онлайн-инструментов. Взаимодействие основано на предварительном определении правительством вопросов, по которым запрашиваются мнения граждан и которые требует предоставления информации.

Электронное партнерство: отношения, основанные на партнерстве с правительством, в котором граждане активно участвуют в процессе формирования политики с помощью различных онлайн-инструментов. На этом этапе признается роль граждан в предложении вариантов политик и формировании политического диалога, хотя ответственность за окончательное решение или формулировка политики лежит на правительстве.

К сожалению, такое, более узкое, понимание электронного участия концентрируется на создании «официальных площадок» для реализации гражданами электронного участия и оставляет за бортом неформальные инструменты, такие, как социальные сети, независимые сайты-агрегаторы петиций и т.п.

<sup>74</sup> АППК РК <https://adilet.zan.kz/rus/docs/K2000000350>

<sup>75</sup> Situation Review: Safety and Security of Cyberspace and E-Democracy in the Eastern Partnership Countries [https://ega.ee/wp-content/uploads/2017/10/ega\\_e-demcyber\\_FINAL\\_web.pdf](https://ega.ee/wp-content/uploads/2017/10/ega_e-demcyber_FINAL_web.pdf)

## Инструменты электронного участия в Казахстане

В рейтинге Индекса электронного участия (E-Participation Index)<sup>76</sup>, который составляется ООН, в 2020 году Казахстан занимает 29 место. Это показывает большой прогресс, поскольку в 2018 году в этом рейтинге Казахстан занимал 42 место. Индекс электронного участия в большей степени отражает реальные запросы граждан к национальной системе электронного правительства: степень информационной открытости государства и механизмы предоставления гражданам публичной информации, уровень вовлечения граждан в консультации с государственными органами и привлечения людей к обсуждению вопросов государственной политики, а также эффективные механизмы участия граждан в процессах принятия решений онлайн.

Государственная программа «Цифровой Казахстан»<sup>77</sup> в качестве одного из направлений реализации ставит задачу «перехода на цифровое государство» – преобразования функций государства как инфраструктуры предоставления услуг населению и бизнесу. При этом в идеале должна быть реализована модель управления, когда не гражданин обращается в госорганы за услугами, а государство, понимая потребности граждан, связывается с ними для оказания государственных услуг без необходимости физического посещения учреждений.

В настоящее время в Казахстане работает портал электронного правительства eGov<sup>78</sup>, который содержит вкладку «Электронное участие». Для пользования порталом и получения государственных услуг в электронном виде в Казахстане в 2003 году были внедрены электронные цифровые подписи – ЭЦП.<sup>79</sup> В то же время наблюдается постоянное увеличение количества сервисов, для которых, помимо ЭЦП, доступен другой способ авторизации – одноразовый пароль, получаемый с помощью СМС или push-уведомления. Планируется также использование биометрических систем идентификации в будущем.

<sup>76</sup> Онлайн версия исследования ООН Электронное Правительство 2020 (рус) <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf>

<sup>77</sup> Программа «Цифровой Казахстан» <https://digital.kz/o-programme/>

<sup>78</sup> Сайт eGov <https://egov.kz/cms/ru>

<sup>79</sup> Особенности применения электронной цифровой подписи в электронных документах <https://article.kz.com/article/13436>

Инструментом электронного участия является портал Открытого правительства<sup>80</sup>, являющийся, в свою очередь, агрегатором для порталов Открытых данных, Открытых НПА, Открытого диалога, Открытых бюджетов и Оценки эффективности деятельности государственных органов. Кроме этого, в списке инструментов находится портал Государственных закупок, и в 2021 г. запущен портал e-Otinish<sup>81</sup>, с помощью которого граждане могут подавать обращения в любые государственные органы Казахстана.

### Проблемы и точки роста

Реализация электронного участия в Казахстане, как и в других странах, встречает два основных типа проблем.

Первый тип проблем связан с технической и инфраструктурной составляющей деятельности Электронного правительства в целом. Имелись случаи технических сбоев и отказов, связанные с большим количеством обращений. Так, в период вспышки Covid-19 и объявления в стране чрезвычайного положения весной 2020 года, правительство принимало меры для поддержки граждан, потерявших доходы в связи с объявленным карантинном. В числе принимаемых мер была выплата пособия в размере минимальной заработной платы для граждан, потерявших доходы. Зарегистрироваться для получения пособия необходимо было на сайте eGov, но сайт не справился с количеством обращений. Заявления на выплату пособия подали более 8 миллионов граждан, причем одновременно подавалось до 25 тысяч обращений<sup>82</sup>. В этих условиях руководство НАО «Правительство для граждан» (оператор сайта eGov) было вынуждено организовать работу телеграм-ботов и запустить специальный сайт для приема обращений. Проблемы с доступом к portalу продолжались больше недели.

В целом пандемия коронавируса резко усилила актуальность электронного правительства, поскольку введенный карантин сделал невозможным получение государственных услуг каким-либо другим способом, кроме электронного обращения. Портал электронного правительства не всегда имел возможность обслуживать всех желающих получить государственные услуги в связи с большим количеством обращений. Было

<sup>80</sup> Сайт Открытое Правительство <https://open.egov.kz>

<sup>81</sup> Портал для подачи обращений граждан в госорганы <https://eotinish.kz>

<sup>82</sup> Новостной сайт Forbes.kz [https://forbes.kz/news/2020/04/04/newsid\\_222566](https://forbes.kz/news/2020/04/04/newsid_222566)

принято решение об использовании ботов в мессенджере «Телеграм», распределяющих запросы по областям и дающих стандартизированные формы обращений по одинаковым запросам. Такой подход позволил разгрузить серверы электронного правительства и значительно упростил доступ для граждан к самой востребованной на тот период услуге. Этот опыт является безусловно позитивным и может использоваться в будущем для совершенствования сервиса.

Все имеющиеся технические и инфраструктурные проблемы, связанные с функционированием портала электронного правительства, могут быть решены, и для этого пока не нужны никакие системные изменения. К сожалению, этого нельзя сказать о других проблемах полноценной реализации электронного участия в Казахстане.

Эти проблемы связаны с системным несовершенством подхода государства к реализации электронного участия. Государство делает ставку на развитие государственных сервисов, полностью игнорируя все альтернативы. Большое количество общественно важных вопросов и проблем активно обсуждается в социальных медиа; вопросы, волнующие граждан, формулируются и размещаются в виде петиций на независимых сайтах-агрегаторах петиций, производится сбор подписей. Однако вся эта гражданская активность, являющаяся на самом деле тоже электронным участием, не доходит до властей. Очевидно, что одной из главных причин январских событий 2022 стала слабая коммуникация между властью и обществом.

Определенные позитивные изменения все-таки имеются. Так, 31 января 2022, через 20 дней после январских событий, президент Казахстана впервые было принято решение о смене акима г. Алматы после появления петиции. Петиция была размещена на независимом сайте «Өтініш»<sup>83</sup> и не имела юридической силы, однако сыграла важную роль «социального термометра» и показала остроту проблемы городского управления в г. Алматы. К сожалению, пока это единственный пример принятия решения на основе неофициального обращения, однако сам факт того, что государство создало такой прецедент, обнадеживает.

На портале электронного правительства появился сервис E-Otinish, облегчающий подачу обращений в госорганы, однако

<sup>83</sup> Сайт петиций ОФ Талан <https://www.otinish.kz/ru/petition/83/>

до сих пор не принят пакет поправок в Административный Процессуально-Процедурный Кодекс (АППК), направленный на легализацию онлайн петиций. Законопроект, включающий поправки в АППК<sup>84</sup>, поступил в Мажилис в ноябре 2021 года и вызывает большое количество вопросов. Самые важные из них – завышенные требования по срокам и количеству стартовых подписей, срокам сбора и количеству подписей под петициями различного уровня, обширный список тем, которые не могут быть предметом петиции, завышенные сроки рассмотрения петиций и неопределенность с итогами рассмотрения. Более подробно поправки в АППК и рекомендации к разработчикам и организациям гражданского общества рассмотрены в материале, размещенном на сайте LPRC (Центра Исследования Правовой Политики).<sup>85</sup>

Таким образом, для развития и усиления инструментов электронного участия необходимы усилия и в юридической, и в процедурной, и в технической и инфраструктурной части.

Очевидной точкой роста является блок законопроекта о петициях, после принятия которого станет возможным реализация онлайн петиций в Казахстане. Однако в том виде, в котором в текущем варианте законопроекта предлагается подавать и рассматривать онлайн петиции, вряд ли этот инструмент будет эффективен. Наиболее разумным сейчас было бы полностью пересмотреть предлагаемые поправки в АППК в части условий подачи, сроков рассмотрения, сбора подписей и их количества. Также нужно пересмотреть и список «запретных тем», которые не могут пока, в предложенной редакции законопроекта, быть предметом петиций. Государственный портал онлайн петиций должен стать инструментом быстрого реагирования на имеющиеся вызовы, а не служить еще одним имитационным органом, каким он видится сейчас – медленным, сложным, забюрократизированным и безответственным. И пока закон еще не принят, и у законодателей, и у организаций гражданского общества есть возможность улучшить предлагаемый законопроект и сделать государственный портал онлайн петиций действенным и востребованным инструментом.

<sup>84</sup> Сайт Открытые НПА <https://legalacts.egov.kz/npa/view?id=9687582>

<sup>85</sup> Сайт Центра исследований правовой политики <https://lprc.kz/wp-content/uploads/2021/11/online-petitions-1.pdf>

Другой важной точкой роста является развитие мобильных решений и платформ электронного правительства. Уже сейчас самые востребованные услуги портала eGov доступны в мобильном приложении<sup>86</sup>; более того, такие документы, как паспорт вакцинации, доступны только в мобильном приложении. Развитие и совершенствование мобильного приложения, использование ботов в социальных медиа и мессенджерах помогут сделать электронное участие более доступным для граждан Казахстана и сделать государственное управление в стране более эффективным.

## ГЛОССАРИЙ

**Электронное правительство (e-Government)** – информационная система, обеспечивающая взаимодействие граждан, бизнеса и правительственных органов в электронном формате с минимальным физическим (личным) контактом.

**Электронное управление (e-Governance)** – использование информационно-коммуникационных технологий (ИКТ) правительством для предоставления государственных услуг, обмена информацией, коммуникационных операций и интеграции различных автономных систем и услуг.

**Электронная демократия (e-Democracy)** – использование информационных и коммуникационных технологий (ИКТ) в политических и управленческих процессах. Электронная демократия — это форма правления, при которой предполагается, что все взрослые граждане имеют право на равное участие в предложении, разработке и создании законов. Электронная демократия включает в себя социальные, экономические и культурные условия, которые позволяют осуществлять свободное и равное политическое самоопределение.

**МПГПП** – Международный Пакт о Гражданских и Политических Правах, основан на Всеобщей декларации прав человека, и обязывает страны-участницы уважать гражданские и политические права людей, включая право на жизнь, свободу религии, свободу слова, свободу собраний, избирательные права, права на надлежащую правовую процедуру, справедливое судебное разбирательство и т. д. Принят 16.12.1966, вступил в силу 23.03.1976.

<sup>86</sup> Сайт eGov [https://egov.kz/cms/ru/news/mobile\\_application](https://egov.kz/cms/ru/news/mobile_application)

**МПЭСКП** – Международный Пакт о Экономических, Социальных и Культурных Правах, основан на Всеобщей декларации прав человека и обязывает страны-участницы уважать экономические, социальные и культурные права людей, включая право на самоопределение, труд, социальное обеспечение, образование и т.д. Принят 16.12.1966, вступил в силу 3.01.1976.

**ЭЦП** – Электронная Цифровая Подпись, набор электронных цифровых символов, подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания. Подпись формируется в результате преобразования информации с использованием средств криптографической защиты информации. Она идентифицирует владельца сертификата ключа подписи, а также устанавливает отсутствие искажения информации в электронном документе.

### **Творческое задание**

Как, на ваш взгляд, должен быть реализован инструмент онлайн петиций в Казахстане? Что бы вы хотели изменить в той концепции, которая предлагается сейчас?

# ОГРАНИЧЕНИЕ

ИНТЕРНЕТА И  
БЛОКИРОВКИ  
КОНТЕНТА



*Елжан Кабышев*

## ОГРАНИЧЕНИЕ ИНТЕРНЕТА И БЛОКИРОВКИ КОНТЕНТА

Вопрос ограничения контента и интернета является очень дискуссионным во всем мире. Не существует единого подхода к определению нежелательного контента, так как национальные законодательства не всегда совпадают с международными стандартами.

### Международное законодательство

Отключение интернета в стране может являться нарушением прав человека. Совет ООН по правам человека на 47-й сессии 7 июля 2021 года принял [Резолюцию № A/HRC/47/L.22](#), которая «безоговорочно осуждает меры, которые в нарушение международного права прав человека мешают лицу или лишают его возможности искать, получать или передавать информацию в режиме онлайн, включая отключение Интернета и цензуру в режиме онлайн, призывает все государства воздерживаться от таких мер и прекратить их использование и призывает также государства обеспечить, чтобы все внутренние законы, политика и практика соответствовали их международным обязательствам в области прав человека, касающимся свободы мнений и их свободного выражения, а также ассоциации и мирных собраний, в онлайн среде».

“Право на интернет” или “право на доступ в интернет” является вопросом дискуссионным. Так, например, в исследовательском документе [“Интернет шатдаун и лимиты права”](#) авторы Giovanni De Gregorio и Nicole Stremlau указывают, что вопрос всё большего количества отключений интернета по всему миру, включая Великобританию и Соединенные Штаты, становится актуальнее в силу того, что социальные сети и мессенджеры не справляются с растущим негативным и вредным контентом.

Исследователи отмечают, что интернет следует рассматривать с точки зрения соответствия реализации прав человека, «инструментом», «механизмом реализации свободы выражения

мнений», а доступ к интернету, в свою очередь, не может являться «правом».

Действительно, в настоящее время «право на интернет» или «право на доступ в интернет» не являются в традиционном понимании правами человека, указанными в [Международном билле о правах человека](#). В данном контексте нужно ответить на вопрос: может ли шатдаун интернета негативно влиять на права человека с точки зрения «инструмента реализации права человека?». Следует отталкиваться от следующих принципов, указанных в [Сиракузских принципах](#) толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах:

- *допустимости;*
- *потребности;*
- *законности;*
- *соразмерности.*

Принцип «допустимости» означает, что основание ограничения права человека должно быть предусмотрено в Сиракузских принципах. Согласно п. 39 Принципов, государство-участник принимает меры отступления от своих обязательств [Международного пакта о гражданских и политических правах](#) (МПГПП) только в случаях исключительной и действительной или неминуемой опасности, которая угрожает жизни нации.

***Термин «угроза жизни нации» применяется, когда угроза:***

- затрагивает всё население и либо всю или часть территории государства;
- представляет опасность для физического здоровья населения, политической независимости или территориальной целостности государства или достаточного функционирования институтов, необходимых для обеспечения и защиты признаваемых в Пакте прав.
- В то же время государство, использующее право отступления, должно ввести режим ЧП, а также немедленно проинформировать другие государства, участвующие в МПГПП, через Генерального секретаря ООН о положениях, от которых оно отступило, и о причинах, побудивших к такому решению.

**Уведомление должно содержать в себе следующую информацию:**

1. перечисление положений Пакта, от которых государство-участник отступило;
2. копию документа об объявлении ЧП, а также конституционные положения, законы или указы, в соответствии с которыми вводится ЧП, с тем, чтобы государства-участники могли оценить степень отступления;
3. срок начала и окончания действия ЧП;
4. объяснение причин, по которым правительство решило прибегнуть к отступлению, включая краткое описание фактов и обстоятельств, которые привели к введению ЧП;
5. краткое описание того, какие последствия ожидаются от отступления от положений Пакта, и какое влияние они будут иметь на гарантируемые в Пакте права, включая копии решений об отступлении от этих прав, которые были приняты до уведомления.

В случае, если уведомление об отступлении не было незамедлительно направлено в должной форме государством-участником, то это государство тем самым нарушает свои обязательства перед остальными участниками и может лишиться правовой защиты, предусмотренной положениями Пакта.

Принцип «потребности» означает, что ограничение должно быть необходимым для государства или общества. При введении меры ограничения нужно отталкиваться от ответа на вопрос «является ли необходимым отключение интернета или контента в сети в целях безопасности государства и общества?».

**Принцип «законности» означает, что ограничение должно отвечать следующим пунктам:**

1. предусмотрено национальным законодательством и не противоречит международным стандартам;
2. законодательная база не должна быть произвольной и необоснованной;
3. нормы должны быть чёткими и конкретными, без содержания расплывчатых понятий;

4. должны быть предусмотрены гарантии и эффективные средства правовой защиты от незаконного или неправомерного введения или применения ограничений прав человека.

В [докладе A/HRC/17/27](#) от 16 мая 2011 года Специального докладчика Совета ООН по правам человека по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франк Ла Рю отмечает, что «... любое ограничение права на свободное выражение мнений должно соответствовать четким критериям, предусмотренным международным правом. Право людей выражать свое мнение через Интернет может ограничиваться разными способами: от технических мер по закрытию доступа к конкретному контенту, таких как блокирование или фильтрация, до недостаточного гарантирования права на неприкосновенность частной жизни и защиту личных данных, что мешает распространению мнений и информации. Специальный докладчик полагает, что произвольное использование уголовного законодательства с целью применения наказаний за законное выражение мнений не только является одной из наиболее пагубных форм ограничения этого права, поскольку оно не только создает "эффект замораживания", но и приводит к нарушениям других прав человека, таким как произвольное задержание и пытки и другие жестокие, бесчеловечные или унижающие достоинство виды обращения и наказания».

### **Национальное законодательство**

Ограничение, а также непосредственно само отключение интернета, предусмотрены в [Законе «О чрезвычайных положениях»](#) и [Законе «О связи»](#). Ограничение связи является основной мерой, которая применяется во время введения ЧП, и закреплено в [пп. 10 п. 1 ст. 15](#) закона.

Государство вправе управлять сетями связи не только в качестве ограничения, но также и в части приоритизации, как указано в ст. 14 вышеуказанного закона. По [информации](#) Palo Alto Networks, организации, занимающейся кибербезопасностью, «приоритизация трафика» (QoS — Quality of Service) - это набор технологий, которые работают в сети, чтобы гарантировать её способность надежно запускать высокоприоритетные

приложения и трафик при ограниченной пропускной способности сети.

В статье 41-1 Закона «О связи» предусмотрен порядок приостановления работы сетей и средств связи.

Генеральная прокуратура вносит в Комитет национальной безопасности (КНБ) представление о принятии мер по временному приостановлению работы сетей и (или) средств связи, оказания услуг связи, либо вносит в уполномоченный орган в области информации, Министерство информации и общественного развития (МИОР), представление об устранении нарушений законности с требованием о принятии мер по временному приостановлению доступа к интернет-ресурсам и (или) размещенной на них информации.


В случаях, не терпящих отлагательств и могущих привести к совершению тяжких и особо тяжких преступлений, КНБ вправе сам приостанавливать работу сетей и (или) средств связи, оказание услуг связи, доступ к интернет-ресурсам и (или) размещенной на них информации в интересах всех субъектов оперативно-розыскной деятельности с последующим уведомлением уполномоченных органов в области связи, информации и Генеральной прокуратуры Республики Казахстан в течение двадцати четырех часов.

Ограничение к определенному интернет-контенту или к сайту должно быть основано на основании предписания МИОР, Генеральной прокуратуры или решения суда. Однако практика такова, что абсолютное большинство интернет-контента ограничивается предписаниями МИОР.

Реализуют техническое ограничение доступа к сайту - операторы связи и АО "Государственная техническая служба", согласно статье 41-1 Закона "О связи".


Генеральная прокуратура, в свою очередь, по сообщениям МИОР, в принципе не ограничивает интернет-контент, либо же обращается в судебные органы для ограничения. Имеется информация, что ограничения были лишь в 2014 году — 33 материала по основаниям пропаганды идей терроризма и религиозного экстремизма, и в 2015 году — 35 материалов по аналогичному основанию.

В целом же, по официальным данным, с января 2014 года по январь 2022 года в интернете ограничено около 93860 материалов, среди которых доля внесудебного ограничения составляет 99,08% от общего числа.




**ЧТО НУЖНО ЗНАТЬ О БЛОКИРОВКАХ САЙТОВ В КАЗАХСТАНЕ?**

В соответствии с Законом интернет-ресурсы приравнены к СМИ. Исходя из этого, все требования, касающиеся СМИ, распространяется и на сайты. Что касается обязательной постановки на учет, таких требований к интернет-ресурсу нет. Но вы можете зарегистрировать сайт как сетевое издание в добровольном порядке.


**ВИДЫ БЛОКИРОВОК** 

**ВО ВНСУДЕБНОМ ПОРЯДКЕ**



**ГЕНЕРАЛЬНЫЙ ПРОКУРОР ИЛИ ЕГО ЗАМЕСТИТЕЛИ** - в случаях использования сетей или средств связи в преступных целях, наносящих ущерб интересам личности, общества и государства, а также для распространения информации, нарушающей законодательство о выборах, содержащей призывы к осуществлению экстремистской и террористической деятельности, массовым беспорядкам, а равно к участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, пропагандирующих сексуальную эксплуатацию несовершеннолетних и детскую порнографию.


**ПО РЕШЕНИЮ СУДА**




**УПОЛНОМОЧЕННЫЙ ОРГАН** выявляет нарушения на основе мониторинга и отправляет дело в суд

**ПРЕДСЕДАТЕЛЬ КНБ, ЕГО ЗАМЕСТИЛИ ИЛИ НАЧАЛЬНИКИ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ КНБ ЛИБО ЗАМЕЩАЮЩИЕ ИХ ЛИЦА** - в случаях, не терпящих отлагательства и могущих привести к совершению тяжких и особо тяжких преступлений, а также преступлений, подготавливаемых и совершаемых преступной группой.

**ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА, КНБ, МВД, МИНИСТЕРСТВО ОБОРОНЫ** - при угрозе или возникновении чрезвычайной ситуации социального, природного и техногенного характера, а также введении чрезвычайного положения на территории использования, а также приостановление деятельности сетей и средств связи, за исключением правительственной и президентской связи, сетей и средств связи экстренных служб



**ЧТО НУЖНО ЗНАТЬ О БЛОКИРОВКАХ САЙТОВ В КАЗАХСТАНЕ?**



**ПРОЦЕДУРА И СРОКИ**

Уполномоченный орган в **точное время** с момента получения направляет требование о принятии мер по выполнению предписания операторам связи или в государственную техническую службу.

После получения уведомления и проверки его достоверности уполномоченный орган дает поручение операторам связи и (или) государственной технической службе об отмене приостановления сайта. Операторы связи и (или) государственная техническая служба обязаны **немедленно** выполнить поручение.

Генеральный Прокурор или его заместители вносят в уполномоченный орган (сейчас – Министерство цифрового развития, инновации и аэрокосмической промышленности) предписание об устранении нарушений закона с требованием о принятии мер по временному приостановлению работы сетей или средств связи, оказания услуг связи, доступа к интернет-ресурсам или размещенной на них информации.

Операторы связи или государственная техническая служба обязаны выполнить требование в **точное не более трех часов**.

В случае если лицо, использующее сети в преступных целях, удалило противоправную информацию, то оно направляет уведомление об этом в уполномоченный орган.

В случаях, не терпящих отлагательства и могущих привести к совершению тяжких и особо тяжких преступлений, а также преступлений, подготавливаемых и совершаемых преступной группой, Председатель КНБ, его заместители или начальники территориальных органов КНБ либо лица, их замещающие, вправе приостанавливать работу сетей и (или) средств связи, оказание услуг связи, доступ к интернет-ресурсам и (или) размещенной на них информации в интересах всех субъектов оперативно-розыскной деятельности с последующим уведомлением уполномоченного органа в области связи и Генеральной прокуратуры Республики Казахстан в **течение двадцати четырех часов**.

Проверить, доступен ли сайт в КАЗАХСТАНЕ, а также пожаловаться на распространение ложной информации можно на сайте Министерства информации и общественного развития

<http://mic.gov.kz/ru/complain>



## Творческое задание

Вы - глава государственного органа, который модернизирует общественное сознание страны, и занимаетесь государственной политикой в отношении интернета и его контента. Однажды вы замечаете, что в социальных сетях распространяется картинка, которая становится вирусной. Вам дали поручение запретить этот материал, выписав соответствующее предписание с указанием правонарушений. Чем больше правонарушений с указанием Законов и определенных норм - тем лучше, так как вы будете эффективнее оправдывать блокировку картинки на местном телеканале Бахар 24/7.

Вам дают картинку на рассмотрение, на которой изображён бывший глава государства - Эль Президенте - со смешными нарисованными усами и очками (статья 373 УК РК<sup>87</sup>), рядом с ним изображен нынешний действующий глава государства с нарисованной бородой с надписью "мой тигр, мой краш"

<sup>87</sup> Публичное оскорбление и иное посягательство на честь и достоинство Первого Президента Республики Казахстан – Елбасы, осквернение изображений Первого Президента Республики Казахстан – Елбасы, воспрепятствование законной деятельности Первого Президента Республики Казахстан – Елбасы

(статья 375 УК РК<sup>88</sup>) и знакомый вами депутат Парламента с нарисованным цилиндром и подписью “кринж” (статья 376 УК РК<sup>89</sup>, 274 УК РК<sup>90</sup>). На фоне картинки вы можете различить флаг запрещенной организации Антикраш (Закон “О противодействии терроризму” и Закон “О противодействии экстремизму”, Закон “О защите детей от информации, причиняющей вред их здоровью и развитию”), с изображенными на ней цитатой, что нужно установить некий околорелигиозный строй в стране (статья 174 УК РК<sup>91</sup>, статья 179 УК РК<sup>92</sup>).

В связи с ростом популярности в соцсетях и мессенджерах, эта картинка используется также наркодиллерами и подписывают они в некоторых картинках словом “медлительность” и ссылкой на мессенджер, где это добро можно приобрести (статья 299-1 УК РК<sup>93</sup>).

Проанализировав эту картинку, вы начали писать в предписании какие правонарушения были совершены.

*Ответ: не менее 10 правонарушений*

---

<sup>88</sup> Посягательство на честь и достоинство Президента Республики Казахстан и воспрепятствование его деятельности

<sup>89</sup> Посягательство на честь и достоинство депутата Парламента Республики Казахстан и воспрепятствование его деятельности

<sup>90</sup> Распространение заведомо ложной информации

<sup>91</sup> Разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни

<sup>92</sup> Пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя Республики Казахстан

<sup>93</sup> Пропаганда или незаконная реклама наркотических средств, психотропных веществ или их аналогов, прекурсоров

# ОНЛАЙН-АДВОКАЦИЯ И ОНЛАЙН-АКТИВИЗМ



*Татьяна Чернобилъ*

## ОНЛАЙН-АДВОКАЦИЯ И ОНЛАЙН-АКТИВИЗМ

### Что такое онлайн-активизм?

Онлайн активизм, или киберактивизм – это гражданские действия для достижения социально значимых перемен с использованием цифровых медиа и технологий.

Онлайн активизм сегодня привлекает и вовлекает гораздо больше людей, чем активизм оффлайн. Почему? Потому что он позволяет людям свободнее самовыражаться, скрываясь за аватарками, то есть, как они считают, анонимно (что на самом деле не так – социальные сети практически не оставили места для анонимности). Тем не менее, интернет действительно создает иллюзию одновременно и дистанционирования от аудитории и солидарности с аудиторией, и в целом более раскрепощенного общения, что это может быть, как хорошо, так и плохо. Другая причина - для участия в онлайн-активизме не требуется много времени, усилий или заранее спланированных действий со стороны пользователя.

Онлайн активизм стал более заметен с развитием социальных сетей, особенно, Facebook и Instagram, а в начале 20-х годов - TikTok.

### Онлайн-кампании

Среди онлайн-кампаний, которые привлекли огромное внимание и волну сторонниц по всему миру, – кампания #MeToo. В 2006 году американская активистка за права женщин-жертв сексуализированного<sup>94</sup> насилия Тарана Бёрк стала



*Тарана Бёрк*

<sup>94</sup> Правильным считается говорить именно «сексуализированное», а не «сексуальное» насилие, чтобы избежать любого налета привлекательности в выражениях, касающихся преступлений против половой свободы и неприкосновенности личности.

использовать это словосочетание, которое переводится как «и я» или «я тоже» для выражения солидарности с жертвами такого насилия. В 2017 году движение получило новый виток, когда американская актриса Алисса Милано в поддержку жертв домогательств голливудского продюсера Харви Вайнштейна, призвала женщин, которые тоже подвергались домогательствам, подписаться под ее постом в Твиттере словами 'me too'. Всего за два дня после этого хештэг MeToo распространили более миллионов пользователей Твиттера. Вскоре хештэг подхватили пользователи Facebook. И там за сутки #MeToo распространили уже более 4.7 миллионов пользователей, сделав 12 миллионов репостов. Хештэг продолжает жить и сегодня.



Среди результатов этой кампании – поддержка жертв сексуализированных домогательств; укрепление сообществ жертв; повышение общественной осведомленности о проблеме сексуализированных домогательств; смещение общественного мнения в сторону однозначной поддержки жертв; изменение законодательства; прерывание молчания вокруг проблемы сексуализированных домогательств, насилия и травли; привлечение если не к ответственности, то к ответу многих влиятельных мужчин, виновных в домогательствах; создание фондов в поддержку жертв домогательств; принятие новой политики по домогательствам Международной организацией труда (МОТ).

В регионе Восточной Европы и Центральной Азии аналогом кампании #MeToo сначала стало движение #ЯНеБоюсьСказать (рус. «я не боюсь сказать»), которое начала украинская журналистка и феминистка Анастасия Мельниченко в украинском Facebook за год до #MeToo. В Украине результатом этой кампании стало обсуждение на уровне Рады необходимости присоединения Украины к Конвенции Совета Европы о предотвращении и борьбе с насилием в отношении женщин и домашним насилием (Стамбульская конвенция).

В казахстанском сегменте интернета аналогом #MeToo стала онлайн-кампания #HeMолчи, начатая правозащитницей Диной Тансари. Теперь #HeMолчи – это общественный фонд, который на своем сайте сообщает о более чем 110 привлеченных за пять лет к ответственности насильников.

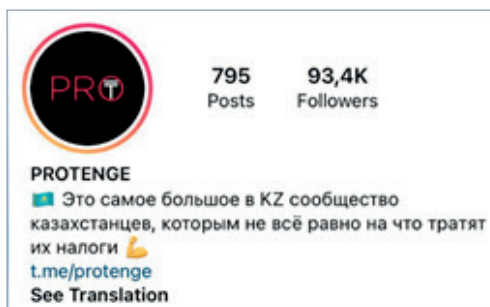
# #HeMолчикz

## Онлайн-петиции и другие формы онлайн-активизма

Международное правозащитное движение **Amnesty International** (рус. «Международная амнистия») регулярно предлагает своим сторонникам подписываться под петициями в адрес правительств разных стран с требованиями принять или отменить меры, нарушающие права человека тех или иных активистов или правозащитников. Петиции (обращения) можно заполнить как онлайн, так и оффлан.



В странах Центральной Азии для создания и подписания петиций с переборами доступны платформы либо **change.org** либо **avaaz.org**.



Набирающий популярность вид онлайн-активизма – онлайн-расследования и презентация их результатов. Инстаграм-аккаунт **ProTenge**, а позже также канал в Telegram, основанный казахстанской журналисткой

Джамилей Маричевой в 2020 году, ежедневно информирует почти сто тысяч казахстанцев о нецелевом или подозрительном расходовании государственных бюджетных средств и, главное, мобилизует читателей к действию: учит и мотивирует их самим отслеживать манипуляции бюджетными средствами, рассказывать о них, оспаривать случаи нецелевого использования и не допускать подобного в будущем. В конце 2021 года Джамилей Маричева была удостоена звания «Выдающиеся борцы с коррупци-

ей» (Anticorruption champions), которое ежегодно присваивает активистам и журналистам во всем мире государственный департамент США.

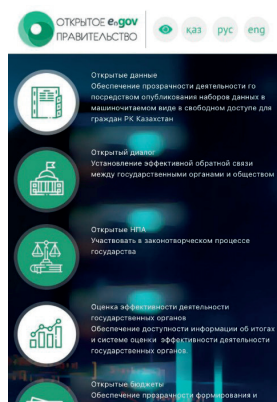
Другой популярный вид онлайн-активизма – арт-активизм, когда художники выражают свое мнение в соцсетях. В Казахстане можно вспомнить Le Shapalague Comics из Инстаграм или аккаунты с сатирическими новостями или пародиями на новости.

Как правило, онлайн-активизм делают возможным социальные сети, где легко можно получить выход на довольно большую аудиторию и мобилизовать пользователей к действиям в защиту общественных интересов.

Часто подобного рода онлайн-активизм – выход для активистов в тех странах, где проявлять офлайн-активизм небезопасно из-за опасений преследований со стороны государства.



### Что такое онлайн-адвокация?



**Онлайн-адвокация** – это разновидность онлайн-активизма, то есть те же действия в защиту общественных интересов, но направленные на представителей власти как лиц, принимающих решения.

Большие возможности для онлайн-адвокации в Казахстане дает платформа «Открытое правительство» EGov. На портале egov можно получить огромное количество госуслуг, а также отследить законотворческие инициативы, оставить свои комментарии, направить обращения к представителям тех или иных

государственных органов, пожаловаться на их действия или бездействия. Все это – формы онлайн-адвокации.

Цифровая среда предлагает очень большие возможности для активного гражданского участия в управлении делами государства.

# АНОНИМНОСТЬ

## В ИНТЕРНЕТЕ



*Елжан Кабышев*

## АНОНИМНОСТЬ В ИНТЕРНЕТЕ

### Международные стандарты

Право на анонимность в интернете не предусмотрено в международно-правовых документах. Однако в последнее время в связи с ростом интернет-технологии выпускаются доклады об анонимности.

22 мая 2015 года был выпущен [Доклад](#) Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кея. Доклад рассматривает вопрос об использовании средств шифрования и анонимности при передаче цифровых сообщений. С учетом изученных международных и национальных норм и судебных решений, а также материалов, полученных от государств и гражданского общества, в докладе сделан вывод о том, что шифрование и анонимность позволяют людям осуществлять свои права на свободу мнений и их свободное выражение в цифровой век и ввиду этого могут заслуженно пользоваться надежной защитой.

При подготовке доклада Специальный докладчик направил государствам вопросник для сбора представляющей интерес информации об их законодательстве, нормативах, политике и практике. На опросник ответили 16 стран, и Казахстан - в этом списке.

Спецдокладчик сообщает, что неприкосновенность частной жизни является залогом свободы мнений и их свободного выражения.

Статья 17 [Международного пакта о гражданских и политических правах](#) (МПГПП), статья 12 [Всеобщей декларации прав человека](#) (ВДПЧ) прямо защищают каждого человека от "произвольного или незаконного вмешательства в его личную и семейную жизнь, произвольного или незаконного посягательства на неприкосновенность его жилища или тайну его корреспонденции" и "незаконных посягательств на его честь и репутацию" и предусматривает, что "каждый человек имеет

право на защиту закона от такого вмешательства или таких посягательств”.

**Докладчик осудил такие практики государств, как:**

1. запрет на индивидуальное использование технологий шифрования и борьба с применением средств шифрования;
2. намеренное понижение степени эффективности шифрования;
3. депонирование ключей;
4. обязательное раскрытие ключа по сравнению с адресными распоряжениями о расшифровке данных;
5. запрет анонимных высказываний в интернете;
6. принуждение к регистрации сим-карт и мобильных устройств под настоящим именем для доступа в интернет;
7. политика локализации хранения данных внутри страны, и фиксация деятельности всех пользователей страны в интернете.

В Докладе Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю сообщается, что право на неприкосновенность личной жизни часто понимается как одно из базовых условий реализации свободы выражения мнений. Чрезмерное вторжение в личную жизнь может как напрямую, так и косвенно ограничивать свободное развитие идей и свободный обмен ими. Ограничения на анонимность при передаче сообщений, например, оказывают очевидное пугающее воздействие на жертв всех форм насилия и посягательств, которые могут неохотно предоставлять соответствующую информацию, опасаясь двойной виктимизации.

Анонимность, по общему признанию, играет важную роль в защите и поощрении частной жизни, свободного выражения мнений, политической подотчетности, участия общественности и публичных обсуждений. Но ни во ВДПЧ, ни в МПГПП анонимность не упоминается. В ходе переговоров по подготовке Пакта было предложено включить в пункт 1 статьи 19 фразу "анонимность не допускается". Однако это предложение было отклонено "среди прочего, на том основании, что анонимность может в некоторых случаях оказываться необходимой для

защиты автора" и "такая оговорка может стать препятствием для использования псевдонимов".

В Докладе А/НRC/29/32 Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение от 22 мая 2015 года сообщается, что запрет анонимности в онлайн-среде препятствует осуществлению права на свободное выражение мнений. Во многих государствах запрет вводится безотносительно каких-либо конкретных государственных интересов. Согласно Конституции Бразилии (статья 5) запрещены анонимные выступления.

Анонимность также запрещена положениями Конституции Республики Венесуэла (статья 57). В 2013 году во Вьетнаме было запрещено использование псевдонимов, ввиду чего всем частным лицам, ведущим персональные блоги, пришлось официально сообщить свое настоящее имя и адрес. В 2012 году в Исламской Республике Иран было введено требование о регистрации всех адресов IP, используемых в стране, а посетителей Интернет-кафе обязали регистрироваться под своим настоящим именем до начала пользования компьютером. В соответствии с Органическим законом о телекоммуникации, действующий в Эквадоре, лица, оставляющие комментарии на веб-сайтах, и владельцы мобильных телефонов обязаны регистрироваться под своим настоящим именем.

### **Национальное законодательство**

Вопрос анонимности в сети в Казахстане весьма чувствительный. Так, в Казахстане официально запрещены анонимные комментарии с 2017 года. Статья 36 Закона "Об информатизации" пополнилась новым пунктом 5-1 следующего содержания: "Оказание собственником или владельцем общедоступного электронного информационного ресурса услуги по размещению пользователем информации в Интернет осуществляется на основании соглашения, заключаемого в письменной форме (в том числе электронной), с идентификацией на портале "электронного правительства" или посредством использования зарегистрированного на общедоступном информационном электронном ресурсе абонентского номера сотовой связи пользователя с отправлением короткого текстового сообще-

ния, содержащего одноразовый пароль, для заключения соглашения.

*Размещение информации пользователем осуществляется под своим именем или псевдонимом (вымышленным именем). Обезличивание персональных данных осуществляется на основании и в порядке, определенных соглашением».*

Вопросы обезличивания персональных данных регулируются статьей 17 [Закона Республики Казахстан “О персональных данных и их защите”](#).

*«Собственник или владелец электронного информационного ресурса, оказывающего услуги по размещению пользователем информации в Интернете, обязаны хранить информацию, используемую при заключении соглашения, весь период действия, а также в течение трех месяцев после расторжения соглашения и создавать организационные и технические условия для проведения оперативно-розыскных и контрразведывательных мероприятий субъектами оперативно-розыскной и контрразведывательной деятельности».*

Соответствующая норма была добавлена принятием [Закона Республики Казахстан от 28 декабря 2017 года № 128-VI ЗРК “О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информации и коммуникаций”](#).

В связи с нововведением казахстанские СМИ в основном отключили возможность комментирования, либо же вставили плагин комментариев социальных сетей.

### **IMEI + ИИН + номер телефона**

С 1 января 2019 года получить доступ в интернет анонимно для граждан практически невозможно. Услуга доступа в интернет не будут оказываться тем абонентам, которые не зарегистрировали абонентские устройства сотовой связи. Согласно статье 36-2 [Закона “О связи”](#), владелец абонентского устройства сотовой связи обязан зарегистрировать его у оператора сотовой связи в соответствии с правилами регистрации абонентских устройств сотовой связи, в противном случае не будет получен доступ в интернет. Для регистрации устройства абонент предоставляет оператору связи следующие данные:

1. Индивидуальный идентификационный номер (ИИН) или бизнес-идентификационный номер (БИН);
2. Идентификационный код абонентского устройства сотовой связи (IMEI, англ. International Mobile Equipment Identity - международный идентификатор мобильного оборудования);
3. Абонентский номер, который используется на абонентском устройстве сотовой связи.

Эти данные оператор связи передает в базу данных идентификационных кодов абонентских устройств сотовой связи (БДИК). Оператором базы является РГП “Государственная радиочастотная служба” Министерства цифрового развития, инноваций и аэрокосмической промышленности РК. РГП “Государственная радиочастотная служба” разместила на своем интернет-ресурсе следующие сервисы, которые по запросу пользователя берут данные из БДИК:

1. сервис проверки регистрации IMEI;
2. сервис проверки мобильных номеров, зарегистрированных на ИИН;
3. сервис проверки регистрации, связи ИИН и IMEI;
4. сервис проверки количества абонентских номеров, зарегистрированных на IMEI.

Согласно пункту 21 [Правил регистрации абонентских устройств сотовой связи](#), оператор связи осуществляют оплату услуг РГП “Государственная радиочастотная служба” за предоставление доступа к ресурсам БДИК. Соответственно, данное нововведение несет определенные расходы для субъектов бизнеса, что увеличивает стоимость услуг для конечных пользователей.

Изменение номера IMEI является уголовным правонарушением согласно [Статья 213 Уголовного Кодекса РК](#) «Неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства». Санкция данной статьи предусматривает наказание в виде:

- штрафа в размере до 160 МРП;
- либо исправительными работами в том же размере,

- либо привлечением к общественным работам на срок до 160 часов,
- либо арестом на срок до 40 суток.

Нововведение по регистрации абонентских устройств государство **обосновало** противодействием ввозу и реализации контрафактных устройств и кражей.

Спецдокладчик в Докладе A/HRC/29/32 со своей стороны отмечает тенденцию государственной политики по идентификации людей посредством SIM-карты по всему миру: *"[...] Правительства часто требуют регистрации сим-карты; так, почти в 50 странах Африки действуют или принимаются законы, требующие при активации сим-карты вводить персональные данные, удостоверяющие личность. В Колумбии с 2011 года введен порядок обязательной регистрации номеров мобильной связи, а в Перу начиная с 2010 года все сим-карты привязываются к национальному идентификационному номеру"*.

Спецдокладчик отмечает, что регистрация номера и анонимность человека - несовместимые вещи: *"Возможность введения таких правил рассматривается и в других странах. Такие правила нарушают анонимность, в особенности в случае лиц, выходящих в Интернет только с помощью мобильных технологий. Обязательная регистрация сим-карт дает правительствам возможность следить за частными лицами и журналистами в гораздо большей степени, чем того требуют их законные интересы"*.

### **Сертификат безопасности**

Законом "О связи" предусмотрено использование сертификата безопасности. Пункт 36-1 статьи 2 раскрывает понятие "сертификата безопасности" в следующей редакции: "набор электронных цифровых символов, применяемый для пропуска трафика, содержащего протоколы, поддерживающие шифрование".

Операторы междугородной и (или) международной связи (то есть провайдеры) обязаны осуществлять пропуск трафика с использованием протоколов, поддерживающих шифрование с применением сертификата безопасности, за исключением трафика, зашифрованного средствами криптографической защиты

информации на территории страны (подпункт 4 пункта 3-1 статьи 26 Закона “О связи”).

Согласно статье 11 Приказа № 23/нс от 27 марта 2018 года “Об утверждении Правил выдачи и применения сертификата безопасности”, “Операторы связи обеспечивают распространение сертификата безопасности среди своих абонентов, с которыми заключены договоры на оказание услуг связи”.

По задумке государства сертификат безопасности используется для ограничения распространения по сети телекоммуникаций информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан.

В случае, если операторы связи не исполняют данные Правила, то подпунктом 9-3 “Нарушения операторами связи правил применения сертификата безопасности” и подпунктом 9-5 “Предоставления оператором связи доступа к информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан» (часть дополнена подпунктами 9-1 – 9-6 в соответствии с Законом Республики Казахстан № 419-V от 24 ноября 2015 года) статьи 637 “Нарушение законодательства Республики Казахстан в области связи” [Кодекса об административных правонарушениях](#) предусмотрена административная ответственность операторов связи, которая влечет штраф:

- на физических лиц в размере 10 месячных расчетных показателей (МРП),
- на должностных лиц, субъектов малого предпринимательства в размере 20 МРП,
- на субъектов среднего предпринимательства - в размере 40 МРП,
- на субъектов крупного предпринимательства - в размере 100 МРП.

Таким образом, внедрение сертификата для операторов связи носит обязывающий характер и предусматривает административную ответственность за его неисполнение, в частности КоАП РК.

Государственный уполномоченный орган (МЦРИАП) сообщал, что пользователь вправе не устанавливать сертификат на свое устройство, так как в законе не предусмотрена обязывающая норма для абонента и не имеется ответственности за не установку.

Но есть нюанс, который заключается в следующем. В соответствии с пунктом 3 Правил выдачи и применения сертификата безопасности, оператор связи направляет заявление на выдачу сертификата безопасности по форме (приложение №1 к Правилам) в органы национальной безопасности. В течение 10 рабочих дней осуществляется выдача сертификата.

Далее, согласно пункту 10 Правил, операторы связи уведомляют абонентов письменно в произвольной форме, с которыми заключены договоры на оказание услуг связи, об изменении условий предоставления доступа к сервисам или ресурсам. Операторы связи обеспечивают распространение сертификата, публикуют на своих официальных интернет-ресурсах инструкции по его установке.

То есть говорить о добровольности установки сертификата довольно сложно, так как данный вопрос решается не на уровне законов, а на уровне договорных отношений между абонентом и оператором связи, оказывающим услуги. Оператор связи скован нормативными правовыми актами, и в случае их нарушения, ему грозит ответственность.

В свою очередь пользователь может отказаться от услуг оператора связи, но в таком случае говорить о свободном доступе в интернет без сертификата не имеет смысла.

Государством использование сертификата безопасности оправдывается в целях ограничения запрещенных материалов по вступившим в законную силу решений судов и законами РК.

Но данный метод ограничения довольно спорный в силу следующих обстоятельств:

1. Ограничивается право на тайну переписки, право на тайну личной жизни, свобода поиска, получения и распространения информации. В целом трафик пользователя становится читаемым.
2. Устанавливается онлайн-цензура.
3. Требуется установка сертификата безопасности напрямую на устройства абонента.
4. Используется MITM (man-in-the-middle), то есть встраивается третья сторона между абонентом и сервером.

## ГЛОССАРИЙ

**Анонимность** - (с греческого "анопота" - "безымянность") - это состояние, когда нет какой-либо информации об определенном лице, и его практически нельзя идентифицировать.

**Анонимность в интернете** - - это комплекс мер и способов, в частности, как сокрытие или подмена IP-адреса, запрет cookies и отслеживания рекламными трекерами, основной целью которой является сохранение в тайне своей цифровой личности.

## Творческое задание

Тема для обсуждения в группах:

*Что для вас более важно и почему?*

- анонимность с возможностью свободно реализовывать право на выражение своего мнения без последствий,
- либо же тотальная слежка, однако с высоким уровнем безопасности и защиты населения и вас самих?

Поясните свой ответ с достаточными аргументами

# ФАКТЧЕК

КАК ЖУРНАЛИСТСКИЙ  
ФОРМАТ И НЕОБХОДИМЫЙ  
НАВЫК

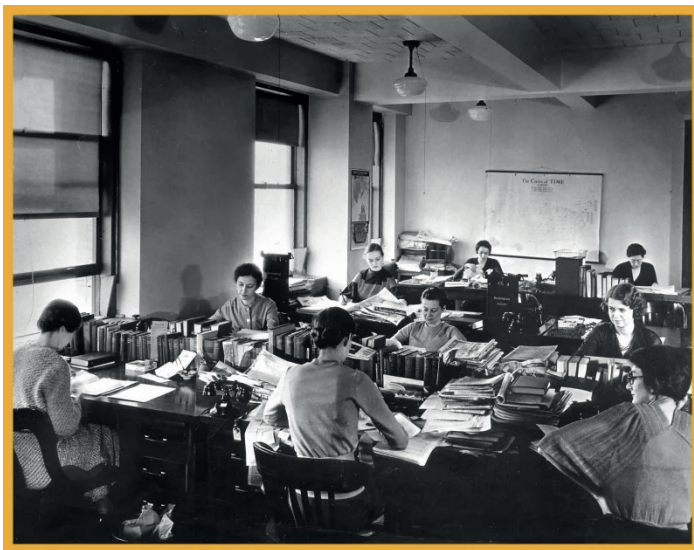


Павел Банников

## ФАКТЧЕК КАК ЖУРНАЛИСТСКИЙ ФОРМАТ И НЕОБХОДИМЫЙ НАВЫК

### История фактчека: от «девочек» до Нобелевки

Вопреки достаточно распространённому даже в среде самих журналистов стереотипу, фактчек не является для журналистики новым, возникшим сравнительно недавно, явлением. Профессия фактчекера появилась в начале 1920-х годов, а в словарях была зафиксирована уже в 1922<sup>95</sup>. Наличие службы фактчека/бюро проверки — обычное дело для печатных изданий на протяжении почти всего 20 века. Если вы помните фильм «Сбежавшая невеста» с Ричардом Гиром и Джулией Робертс в главных ролях, то наверняка обратили внимание, что персонажа Гира увольняют из редакции ровно за нарушение правил фактчека при подготовке материала.



*Женское фактчекерское бюро за работой, 1933 г.*

<sup>95</sup> Here's How the First Fact-Checkers Were Able to Do Their Jobs Before the Internet

«Девочки, которые могут спасти любой текст» — так называли фактчекеров журналисты TIME. В начале 20 века женщине стать автором было весьма непросто, и одной из немногих возможностей для женщины попасть в журналистику стала профессия фактчекера. В значительной мере первые фактчекеры несли на себе и корректорские функции, однако важное их отличие от корректоров заключалось в проверке не только написания слов, но и фактов, представленных в материале. Если корректорский стол занимали словари, то стол фактчекера ломился от энциклопедий, справочников «Кто есть кто» и газетных вырезок, а в библиотеках их знали в лицо, почти как сотрудников.

К середине 20 века фактчекерская служба или бюро проверки существовали практически во всех крупных СМИ по всему миру. В это же время фактчек начинает своё движение к современному состоянию: появляется всё больше открытых данных, возможностей для быстрого получения и обработки информации, но окончательно формат формируется к началу 2000-х после начала глобального кризиса доверия к СМИ, отчасти вызванному управленческими решениями.

### **Кризис СМИ в 1990-х**

Глобальный тренд 1990-х — сокращение редакторского штата и штатных журналистов. В целях экономии издатели сокращают не только число журналистов, отдавая предпочтение стрингерам на местах, но и редакции. И первыми «под нож» вместе с профильными редакторами идут бюро проверки. Внутриредакционная проверка в большей мере остаётся делом печатных изданий с историей и репутацией, но даже они отказываются в какой-то момент от услуг профессиональных фактчекеров, перекладывая эту обязанность на авторов и выпускающих редакторов. Так, отдел фактчека в Newsweek был упразднён в 1996 году<sup>96</sup>. Безусловно, это не единственная причина кризиса доверия к СМИ, исследователи называют в числе причин и тягу к сенсационализму, и предпочтение мнений вместо фактов, и увлечение издателей политическим активизмом, и популизм политических лидеров в их конфронтации с журналистикой<sup>97</sup>.

<sup>96</sup> Newsweek ditched its fact-checkers in 1996, then made a major error - Poynter

<sup>97</sup> Lack of trust in the news media, institutional weakness, and relational journalism as a potential way forward - Seth C Lewis, 2019

Вкупе весь ряд причин, вызвавших кризис доверия приводит к тому, что из почти столетнего опыта внутриредакционного фактчекинга формируется новый формат журналистской работы и написания журналистского материала<sup>98</sup>. И этот формат оказывается успешным и востребованным. Яркие свидетельства тому — Пулитцеровская премия<sup>99</sup> фактчекинговому проекту PolitiFact в 2009 году и Нобелевская премия мира, разделенная между главным редактором российского издания «Новая газета» и соучредительницей занимающегося фактчеком и расследованиями филиппинского проекта Rappler Марии Рессе<sup>100</sup> в 2021.

### Фактчек как внутриредакционный процесс и как формат

Фактчек как внутриредакционный процесс мало изменился за сто лет существования профессии. Фактчекер остаётся связующим звеном между автором и редактором, именно на этом этапе происходит оценка фактологичности и фатичности информации. Основная задача внутриредакционного фактчека — не допустить случайного или целенаправленного дезинформирования аудитории. Задача фактчекерской редакции с одной стороны — нивелировать вред от уже распространившейся дезинформации, с другой — дать независимую оценку фактическим высказываниям, которые могут повлиять на общество. Результаты внутриредакционного фактчека редко выходят за пределы редакции, тогда как можно отобразить сходство и разницу между внутриредакционным фактчеком и фактчеком как форматом в следующей схеме:

	Внутриредакционный фактчек	Фактчек как формат
Момент проверки	До публикации в собственном издании	После публикации проверяемого высказывания на другом ресурсе
Методы проверки	Открытые данные, инсайдерские данные	Только открытые данные
Материал для проверки	Вся поступающая фактологическая информация	Высказывания, отобранные в соответствии с принципами отбора конкретного фактчекингового ресурса
Аудитория	Редакция	Широкая аудитория

<sup>98</sup> (PDF) Теоретическое обоснование фактчека как формата журналистики | Pavel Bannikov and Tasha Sokolova - Academia.edu

<sup>99</sup> PolitiFact wins Pulitzer

<sup>100</sup> 100 лет тюрьмы: кто такая Мария Ресса, получившая Нобелевскую премию мира | Forbes Woman

Отчасти фактчек как формат журналистики близок к расследованию, но два принципиальных момента отличают их друг от друга:

1. Отношение к открытым данным: фактчек (как формат) опирается только на открытые данные и раскрытые источники, расследование же (как и редакционный фактчек) может опираться и на закрытые источники, на серые и чёрные данные и на анонимные источники.
2. Расследование/исследование обязательно ставит новый вопрос. Фактчек отвечает на уже сформулированный вопрос, на который можно ответить в формате «да/нет»: лжёт ли спикер или говорит правду? Правдив или ложен существующий нарратив?

### **Открытые данные**

В фактчеке форматно недопустимо использование анонимных источников и закрытых или серых данных. И именно революция web 2.0 и появление множества машиночитаемых открытых данных стали одним из основных двигателей развития фактчека как отдельного формата. Ещё в 2000 году невозможно было себе представить тот массив данных, к которым возможно получить доступ, просто оплатив подключение к интернету, а доступ к спутниковым снимкам практически в реальном времени казался нереализуемой мечтой.

Тем не менее, важно отметить и сложность работы с такими данными: часть из них методологически структурирована, как, например, данные Всемирного банка или SIPRI, часть не структурирована и переходит из серой зоны в белую, как, например, сливы финансовой документации банков (Pandora Papers) переписки или данных спецслужб (WikiLeaks). Часть данных — «сырые», такие как открытые публикации в социальных сетях (публичная оферта большинства соцсетей позволяет использовать любые данные, опубликованные не в формате friends only). В случае со структурированными данными работа максимально проста и требует лишь понимания методологии, сырые данные требуют дополнительных навыков и инструментов. Благодаря технологическому рывку и вниманию к работе

расследователей и фактчекеров регулярно появляются новые инструменты работы с сырыми данными<sup>101</sup>.

Кажущаяся простота верификации при наличии большого количества данных и доступа к интернету — один из вызовов, который стоит перед каждым, кто занимается проверкой данных.

### Принципы отбора материала

Чтобы утверждение могло быть проверено силами фактчека, оно должно соответствовать нескольким параметрам — принципам отбора.

Первое и самое главное условие для любой проверки — это принципиальная проверяемость. Утверждение должно быть конкретным, а не абстрактным, а фактчекер должен обладать необходимыми для проверки средствами. Проверить размытое заявление политика о том, что страна стала жить лучше, невозможно, так как в нём отсутствуют принципиально проверяемые элементы. Однако если политик скажет, как именно изменились какие-то макро- и микроэкономические показатели, в его слова появятся факты, и журналист сможет их проверить. При этом не для любых данных у журналиста достаточно средств проверки. Например, переданные инсайдером в СМИ показатели из засекреченных статей бюджета непроверяемы, даже если информация фактологическая.

Второй важный критерий в опыте фактического СМИ — уровень ретрансляции. Обычно проверяются утверждения, широко разошедшиеся в обществе, опубликованные во многих СМИ, упоминаемые блогерами и известные широкому кругу читателей. Уровень ретрансляции — не постоянная во времени величина, ещё вчера никто мог не упоминать о каком-то факте, а после того, как его разместил у себя на страничке блогер с миллионной аудиторией, он становится широко известен. Ярким примером изменчивости уровня ретрансляции может служить популярность витамина C для лечения различных заболеваний. Когда Лайнус Полинг в 1970 году только опубликовал свою книгу об уникальном витамине для поддержания здоровья, информация о незаменимости витамина С была повсюду. Со временем интерес к веществу постепенно утихал, однако с наступлением пандемии новой коронавирусной инфекции публикации об целебных

<sup>101</sup> Bellingcat's Online Investigation Toolkit [bit.ly/bcattools]

свойствах витамина снова стали широко распространяться. Учитывая возросший уровень ретрансляции, утверждения о полезности этого БАДа стали предметом рассмотрения фактчекеров.

Третий критерий отбора материалов для фактчека — общественный интерес и общественная значимость проверяемого утверждения. В первую очередь проверке подвергаются те высказывания, которые или принадлежат ключевым лицам страны или, чья правдивость или ложность влияет на жизнь многих людей.

Те утверждения, которые соответствуют всем трём критериям одновременно, и представляют собой исходный материал для фактчека.

### **Вердикты в фактчеке**

Так называемая «вердиктная линейка» — необходимый атрибут фактчекерского издания. Отчасти от того, насколько она подробна и детально проработана, зависит и сам выбор материала для анализа. Большинство высказываний невозможно разделить на две корзины: правда или ложь. Это сильно упрощало бы саму картину мира, ведя к дополнительным искажениям. Поэтому фактчекерские редакции создают более детальные линейки вердиктов, включающие в себя различные промежуточные позиции. Ознакомимся с наиболее популярными из них.

Вслед за правдой во многих СМИ есть вердикт «большой частью правда». Он означает, что проверенное утверждение в основном соответствует действительности, однако незначительные детали, не влияющие на общее понимание темы, приведены не совсем точно или опущены. Такой вердикт, например, был присвоен утверждению, что компания Apple замедляет старые модели iPhone. Фактчекеры нашли<sup>102</sup> свидетельства того, что компания сама призналась в замедлении старых моделей, однако делала это, по их словам, в благих целях — чтобы не допустить внезапного отключения из-за перегрузок. В целом проверяемое утверждение соответствует действительности, при этом существует ещё декларируемый благородный мотив, о котором во многих публикациях о замедлении старых моделей не говорят.

<sup>102</sup> Правда ли, что Apple замедляет старые айфоны, чтобы стимулировать продажи новых?

Пожо́ж на вердикт «большей частью правда» также вердикт «скорее всего правда», однако есть существенное различие. В случае вердикта «большей частью правда» сумма доказательств у фактчекеров достаточно существенна, при этом недостаточна для вынесения однозначного вердикта «правда».

Следом по градации от правды ко лжи идёт вердикт «полуправда», он означает, что в проверяемом утверждении правдивые и неправдивые элементы представлены почти поровну. Такой вердикт фактчекеры вынесли распространённому утверждению «самка богомола после спаривания съедает самца». Выяснилось<sup>103</sup>, что практика сексуального каннибализма действительно распространена, однако предварительно поевшая самка обычно оставляет партнёра в живых. Также по аналогии с вердиктами «большей частью правда» и «скорее всего правда» существуют вердикты «большей частью неправда» и «скорее всего неправда». Некоторые ресурсы (например, Factcheck.kz) используют также вердикт «манипуляция», он означает, что данные частично корректны, но искажают ситуацию с целью тем или иным образом повлиять на общественное мнение<sup>104</sup>.

Некоторые фактчекерские ресурсы, например, «Проверено. Медиа» отдельно рассматривают случай, когда цитата или изображение сами по себе верны, но вырваны из контекста. Таким вердиктом журналиста обозначили фотографию<sup>105</sup>, подпись к которой гласила, что это скелет доисторической рептилии титанобоа. Фотография — не фотошоп и не подделка, однако подпись не соответствовала действительности, это был не скелет доисторического животного, а музейная скульптура из алюминия и нержавеющей стали. Также порой фактчекеры выделяют отдельный вердикт «сатирические новости», он означает, что информацию, придуманную заведомо сатирическим изданием, СМИ или спикеры выдают за настоящую. Такие ситуации часто случаются с публикациями ИА «Панорама».

При том, что линейке вердиктов полной правде обычно соответствует только один вердикт, обозначать полностью неправдивую новость может несколько вердиктов. Помимо собственно «Неправды» используются вердикты:

- «фейк» или «дезинформация» для обозначения намеренной дезинформации;

<sup>103</sup> Правда ли, что самка богомола после спаривания съедает самца?

<sup>104</sup> Что означают наши вердикты | Право на правду

<sup>105</sup> Правда ли, что на фото изображён скелет гигантской змеи титанобоа?

- «заблуждение» для обозначения широко распространённого неверного суждения, при этом облаченного в форму народной мудрости или общего знания (например, вера<sup>106</sup> в то, что существуют продукты с отрицательной калорийностью)
- а также яркий образный вердикт «pants on fire»<sup>107</sup>, используемый в проекте PolitiFact, для обозначения неприкрытой и абсурдной лжи.
- Также встречаются вердикты «верная атрибуция цитаты», «неверная атрибуция цитаты», «городская легенда», «миф», «мошенничество».

### Право на ошибку

Несмотря на принятые в рамках формата ограничения, фактчек не гарантирует стопроцентную точность и не берёт на себя функцию глашатая истины в последней инстанции. Человеческий фактор, некорректность исходных данных, новые данные, пусть и крайне редко, но могут привести к ошибке. Поэтому в рамках Международной сети фактчекеров<sup>108</sup> принято правило открытости и прозрачности внесения корректив в фактчекинговые материалы. В случае обнаружения неточности, меняющей восприятие проверки, или в случае ошибки, редакция обязуется внести корректировки, сохранив при этом первоначальную версию текста и обеспечив читателю доступ к информации об ошибке.

### Творческое задание

Объединитесь в команды не менее 4 человек. Вы — стартаперы-создатели нового фактчекерского проекта. Ваша задача составить собственную вердиктную линейку, где крайними полюсами будут правда и ложь.

Команда 1 должна выбрать для себя и обосновать четыре вердикта, команда 2 — шесть вердиктов, команда 3 (если достаточно участников) — семь и более вердиктов.

Время на выполнение задания 15 минут.

От каждой команды выступает один человек.

Время на презентацию: 7 минут для первой и второй команды, 10 минут для третьей.

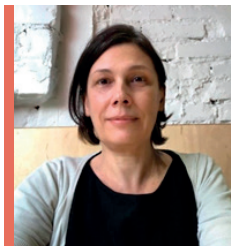
<sup>106</sup> Правда ли, что существуют продукты с отрицательной калорийностью?

<sup>107</sup> Английская идиома, соответствующая русскоязычной присказке «на лгунишке горят штанишки»

<sup>108</sup> International Fact-Checking Network - Poynter



## АВТОРЫ МОДУЛЯ:



### **ТАТЬЯНА ЧЕРНОБИЛЬ**

Юрист, независимый консультант по международному праву в области прав человека, специализируется на вопросах недискриминации, права на частную жизнь, права на справедливый суд, цифровым правам, международным механизмам защиты прав человека и другим.



### **ГУЛЬМИРА БИРЖАНОВА**

Юрист, соучредитель ОФ "Правовой медиа-центр". Эксперт в области национального и международного медиа-права. Участник Коалиции новое поколение правозащитников и член Экспертной группы по цифровым правам.



### **ДИАНА ОКРЕМОВА**

Журналист, директор Правового медиа-центра, член рабочих групп по доступу к информации, регулированию СМИ, интернета, защиты персональных данных. Является членом Экспертного совета по правам человека при Уполномоченном по правам человека в Казахстане, членом Национального совета заинтересованных сторон Министерства по инвестициям и развитию, экспертом ОБСЕ по правам человека.



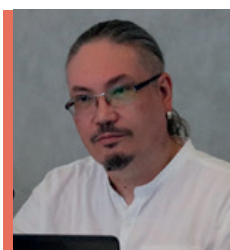
### **ОЛЬГА ДИДЕНКО**

Региональный консультант по медиазаконодательству Internews в Казахстане, участница рабочих групп по разработке законов «О средствах массовой информации», «О рекламе», «О телерадиовещании», «О доступе к информации».



### **ДАНА МУХАМЕДЖАНОВА**

Докторант PhD, заместитель директора Высшей школы права КазГЮУ имени М.С. Нарикбаева, директор филиала Digital Rights Center Qazaqstan в Нур-Султане региональный консультант по медиазаконодательству Internews в Казахстане



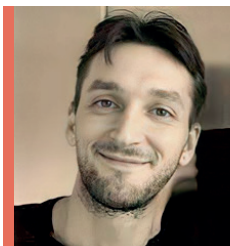
### **ДАНИЛА БЕКТУРГАНОВ**

Социолог, политолог, директор ОФ «Гражданская экспертиза», член Экспертной группы по цифровым правам.



### **ЕЛЖАН КАБЫШЕВ**

Руководитель ОФ "Digital Paradigm", менеджер проектов "Ландшафт цифровых прав и свобод" и "Internet Freedom", участник Экспертной группы по цифровым правам, Data Privacy Professional (GDPR DPP)



### **ПАВЕЛ БАННИКОВ**

Журналист, фактчекер, преподаватель медиаграмотности. С 2005 года репортёр, редактор и колумнист в казахстанских научно-популярных и общественно-политических изданиях. Главный редактор проекта factcheck.kz с 2017 по 2022 год. Составитель и редактор ряда исследовательских работ по языку вражды, методических пособий по журналистике, учебника по медиаграмотности для средних школ Республики Казахстан.


# Для заметок


A series of horizontal dotted lines for writing notes.



## ОФ «Правовой медиа-центр»


### Наши контакты:

 Казахстан, г. Астана, ул.Отырар, 15, офис 504

 8 (7172) 42-44-32

 E-mail: [mediastana@gmail.com](mailto:mediastana@gmail.com)

 [lmc.kz](http://lmc.kz)

 [lmc.kz](https://www.instagram.com/lmc.kz)

 [lmc.kz](https://www.facebook.com/lmc.kz)

 [lmc\\_kz](https://www.telegram.com/lmc_kz)