SOROS.KZ

ХЛЫНЦОВ АЛЕКСАНДР

ПРАВО НА ОНЛАЙН-АНОНИМНОСТЬ И ИСПОЛЬЗОВАНИЕ ШИФРОВАНИЯ В КАЗАХСТАНЕ

НОВОЕ
ПОКОЛЕНИЕ
ПРАВОЗАЩИТНИКОВ

Стипендиальный проект «Новое поколение правозащитников» Программы «Права человека» Фонда Сорос-Казахстан направлен на поиск и подготовку молодых правозащитников, способных разрабатывать качественные аналитические доклады и отчеты и готовых предпринять различные мониторинговые и адвокационные действия по оценке ситуации, связанные с защитой прав человека в Казахстане, с долгосрочной целью содействия становлению нового поколения правозащитников.

В рамках проекта участники проходят серию тренингов по основам защиты прав человека, подготовке мониторинговых исследований и разработке адвокационных стратегий. Полученные в рамках проекта знания и навыки участники используют при подготовке мониторинговых исследований и адвокационных планов по выбранным темам в сфере защиты прав человека.

SOROS.KZ

Публикация подготовлена при финансовой поддержке Фонда Сорос-Казахстан. Точка зрения авторов, отраженная в данном исследовании, может не совпадать с точкой зрения Фонда Сорос-Казахстан. Ответственность за факты, сведения, суждения и выводы, содержащиеся в публикации, несут авторы.

ОБ АВТОРЕ

ХЛЫНЦОВ АЛЕКСАНДР

Родился в городе Шахтинске в 1993 году. Получил среднее образование в школе № 9, затем высшее образование (2011-2015 гг.) по специальности «Геология и разведка месторождений полезных ископаемых» в КарГТУ.

Имеет интерес к правозащитной деятельности в направлении цифровых прав, трудовых прав и права на максимально достижимый уровень физического и психического здоровья.

I. ИССЛЕДОВАТЕЛЬСКИЙ ВОПРОС

Исследование посвящено изучению реализации права на неприкосновенность частной жизни и свободы выражения мнений в условиях внедрения сети Интернет во все аспекты повседневной жизни. В связи с этим встает вопрос приватности – обеспечения анонимности и использования средств шифрования, позволяющих добиться определенной степени конфиденциальности при пользовании интернетом.

ООН подчеркнула, что права, которыми обладает человек в обычной жизни, должны также защищаться и онлайн[1]. Соответственно, право на обеспечение анонимности в интернете и использование средств шифрования гарантируется на основании тех же прав, которые были изложены до массового распространения интернета в соответствующих документах о правах человека, таких как Всеобщая декларация прав человека.

Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободного выражения Дэвид Кайе в мае 2015 года на 29 Сессии по правам человека дал пояснение применению права на неприкосновенность частной жизни и свободу выражения мнений в интернете и выразил обеспокоенность растущей неизбирательной слежкой правительств стран мира и международных корпораций за пользователями в сети, а также запретами на использование средств шифрования и самой возможности анонимного пользования интернетом[2].

Докладчик осудил такие практики правительств, 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.

1. Резолюция, принятая Советом по правам человека 23 марта 2017 года, A/HRC/RES/34/7: https://undocs.org/ru/A/HRC/RES/34/7

2. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кайе, A/HRC/29/32, 22 мая 2015 г.: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/87/PDF/G1509587.pdf?OpenElement

Данное исследование представит характеристику ситуации с правами на анонимность и использование средств шифрования в Республике Казахстан, а также даст рекомендации для сохранения баланса между необходимостью обеспечения безопасности и реализацией свобод, гарантированных правами человека.

II. ЦЕЛИ ИССЛЕДОВАНИЯ

Конечная цель исследования: предоставление рекомендаций для государства и гражданского общества Казахстана, основанных на международном законодательстве, которые направлены на эффективную защиту прав на анонимность и использование средств шифрования. Перед этим будет проведено исследование международного законодательства. Предоставленные рекомендации и выявленные случаи нарушения международного права человека могут быть использованы для дальнейшего адвокатирования рассматриваемого права.

Рекомендации, предоставленные специальным докладчиком ООН по вопросу о поощрении и защите права на свободу мнений и их свободного выражения Дэвидом Кайе, на данный момент являются наиболее полными и подробными в рамках рассматриваемой темы, а также наиболее актуальными для Казахстана.

На основе рекомендаций из доклада Дэвида Кайе можно вывести следующие индикаторы соблюдения рассматриваемого права:

1. Государство на законодательном уровне признает и уважает право каждого на анонимность в интернете и использование средств шифрования и поощряет безопасность и конфиденциальность онлайн путем информирования общественности.

В первую очередь важно добиться признания от государства важности права на анонимность и возможности использования средств шифрования. Необходимо, чтобы государство признавало за каждым гражданином его право беспрепятственно пользоваться средствами шифрования и анонимизации, не заставляло принудительно каждого деанонимизировать себя для пользования сервисами интернета. Также будет немаловажным государству популяризировать среди граждан цифровую грамотность и средства обеспечения приватности, навыки безопасного использования интернета, распоряжения своими персональными данными для предотвращения случаев мошенничества, кибербуллинга и иных правонарушений.

2. Любые ограничения анонимности и шифрования в интернете соответствуют принципам международного права и применяются исключительно на индивидуальной основе и в соответствии с требованиями законности, необходимости, соразмерности и правомерности их цели и только с санкции суда.

Осуществление надзора должно применяться только к конкретным лицам и организациям, надзор за которыми санкционирован судом. Соответственно, санкции суда на осуществление надзора в отношении каждого лица или организации должны удовлетворять требованиям необходимости, правомерности, законности и соразмерности. Неизбирательный надзор за

всеми пользователями интернета в стране, а также надзор без санкции суда не должны осуществляться, так как, помимо нарушения приватности, такие действия могут мешать свободе выражения мнений.

3. Любые новые законы, которые могут ограничить анонимность в интернете и использование средств шифрования, подлежат публичному обсуждению с участием широкого круга представителей гражданского общества и не вводятся с помощью ускоренных законодательных процедур.

Принятие подобных законов не должно осуществляться без обсуждения и в ускоренном порядке. Необходимо взвесить все риски для прав человека подобных законов и регламентов государственных органов. Законы в государстве в целом должны предоставлять возможность и поощрять сохранение приватности пользователей.

4. Государство отказывается от ограничений анонимности и использования средств шифрования, носящих абсолютный, неизбирательный характер: принудительного снижения стандартов безопасности, ограничения на законодательном уровне анонимного общения онлайн, требований обязательной регистрации сим-карт, мобильных средств связи для доступа к услугам интернета, блокирования доступа к услугам средств шифрования (VPN, Tor, Proxy и т.д.), требований использования внутренних серверов для сайтов с национальным доменом .kz, требований компаниям хранить личные данные исключительно на серверах внутри страны, требований аутентификации пользователей при пользовании публичными точками доступа к интернету (Wi-Fi) и других подобных ограничений.

Так как надзор, сопряженный с деанонимизацией и дешифрованием, должен осуществляться только на индивидуальном уровне, с санкции суда, удовлетворяющей требованиям законности, правомерности и соразмерности, то недопустимо осуществление надзора неизбирательного характера, а также ограничения возможности пользоваться средствами шифрования и анонимного пользования интернетом. Поэтому все законы и требования, которые направлены на принудительное снижение стандартов безопасности, ограничение или запрет возможности использовать средства шифрования, прямой запрет анонимного размещения информации в интернете, должны быть отменены. Подобные законы и требования не только нарушают право на неприкосновенность частной жизни, но и создают препятствия свободному выражению мнений.

III. МЕТОДОЛОГИЯ

1. Анализ национального законодательства.

   Сравнение текущего состояния законодательства с договорами в сфере прав человека.

2. Подача запросов в государственные органы.

   Выяснить добросовестность исполнения международных договоров: проводилось ли обсуждение новых законов с гражданской общественностью Казахстана, не использовались ли ускоренные процедуры и т.д.

3. Мониторинг СМИ.

   Сбор данных из средств массовой информации о заявлениях правительственных лиц, касающихся права на анонимность, действий государства и операторов сети Интернет.

4. Интервью с экспертом.

   Провести экспертное интервью о существующих законах и практиках в Казахстане, касающихся права на анонимность, их потенциального вреда для гражданского общества и налогоплательщиков.

5. Опрос.

   Проведение опроса с целью выяснить, с какими проблемами сталкиваются пользователи интернета в Казахстане при применении средств шифрования, при анонимном использовании интернета и устройств с доступом в интернет, а также узнать отношение пользователей к проводимым в государстве практикам.

IV. АНАЛИЗ МЕЖДУНАРОДНЫХ СТАНДАРТОВ И ЗАРУБЕЖНОЙ ПРАКТИКИ

В связи с внедрением новых технологий, таких как интернет, появляются новые возможности выражать свое мнение и получать информацию, но в то же время у правительств и иных структур (корпораций, незаконных формирований) появляются способы, используя уязвимость и преимущества современных технологий, проводить массовую слежку за населением, осуществлять сбор и распоряжаться конфиденциальной информацией по своему усмотрению. В связи с этим ООН, а также правозащитные организации, такие как Human Rights Watch, призывают правительства пересмотреть свое законодательство, а также практические действия, касающиеся сбора личных данных, слежки за сообщениями, обеспечения защиты личной информации и т.д., для того чтобы предотвратить нарушения прав человека[3].

Также ООН и правозащитные организации рекомендуют правительствам не препятствовать возможности легально использовать средства шифрования (сеть Tor, VPN, прокси-сервера), сохранять анонимность (не раскрывать своего имени, не выдавать информацию, позволяющую с точностью идентифицировать личность) при общении в интернете. Это важно для сохранения возможности беспрепятственно выражать свое мнение, пользоваться интернетом для реализации других прав человека на условиях неприкосновенности частной жизни. ООН признает, что права, которыми человек обладает в обычной жизни, должны также защищаться и в виртуальной среде[4].

Право на анонимность в интернете традиционно связано с правом на неприкосновенность частной жизни и свободу выражения мнений.

Право на неприкосновенность частной жизни защищается статьей 12 Всеобщей декларации прав человека:

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.

3. Статья UN: Online Anonymity, Encryption Protect Rights: https://www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights

4. Утверждения из первых 2-х абзацев основаны на статье под ссылкой 1, Резолюции, принятой Советом по правам человека 23 марта 2017 года, A/HRC/RES/34/7: https://undocs.org/ru/A/HRC/RES/34/7 , а также на докладе под ссылкой 3.

Также это право нашло свое юридическое закрепление в Международном пакте о гражданских и политических правах (статья 17):

1. *Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию.*
2. *Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.*

Это право защищается также такими международными документами, как Конвенция о правах ребенка (статья 16), Конвенция о правах инвалидов (статья 22), Конвенция о защите прав всех трудящихся-мигрантов и членов их семей (статья 14) (тексты этих статей во многом дублируют текст Статьи 17 Международного пакта о гражданских и политических правах), а также региональными Европейской конвенцией по правам человека (статья 8) и Американской конвенцией о правах человека (статья 11).

Статья 8 Европейской конвенции по правам человека:

1. *Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.*
2. *Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц.*

Статья 11 Американской конвенции о правах человека:

1. *Каждый имеет право на уважение его чести и признание его достоинства.*
2. *Никто не может быть объектом произвольного и оскорбительного вмешательства в его личную жизнь, жизнь его семьи, нарушения неприкосновенности его жилища или тайны его корреспонденции или незаконных нападок на его честь и репутацию.*
3. *Каждый имеет право на защиту закона от таких вмешательств, нарушений и нападок.*

Свобода выражения мнения защищается статьями следующих международных и региональных документов: 19 статьей Всеобщей декларации прав человека, 19 статьей Международного пакта о гражданских и политических правах, статьей 9 Африканской хартии прав человека и народов, статьей 13

Американской конвенции о правах человека и статьей 10 Европейской конвенции по правам человека.

Статья 19 Всеобщей декларации прав человека:

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.

Статья 19 Международного пакта о гражданских и политических правах:

1. *Каждый человек имеет право беспрепятственно придерживаться своих мнений.*
2. *Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору.*
3. *Пользование предусмотренными в пункте 2 настоящей статьи правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:*

   a) для уважения прав и репутации других лиц;

   b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

Статья 9 Африканской хартии прав человека и народов:

1. *Каждый человек имеет право получать информацию.*
2. *Каждый человек имеет в рамках закона право выражать и распространять свое мнение.*

В мае 2015 года на 29 сессии Совета по правам человека специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободного выражения Дэвид Кайе представил свой отчет о шифровании, анонимности и структуре прав человека.

В своем первом докладе Совету по правам человека Специальный докладчик затрагивает два взаимосвязанных вопроса: во-первых, защищают ли права на неприкосновенность частной жизни и свободу мнений и их выражения безопасное онлайн-общение, особенно с помощью шифрования или

анонимности. И, во-вторых, при условии положительного ответа, в какой степени правительства в соответствии с законодательством о правах человека могут вводить ограничения на шифрование и анонимность[5].

Докладчик также осудил практики, к которым прибегают государства, чтобы ограничить анонимность в интернете и возможности шифрования, такие 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.

Докладчик дал рекомендации государствам:

1. Пересмотреть законы для поощрения и защиты прав на неприкосновенность частной жизни и свободу выражения мнений.
2. Проводить политику неограничения и всесторонней защиты шифрования и анонимности, применяя ограничения только на индивидуальной основе и в соответствии с требованиями законности, необходимости, соразмерности и правомерности их цели.
3. Проводить публичные обсуждения с участием широкого круга представителей гражданского общества и групп меньшинств при пересмотре или принятии законодательных предложений об ограничении анонимности и шифрования.
4. Поощрять использование надежных средств шифрования и анонимности.
5. Отказаться от любых мер, снижающих степень безопасности частных лиц в онлайн-среде, в том числе от удаленного скрытого администрирования, низких стандартов шифрования и систем депонирования ключа. Кроме того, государствам следует воздержаться от введения

5. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кайе, A/HRC/29/32, 22 мая 2015 г.: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/87/PDF/G1509587.pdf?OpenElement [последний доступ 31.03.19]

требований, при которых обязательным условием для доступа к электронным сообщениям или онлайн-услугам являлась бы идентификация пользователей или которые предусматривали бы регистрацию сим-карты владельцев мобильных телефонов.

В докладе Специального докладчика по свободе выражения мнений за 2013 год подчеркивается важное значение взаимосвязи между правами на неприкосновенность частной жизни и свободы выражения мнений в киберпространстве[6]. В докладе также отмечается, что ограничения на анонимность облегчают слежку за коммуникациями государств и оказывают воздействие на возможность выражения мнений и идей.

Некоторые возможности, которые защищают право на анонимность, появились на основе решений Совета Европы и Европейского союза[7]. Комитет министров Совета Европы принял Декларацию о свободе общения в Интернете в мае 2003 года. Принцип 7 декларации гласит: *«В целях обеспечения защиты Интернета от контроля и расширения свободного выражения идей и информации государства-члены должны уважать желание пользователей Интернета не раскрывать свою личность. Это не мешает государствам-членам принимать меры и осуществлять сотрудничество в целях установления лиц, виновных в преступных деяниях, в соответствии с национальным законодательством, Конвенцией о защите прав человека и основных свобод и другими международными соглашениями между правоохранительными органами и органами юстиции».*

В своей судебной практике Европейский суд по правам человека (ЕСПЧ) признает важность анонимности для прав на свободу выражения и конфиденциальность. В то же время суду было ясно, что анонимность не является абсолютной и может быть ограничена для защиты других законных интересов, особенно защиты уязвимых групп населения. В частности, он заявил, что анонимность и конфиденциальность в интернете не должны заставлять государства отказываться от защиты прав потенциальных жертв, особенно в отношении уязвимых лиц[8].

Хотя свобода слова и конфиденциальность связи являются основными соображениями и пользователи интернета должны иметь гарантию того, что их собственная конфиденциальность и свобода выражения будут уважаться, такая гарантия не может быть абсолютной и должна иногда уступать другим законным целям, таким как предотвращения беспорядков, преступлений или защита прав и свобод других лиц[9].

6. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю, A/HRC/23/40, 17 апреля 2013 г.: https://undocs.org/ru/A/HRC/23/40 [последний доступ 31.03.2019]

7. RECOMMENDATION No R (99) 5 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES FOR THE PROTECTION OF PRIVACY ON THE INTERNET: https://www.refworld.org/pdfid/3dde380a4.pdf [последний доступ 31.03.19]

8. Дело K.U. v. FINLAND (no.2872/02), Совет Европы, 2 декабря 2008: http://www.adae.gr/fileadmin/docs/nomoi/Eyropaiki_Enosi/KU_v._Finland.pdf [последний доступ 31.03.19]

9. Пояснительная записка Совета Европы по свободе выражения мнений и информации, 18 пункт: https://www.coe.int/en/web/freedom-expression/freedom-of-expression-and-information-explanatory-memo [последний доступ 31.03.19]

ОБСЕ также подтверждает, что право на свободу выражения мнений универсально для обычного и онлайн-общения, а любое ограничение свободы выражения мнений, в том числе и в интернете, должно соответствовать международным стандартам и нормам[10].

Совет по правам человека на 28 сессии в 2014 году по итогам дискуссии пришел к выводам о том, что необходимо более действенное соблюдение международных норм о праве на неприкосновенность частной жизни на уровне государств. Также несколько делегаций в этом обсуждении призвали государства пересмотреть практику и процедуры наблюдения за связью, перехвата сообщений и сбора личных данных с целью приведения законодательства в соответствие с международными нормами и требованиями нового века[11].

10. Отчет «Свобода выражения мнений в Интернете: Исследование правовых норм и практик, связанных со свободой выражения мнения, свободным потоком информации и плюрализмом СМИ в Интернете в государствах-участниках ОБСЕ», 2011 г.: https://www.osce.org/ru/fom/89063?download=true [п.д. 31.03.19]

11. Совет по правам человека, Резюме обсуждения на дискуссионном форуме вопроса о праве на неприкосновенность частной жизни в цифровой век, A/HRC/28/39: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39&Lang=R [п.д. 31.03.19]

V. АНАЛИЗ НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Для выяснения соответствия национального законодательства международным договорам и рекомендациям специальных процедур ООН мы проведем сравнение законов РК с индикаторами, составленными на основе рекомендаций специального докладчика ООН.

1. Государство на законодательном уровне признает и уважает право каждого на анонимность в интернете и использование средств шифрования и поощряет безопасность и конфиденциальность онлайн путем информирования общественности.

Право на неприкосновенность частной жизни в Казахстане защищено статьей 18 Конституции РК:

«1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства.

2. Каждый имеет право на тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничения этого права допускаются только в случаях и в порядке, прямо установленных законом.

3. Государственные органы, общественные объединения, должностные лица и средства массовой информации обязаны обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации».

Статья Конституции 20 п. 2 говорит: «Каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом. Перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом».

Статья 144 Гражданского Кодекса РК «Право на охрану тайны личной жизни» указывает на то, что:

«1. Гражданин имеет право на охрану тайны личной жизни, в том числе тайны переписки, телефонных переговоров, дневников, заметок, записок, интимной жизни, усыновления, рождения, врачебной, адвокатской тайны, тайны банковских вкладов.

Раскрытие тайны личной жизни возможно лишь в случаях, установленных законодательными актами.

2. Опубликование дневников, записок, заметок и других документов допускается лишь с согласия их автора, а писем – с согласия их автора и адресата.

В случае смерти кого-либо из них указанные документы могут публиковаться с согласия пережившего супруга и детей умершего».

Однако законов, которые бы гарантировали возможность применения средств шифрования и обеспечение анонимности в интернете с целью реализации конституционных прав в онлайн-среде, не существует. Но статья 36 пункт 5-1 закона «Об информатизации» запрещает анонимное комментирование путем обязательства владельцев электронных ресурсов заключать с читателями письменные соглашения с использованием ЭЦП или sms-идентификации, что идет вразрез с уважением к праву быть анонимным в сети Интернет, а также допускает иные вмешательства.

2. Любые ограничения анонимности и шифрования в интернете соответствуют принципам международного права и применяются исключительно на индивидуальной основе и в соответствии с требованиями законности, необходимости, соразмерности и правомерности их цели и только с санкции суда.

В Казахстане ведение специальных оперативно-розыскных мероприятий, включающих в себя перехват личных сообщений в режиме реального времени, согласно закону «Об оперативно-розыскной деятельности» может осуществляться исключительно с санкции прокурора и только в целях выявления, предотвращения и пресечения преступлений, за которые санкция предусматривает лишение свободы на один год или более, или преступлений, совершенных преступной группой[12].

Новый технический регламент «Общие требования к телекоммуникационному оборудованию по обеспечению проведения оперативно-розыскных мероприятий, сбора и хранения служебной информации об абонентах», разработанный КНБ и вступивший в силу в январе 2018 года, предоставляет правительству постоянный доступ к сетям операторов без уведомления оператора об использовании сети для следственно-розыскных мероприятий[13]. Это может негативно сказаться на свободе выражения мнений и приватности пользователей, так как государству не нужно предъявлять оператору особых или периодических требований для получения персональных данных пользователей[14].

12. Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности»: https://online.zakon.kz/document/?doc_id=1003158#pos=228;-46

13. Об утверждении технического регламента «Общие требования к телекоммуникационному оборудованию по обеспечению проведения оперативно-розыскных мероприятий, сбора и хранения служебной информации об абонентах»: https://tengrinews.kz/zakon/komitet_natsionalnoy_bezopasnosti_respubliki_kazahstan/natsionalnaya_bezopasnost/id-V1600014680/

14. Взгляд Telia company на новые правила наблюдения («прямого доступа») в Казахстане: https://www.teliacompany.com/en/news/news-articles/2017/freedom-of-expression-kazakhstan/

3. Любые новые законы, которые могут ограничить анонимность в интернете и использование средств шифрования, подлежат публичному обсуждению с участием широкого круга представителей гражданского общества и не вводятся с помощью ускоренных законодательных процедур.

До настоящего момента в Казахстане не вводились законы, которые бы регламентировали особый порядок рассмотрения новых законопроектов, которые могут потенциально ограничить анонимность в интернете и использование средств шифрования. Обсуждение данных законопроектов происходит на общем основании.

4. Государство отказывается от ограничений анонимности и использования средств шифрования, носящих абсолютный, неизбирательный характер, — принудительного снижения стандартов безопасности, ограничения на законодательном уровне анонимного общения онлайн, требований обязательной регистрации сим-карт, мобильных средств связи для доступа к услугам интернета, блокирования доступа к услугам средств шифрования (VPN, Tor, Proxy и т.д.), требований использования внутренних серверов для сайтов с национальным доменом .kz, требований компаниям хранить личные данные исключительно на серверах внутри страны, требований аутентификации пользователей при пользовании публичными точками доступа к интернету (Wi-Fi) и других подобных ограничений.

В докладе Дэвида Кайе были перечислены следующие практики государств, которые нарушают право на анонимность и использование средств шифрования:

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.

Проверим законодательство Казахстана на наличие подобных практик.

1. Запрет на индивидуальное использование технологий шифрования и борьба с применением средств шифрования.

Решением неназванного суда от 10 сентября 2014 года было запрещено использование сайтов и сетей (анонимайзеры), которые позволяют обходить блокировки[15].

Также в 2018 году был прецедент блокировки сервиса VPN – IPVanish, так как он «используется для обхода технических возможностей операторов связи, применяемых для нераспространения в стране незаконных материалов»[16].

Согласно подпунктам 1-3 пункта 1 статьи 41-1 закона «О связи» запрещается работа сетей и (или) средств связи, оказание услуг связи, доступ к интернет-ресурсам и (или) размещенной на них информации в целях доступа к информации, запрещенной вступившими в законную силу решением суда или законами Республики Казахстан[17].

Под определение сервисов и сайтов, позволяющих обходить блокировки, применяемые для нераспространения в стране незаконных материалов, подпадают любые средства шифрования и анонимизации, такие как VPN, прокси-сервера или сети TOR, I2P, что дает возможность блокировать подобные средства шифрования и резко ограничить их использование в стране.

2. Намеренное понижение степени эффективности шифрования.

В стране неоднократно были осуществлены попытки внедрения национального сертификата безопасности, который потенциально позволяет получить государственным службам доступ ко всему зашифрованному трафику пользователей, его установивших[18]. Внедрение сертификата основывается на статье 26 закона «О связи» и пункте 11 «Правил выдачи и применения сертификата безопасности».

Согласно 26 статье закона «О связи»: «Операторы междугородной и (или) международной телефонной связи обязаны осуществлять пропуск трафика с использованием протоколов, поддерживающих шифрование с применением сертификата безопасности, за исключением трафика, шифрованного средствами криптографической защиты информации на территории Республики Казахстан».

15. Анонимайзеры вне закона: https://www.zakon.kz/4718754-anonimajjzery-vne-zakona.-kazakhstancev.html

16. По решению суда в Казахстане заблокирован VPN-сервис: https://profit.kz/news/45100/Po-resheniu-suda-v-Kazahstane-zablokirovan-VPN-servis/

17. О связи. Статья 41-1. Порядок приостановления работы сетей и (или) средств связи: https://kodeksy-kz.com/ka/o_svyazi/41-1.htm

18. Что такое сертификат Qaznet и безопасен ли он: https://factcheck.kz/glavnoe-en/chto-takoe-sertifikat-qaznet-i-bezopasen-li-on/

Согласно пункту 11 «Правил выдачи и применения сертификата безопасности»: «Операторы связи обеспечивают распространение сертификата безопасности среди своих абонентов, с которыми заключены договоры на оказание услуг связи».

По словам вице-министра цифрового развития РК Аблахана Оспанова, установка сертификата пользователями производится на добровольной основе и законодательство не обязывает их это делать[19].

Однако сами действия государства, такие как создание сертификата и попытка его внедрения, без необходимого информирования общественности о том, что он позволяет вести неизбирательный надзор и тем самым ограничивать возможность быть анонимным и снижать степень эффективности шифрования, – это действия, которые могут привести к нарушениям права человека на неприкосновенность частной жизни.

3. Депонирование ключей.

Депонирование ключей шифрования – передача для учета и хранения ключей шифрования в специализированный центр, созданный государством.

Правила депонирования средств криптографической защиты информации в Казахстане, установленные приказом Председателя КНБ РК от 22 июня 2001 года[20], в данный момент отменены в соответствии с планом мероприятий по реализации Концепции совершенствования разрешительной системы в Республике Казахстан на 2009-2011 годы, согласно приказу Председателя Комитета национальной безопасности РК от 09.06.2009 N 103[21]. В настоящий момент законодательство не обязывает к депонированию ключей.

4. Обязательное раскрытие ключа по сравнению с адресными распоряжениями о расшифровке данных.

В данный момент не существует законов, которые бы обязывали раскрывать ключ шифрования вместо адресной расшифровки данных.

5. Запрет анонимных высказываний в интернете.

Согласно статье 36 пункту 5-1 закона «Об информатизации»: «*Оказание собственником или владельцем общедоступного электронного информационного ресурса услуги по размещению пользователем информации осущест-*

19. Зачем необходимо устанавливать сертификаты безопасности на абонентские устройства: https://www.inform.kz/ru/zachem-neobhodimo-ustanavlivat-sertifikaty-bezopasnosti-na-abonentskie-ustroystva_a3549199

20. Об утверждении правила депонирования средств криптографической защиты информации в Казахстане: https://egov.kz/cms/ru/law/list/V010001601_

21. О признании утратившим силу приказа Председателя КНБ РК от 22 июня 2001 года: https://egov.kz/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjc7PyChKtUvKTS3NT80r0w_Wj9KNgPM8U_UhHA0tvPwMDQ3NjI5BUTmJeemlieqp-ZFGpfkFurkW5o6IiAF0slXc!/#z2

вляется на основании соглашения, заключаемого в письменной форме (в том числе электронной), с использованием идентификации на портале «электронного правительства» или посредством зарегистрированного на общедоступном информационном электронном ресурсе абонентского номера сотовой связи пользователя путем отправления короткого текстового сообщения, содержащего одноразовый пароль для заключения соглашения».

Таким образом, владельцы электронных ресурсов Казахстана обязаны адаптировать свой сайт так, чтобы комментирование на нем было возможно только при аутентификации через ЭЦП или SMS-подтверждение, что не позволяет оставлять комментарии анонимно, без передачи персональных данных сайту.

По заявлениям МИК РК, ведется мониторинг на наличие данного механизма на сайтах Казахстана[22]. В случае отсутствия механизма на сайте владельцы ресурсов получают предписание в порядке 462-й статьи Административного кодекса РК, наказанием за нарушение которой является штраф в размере до 500 МРП.

Это является прямым запретом анонимных высказываний в интернете, что не соответствует рекомендациям специального докладчика.

6. Законы об обязательной регистрации сим-карт и мобильных устройств под настоящим именем для доступа в Интернет.

Согласно «Правилам оказания услуг доступа к сети Интернет» предоставление абоненту доступа к сети Интернет осуществляется только после заключения договора в письменном виде и с указанием сведений об абоненте (для юридических лиц – бизнес-идентификационный номер, данные свидетельства о постановке на учет по налогу на добавленную стоимость; для физических лиц – телефонные номера, идентификационные коды, адреса электронной почты, почтовый адрес, индивидуальный идентификационный номер) с приложением копий перечисленных документов[23].

В то же время предоставление услуг связи по незарегистрированным SIM-картам не может осуществляться с 1 декабря 2014 года в связи с требованиями Министерства по инвестициям и развитию РК[24].

Согласно закону «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам противодействия экстремизму и терроризму» от 22 декабря 2016 года пользователи мобильных телефонов должны зарегистрировать IMEI устройства на свое имя. Услуги связи, согласно зако-

22. МИК РК не будет наказывать интернет-ресурсы за анонимные комментарии до конца марта: https://informburo.kz/novosti/v-mik-rk-rasskazali-kogda-nachnut-nakazyvat-internet-resursy-za-anonimnye-kommentarii.html

23. Правила оказания услуг доступа к сети Интернет от 30 декабря 2011 года № 1718: http://www.adilsoz.kz/acts/show/id/41

24. Регистрация номера: https://activ.kz/ru/news/2685

ну, оператору запрещается предоставлять без регистрации IMEI мобильного устройства абонента[25].

В данный момент правила доступа к общественным точкам Wi-Fi регулируются приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171 «Об утверждении правил оказания услуг связи»[26]. Параграф 2. «Оказание услуг доступа к Интернету в пунктах общественного доступа к Интернету» в Правилах оказания услуг доступа к Интернету обязывает проводить аутентификацию через SMS-пароль для использования сети Wi-Fi:

40. Авторизация пользователя завершается при вводе им одноразового персонального идентификатора (пароля), полученного в SMS-сообщении, в поле «Пароль» специальной формы и пользователю предоставляется доступ к Интернету.

Запрет использовать сим-карты без регистрации, принуждение к аутентификации в общественных точках Wi-Fi через SMS-пароль, а также запрет операторам предоставлять услуги связи без регистрации мобильных телефонов и иных мобильных устройств серьезно ограничивают возможности анонимно пользоваться сетью Интернет для свободного выражения мнений.

7. Политика обязательного хранения данных внутри страны и фиксация деятельности всех пользователей страны в интернете.

Правила оказания услуг доступа к сети Интернет от 30 декабря 2011 года № 1718 также обязывают операторов связи и интернет-провайдеров хранить пользовательские данные, включая номера телефонов, платежные данные, IP-адреса, историю просмотров, протоколы передачи данных и другие данные в течение двух лет и предоставлять доступ в течение 24 часов оперативно-следственным органам, таким как КНБ, с санкции прокурора.

Технический регламент, разработанный КНБ и вступивший в силу в январе 2018 года, предоставляет правительству доступ в реальном времени к сетям операторов, а также требует от операторов устанавливать оборудование, которое бы могло обеспечить сбор и хранение данных пользователей[27].

По статье 36 пункту 5-1 Закона «Об информатизации»: собственник или владелец электронного информационного ресурса обязан хранить информацию, используемую при заключении соглашения, весь период действия, а также в течение трех месяцев после расторжения соглашения.

25. О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам противодействия экстремизму и терроризму: https://online.zakon.kz/document/?doc_id=34199995#pos=403;-54

26. Приказ и. о. Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171 «Об утверждении правил оказания услуг связи»: https://online.zakon.kz/document/?doc_id=39350222&doc_id2=37844864#activate_doc=2&pos=2;-98&pos2=159;-76

27. «Общие требования к телекоммуникационному оборудованию по обеспечению проведения оперативно-розыскных мероприятий, сбора и хранения служебной информации об абонента»: https://tengrinews.kz/zakon/komitet_natsionalnoy_bezopasnosti_respubliki_kazahstan/natsionalnaya_bezopasnost/id-V1600014680/

Сбор информации и постоянное неизбирательное наблюдение позволяют легче раскрывать цифровой след каждого пользователя интернета в стране, что снижает эффективность средств шифрования, а также ограничивает право на неприкосновенность частной жизни. Само существование подобных баз данных создает риски хакерских атак и утечек персональных данных.

Согласно «Правилам регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета» регистрация домена kz стала возможна лишь при наличии сервера на территории Казахстана[28].

Статья 12 закона «О персональных данных и их защите» обязывает владельцев местных компаний хранить собираемые личные данные внутри страны[29].

Сбор данных и размещение сайтов исключительно внутри страны ограничивает возможность для пользователей интернета выбора места хранения своих персональных данных в электронном виде и облегчает возможность противоправного получения государственными органами данных, которые впоследствии могут быть использованы для деанонимизации пользователей интернета.

Как мы можем видеть, большинство рекомендаций специального докладчика ООН Давида Кайе не выполняются в Казахстане на законодательном уровне. Существующие законы прямо противоречат большей части данных рекомендаций. Большая часть законов, противоречащих рекомендациям спецдокладчика, была введена в последние 5 лет с 2015 года, когда доклад был впервые опубликован, что говорит в пользу предположения об игнорировании этих рекомендаций правительством.

28. Правила регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета»: https://tengrinews.kz/zakon/pravitelstvo_respubliki_kazahstan_premer_ministr_rk/hozyaystvennaya_deyatelnost/id-V1800016654/#z6

29. Закон о персональных данных и их защите: https://online.zakon.kz/Document/?doc_id=31396226#pos=3;-180

VI. МОНИТОРИНГ СМИ

Рассмотрим сообщения в казахстанских СМИ, касающиеся следующих видов ограничения права на анонимность и использование средств шифрования:

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.

1. Запрет на индивидуальное использование технологий шифрования и борьба со средствами обеспечения шифрования.

Решением неназванного суда от 10 сентября 2014 года было запрещено использование сайтов и сетей (анонимайзеры), которые позволяют обходить блокировки[30].

«Запретить функционирование сетей и (или) средств связи, используемых в целях обхода технических возможностей операторов связи, применяемых для прекращения распространения на территории Казахстана продукции иностранных средств массовой информации», – сказано в решении суда.

Председатель Комитета связи, информатизации и информации министерства по инвестициям и развитию РК Сакен Сарсенов сообщил, что в этой связи проводится работа по поиску и ограничению доступа интернет-ресурсов, используемых для обхода технических возможностей операторов связи, применяемых для прекращения распространения на территории РК запрещенной информации.

Также в 2018 году был прецедент блокировки сервиса VPN – IPVanish, так как он «используется для обхода технических возможностей операторов связи, применяемых для нераспространения в стране незаконных материалов»[31].

30. Анонимайзеры вне закона: https://www.zakon.kz/4718754-anonimajjzery-vne-zakona.-kazakhstancev.html

31. По решению суда в Казахстане заблокирован VPN-сервис: https://profit.kz/news/45100/Po-resheniu-suda-v-Kazahstane-zablokirovan-VPN-servis/

«Так, в соответствии с решениями Есильского районного суда Астаны, а также районного суда № 2 Ауэзовского района Алматы о запрете функционирования сетей и средств связи, используемых в целях обхода технических возможностей операторов связи, применяемых для прекращения распространения на территории РК продукции иностранных средств массовой информации, министерством было принято решение об ограничении доступа к интернет-ресурсу IPVanish и его внутренним поддоменам», — говорится в ответе Даурена Абаева.

Могут ли в Казахстане технически заблокировать VPN, рассказали в Государственной технической службе КНБ.

«Технически эта возможность есть. Ключевое слово – технически. Блокировка происходит только по деструктивным страницам и контенту. Если будет решение суда или предписание уполномоченного органа, то VPN будет блокироваться. Если не будет, то значит – нет», – сказал заместитель директора ГТС КНБ Зекен Исмаилов, отвечая на вопросы журналистов на брифинге СЦК[32].

По словам Болата Тынымбаева, эксперта в области информационной безопасности: *«Сейчас жители Казахстана все чаще жалуются, что VPN-сервисы также блокируют. Как это происходит: составляется список всех ip-адресов, принадлежащих VPN-сервису, и добавляется в черный список. Блокировка VPN-сервисов может выполняться по сетевым портам. Помимо этого, для блокировки может быть применена техника DPI (deep packet inspection) — технология дорогостоящая, но уже используемая отдельными операторами. Суть технологии в накоплении статистических данных, проверке и фильтрации сетевых пакетов по их содержимому»*[33].

Официальный сайт проекта Tor временно недоступен в Казахстане. Согласно общедоступным данным о его использовании в 2016 году произошло резкое сокращение пользователей «ретрансляторов» Tor и резкое увеличение пользователей, подключающихся через «мосты», которые чаще используются при блокировке IP-адресов реле Tor[34].

2. Намеренное понижение степени эффективности шифрования.

В стране неоднократно были осуществлены попытки внедрения национального сертификата безопасности, который потенциально позволяет получить государственным службам доступ ко всему зашифрованному трафику пользователей, его установивших[35].

Первая попытка внедрить аналогичный сертификат была в 2015 году. Тогда он был отклонен Mozilla, причем по тем же концептуальным причинам, что

32. Могут ли в блокировать VPN в Казахстане: https://tengrinews.kz/kazakhstan_news/mogut-li-blokirovat-VPN-v-kazahstane-374932/

33. Эксперт по информбезопасности — о Telegram, VPN и киберщите: https://www.the-village.kz/village/city/safe-internet/1673-big-brother-is-watching-you

34. See Tor website: Censorship by country: Kazakhstan: https://trac.torproject.org/projects/tor/wiki/doc/OONI/censorshipwiki/CensorshipByCountry/Kazakhstan#a20348

35. Что такое сертификат Qaznet и безопасен ли он: https://factcheck.kz/glavnoe-en/chto-takoe-sertifikat-qaznet-i-bezopasen-li-on/

описаны выше, главная — «человек посередине». Mozilla позиционирует себя как компания, в первую очередь заботящаяся о конфиденциальности пользователей, и такое нарушение конфиденциальности для нее неприемлемо.

17-18 июля 2019 года абонентам мобильных операторов Казахстана было разослано сообщение о том, что всем «необходимо» установить национальный сертификат безопасности с сайта http://qca.kz. В противном случае операторы предупреждают о возможных проблемах с выходом в интернет. Установить тот же самый сертификат операторы связи призывали еще в марте этого года, однако тогда они ограничились сообщениями на сайтах.

Комитет национальной безопасности Казахстана заявил о завершении 7 августа 2019 года «тестирования сертификата безопасности». Президент Казахстана Касым-Жомарт Токаев поблагодарил КНБ за работу. Все это происходило на фоне массовой критики самой технологии Qaznet Trust Network и ее введения. Официально сообщили, что испытания закончены, все поставленные в ходе пилота задачи успешно решены. Установившие национальный сертификат могут его удалить, так как он больше не понадобится. Необходимость его установки может возникнуть в случаях усиления цифровой границы государства в рамках особого регламента[36].

Согласно заявлению, размещенному в официальном телеграм-канале ЦАРКА, властям удалось реализовать инспектирование трети всего трафика столицы[37].

3. Запрет анонимных высказываний в интернете.

В декабре 2017 года правительство приняло новые поправки, которые требуют от пользователей, желающих комментировать на местных веб-сайтах, регистрации с использованием цифровой подписи или SMS-идентификации, выданной правительством. Владельцы местных веб-сайтов также обязаны хранить данные комментаторов не менее трех месяцев и предоставлять правительству информацию о пользователях по запросу[38].

По заявлениям МИК РК, ведется мониторинг на наличие данного механизма на сайтах Казахстана[39]. В случае отсутствия механизма на сайте владельцы ресурсов получают предписание в порядке 462-й статьи Административного кодекса РК, наказанием за нарушение которой является штраф в размере до 500 МРП.

36. «Сертификат безопасности»: «тестирование» завершено — вопросы остаются: https://rus.azattyq.org/a/kazakhstan-security-certificate-reaction/30097562.html

37. Национальный сертификат отменяется: https://t.me/certkznews/493?fbclid=IwAR1v34gDzAuRVEeoAzes_Wa6j3l_mJPnBXcSvpVcgIQ7xj5J0WeiF3wkkn8

38. Анонимные комментарии запретили: Назарбаев подписал закон: https://tengrinews.kz/kazakhstan_news/anonimnyie-kommentarii-zapretili-nazarbaev-podpisal-zakon-334276/

39. МИК РК не будет наказывать интернет-ресурсы за анонимные комментарии до конца марта: https://informburo.kz/novosti/v-mik-rk-rasskazali-kogda-nachnut-nakazyvat-internet-resursy-za-anonimnye-kommentarii.html

В связи с введением новых законов поменялись правила комментирования на одном из крупнейших новостных сайтов Казахстана[40].

4. Законы об обязательной регистрации сим-карт и устройств под настоящим именем для доступа в Интернет.

Согласно «Правилам оказания услуг доступа к сети Интернет» предоставление абоненту доступа к сети Интернет осуществляется только после заключения договора в письменном виде и с указанием сведений об абоненте (для юридических лиц – бизнес-идентификационный номер, данные свидетельства о постановке на учет по налогу на добавленную стоимость; для физических лиц – телефонные номера, идентификационные коды, адреса электронной почты, почтовый адрес, индивидуальный идентификационный номер) с приложением копий перечисленных документов[41].

В то же время предоставление услуг связи по незарегистрированным сим-картам не может осуществляться с 1 декабря 2014 года в связи с требованиями Министерства по инвестициям и развитию РК[42].

23 мая 2018 приказом и.о. министра информации и коммуникаций РК были утверждены правила регистрации мобильных абонентских устройств сотовой связи. Согласно им, чтобы мобильный телефон полноценно функционировал, он должен был быть зарегистрирован до 1 января 2019 года[43].

Позже в министерстве информации и коммуникаций пояснили, что с 1 января тотального отключения незарегистрированных абонентских устройств сотовой связи не будет. Устройство привяжется к той сим-карте, которая в нем установлена, и будет принадлежать тому человеку, на которого была оформлена сим-карта. Как сообщили в компании Altel, никого из абонентов от сотовой связи не отключали. «На сегодняшний день в базе Altel и Tele2 регистрацию IMEI-кода устройств и номера телефона прошли все абоненты. В связи с этим мы продолжаем предоставлять услуги связи в полном объеме всем нашим абонентам», – отметил глава пресс-службы Олжас Бибанов[44].

В марте 2016 года новые правила для точек доступа общего пользования требовали аутентификации пользователя с помощью одноразового кода SMS. Однако, поскольку сим-карты в Казахстане подлежат обязательной регистрации, это может позволить властям контролировать онлайн-активность пользователей, получающих доступ к интернету из публичных точек доступа[45]. Пред-

40. Tengrinews.kz меняет правила комментирования:
https://tengrinews.kz/internet/Tengrinewskz-menyaet-pravila-kommentirovaniya-337759/

41. Правила оказания услуг доступа к сети Интернет от 30 декабря 2011 года № 1718: http://www.adilsoz.kz/acts/show/id/41

42. Регистрация номера: https://activ.kz/ru/news/2685

43. Все, что нужно знать об обязательной регистрации сотовых телефонов в Казахстане:
https://forbes.kz/process/technologies/vse_chto_nujno_znat_ob_obyazatelnoy_registratsii_sotovyih_telefonov_v_kazahstane/

44. Регистрация телефонов: что произошло с устройствами казахстанцев 1 января:
https://tengrinews.kz/kazakhstan_news/registratsiya-telefonov-proizoshlo-ustroystvami-360806/

45. Казахстан ввел новые правила раздачи интернета в общественных местах:
https://digital.report/novyie-pravila-razdachi-interneta-v-obshhestvennyih-mestah-kazahstana-trebuyut-sms-avtorizatsii/

приятия могут быть оштрафованы на сумму до 226 000 тенге за несоблюдение новых правил, в то время как пользователи могут быть оштрафованы на сумму до 22 600 тенге[46].

7. Политика обязательного сохранения провайдером архивов записей и фиксация деятельности всех пользователей страны в интернете.

Трудно оценить масштабы и глубину государственного надзора в Казахстане, но группы по цифровым правам утверждают, что имеется крупномасштабная инфраструктура надзора. Правительственная «система оперативно-розыскных мероприятий» (СОРМ) наблюдения, происходящая из России, аналогична системе других бывших советских республик и позволяет проводить глубокую проверку пакетов (DPI) при передаче данных.

В январе 2018 года вступили в силу новые технические регламенты СОРМ, разработанные Комитетом национальной безопасности[47]. До этого в мае 2017 года компания Telia, которая владеет компанией мобильной связи Kcell, предупреждала, что эти новые требования к надзору предоставляют правительству доступ в реальном времени к сетям операторов, вызывая «потенциально серьезные последствия для свободы выражения мнений»[48].

Представитель анонимной частной телекоммуникационной компании заявил, что администрация президента, Генеральная прокуратура и Комитет национальной безопасности планируют запустить три разные системы мониторинга контента, включая программное обеспечение для мониторинга сайтов социальных сетей. В прошлом администрация города Алматы признавала, что ведет мониторинг популярных сайтов социальных сетей[49]. Государственная техническая служба (ГТС) – государственный орган, созданный в 2008 году, отвечает за мониторинг трансграничного сетевого трафика через систему, называемую «централизованное управление сетями телекоммуникаций» (ЦУСТ). Все операторы связи должны быть подключены к ЦУСТ и обязаны предоставить органам физический доступ к их центрам управления[50].

Активисты, использующие социальные сети, иногда подвергаются перехвату или наказанию, иногда превентивному, со стороны властей, которые заранее знают о запланированных действиях. Поступали сообщения о том, что власти проникли в групповые чаты на WhatsApp и Telegram, основываясь на

46. За подключение к общественному Wi-Fi без SMS-регистрации грозит штраф: https://tengrinews.kz/internet/podklyuchenie-obschestvennomu-Wi-Fi-SMS-registratsii-grozit-311021/

47. Об утверждении технического регламента «Общие требования к телекоммуникационному оборудованию по обеспечению проведения оперативно-розыскных мероприятий, сбора и хранения служебной информации об абонентах»: https://tengrinews.kz/zakon/komitet_natsionalnoy_bezopasnosti_respubliki_kazahstan/natsionalnaya_bezopasnost/id-V1600014680/

48. RESPECTING FREEDOM OF EXPRESSION - TELIA COMPANY'S VIEW ON NEW SURVEILLANCE REGULATION ('DIRECT ACCESS') IN KAZAKHSTAN https://www.teliacompany.com/en/news/news-articles/2017/freedom-of-expression-kazakhstan/

49. Обращения раскаявшихся террористов предложили использовать в борьбе с экстремизмом: https://tengrinews.kz/kazakhstan_news/obrascheniya-raskayavshihsya-terroristov-predlojili-242701/

50. Утверждены единые Правила взаимодействия и централизованного управления сетями телекоммуникаций: https://www.inform.kz/ru/utverzhdeny-edinye-pravila-vzaimodeystviya-i-centralizovannogo-upravleniya-setyami-telekommunikaciy_a2425819

заявлениях активистов о том, что они столкнулись с какими-то последствиями из-за материала, который они разместили только в приложении для общения. Неясно, как власти могли получить доступ к этим чатам[51 52 53].

Казахтелеком утверждает, что его система DPI используется для управления трафиком и не предоставляет доступа к персональным данным пользователей[54]. В июле 2015 года WikiLeaks опубликовал обмен электронными письмами между предполагаемым должностным лицом спецслужб и итальянской фирмой-шпионом Hacking Team. Похоже, что обмен сообщениями электронной почты предполагает, что правительство могло получить программное обеспечение для мониторинга и вмешательства в онлайн-трафик, включая зашифрованные сообщения, а также для проведения целевых атак против определенных пользователей и устройств[55].

Законодательство обязывает как интернет-провайдеров, так и операторов мобильной связи сохранять записи о действиях пользователей в Интернете, включая номера телефонов, платежные данные, IP-адреса, историю просмотров, протоколы передачи данных и другие данные, путем установки специального программного и аппаратного обеспечения, когда это необходимо[56]. Поставщики должны хранить пользовательские данные в течение двух лет и предоставлять доступ в течение 24 часов «оперативно-следственным органам», включая Комитет национальной безопасности, секретные службы и военную разведку, по санкции прокурора или, в некоторых случаях, «по согласованию с Генеральной прокуратурой»[57]. Административный кодекс, действующий с 2016 года, налагает штрафы на интернет-провайдеров в размере до 20 000 долларов США за неспособность хранить пользовательские данные[58].

Доменные имена верхнего уровня, использующие «.kz», должны работать на внутренних серверах[59]. В 2016 году посредством внесения поправок в Закон «Об информатизации» это требование локализации данных было расширено, чтобы обязать все личные данные, собираемые внутри страны местными компаниями, хранить внутри страны[60]. В конце 2017 года правительство объявило, что планирует провести переговоры с зарубежными социальными сетями и

51. Создавшего WhatsApp-группу «Небольшое насыха» мужчину осудили в Акмолинской области: https://tengrinews.kz/kazakhstan_news/sozdavshego-WhatsApp-gruppu-nebolshoe-nasyiha-mujchinu-309934/

52. В Алматы активистов предупредили о недопустимости акций 6 июля: https://rus.azattyq.org/a/27839704.html

53. Суд в Актобе вынес приговор по делу о пропаганде терроризма в WhatsApp'е: https://rus.azattyq.org/a/27914406.html

54. Вот мы и получили официальное подтверждение об использовании DPI от Казахтелекома: https://yvision.kz/post/219289

55. WikiLeaks, «Hacking Team»: https://wikileaks.org/hackingteam/emails/emailid/436130

56. Обязывает ли АИС и КНБ сотовых операторов создать систему прослушки? https://www.zakon.kz/top_news/152528-objazyvaet-li-ais-i-knb-sotovykh.html

57. Правила оказания услуг доступа к сети Интернет от 30 декабря 2011 года № 1718: http://medialawca.org/old/document/-11242

58. Статья 637. Нарушение законодательства Республики Казахстан в области связи: https://online.zakon.kz/Document/?doc_id=31577399#pos=8776;-36

59. Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

60. Kazakhstan: Localization of personal data: https://www.dacbeachcroft.com/en/gb/articles/2016/january/kazakhstan-localization-of-personal-data/

платформами обмена сообщениями в надежде на то, что они будут размещать локальные серверы, которые могли бы обеспечить более легкий доступ к личным данным граждан. Переговоры, как сообщается, должны быть завершены в начале 2019 года[61]. Ранее то же самое было предложено министром внутренних дел Калмуханбетом Касымовым под предлогом борьбы с так называемыми «группами смерти» в социальных сетях, которые якобы побуждают подростков совершать самоубийства[62].

61. Зарубежным соцсетям выдвинут требования по размещению серверов в РК: https://profit.kz/news/42724/Zarubezhnim-socsetyam-vidvinut-trebovaniya-po-razmescheniu-serverov-v-RK/

62. Соцсети могут обязать хранить в Казахстане информацию о гражданах страны: http://today.kz/news/kazahstan/2017-02-13/736099-sotsseti-mogut-obyazat-hranit-v-kazahstane-informatsiyu-o-grazhdanah-stranyi/

VII. ИНТЕРВЬЮ С ЭКСПЕРТОМ

Мной были направлены вопросы представителям казахстанской компании ЦАРКА, деятельность которой заключается в «анализе и предотвращении кибератак, компьютерных преступлений, экстренном реагировании на инциденты информационной безопасности и в развитии института цифровой гигиены и защищенности граждан и организаций Казахстана внутри информационного социума»[63]. Полученные ответы публикую ниже.

1. Как вы оцениваете ситуацию с правом на анонимность и использование средств шифрования в Казахстане?

Пока никаких технических ограничений на использование сервисов VPN или TOR мы не ощущаем, при этом важно понимать, что такая возможность существует и реализуема достаточно легко. В этом смысле все достаточно неплохо.

При этом мы видим определенные шаги государства в сторону деанонимизации, например введение процедуры регистрации при комментировании новостей на новостных порталах. Я считаю это ответной мерой государства против возникающих вызовов. Но, учитывая тренд миграции читателей в социальные сети, данная мера малоэффективна.

2. Как вы оцениваете новый технический регламент КНБ требований к телекоммуникационному оборудованию для следственных оперативно-розыскных мероприятий? Создается ли опасность нарушения права на анонимность этим регламентом?

ВОЗМОЖНО злоупотребление техническими возможностями. Для контроля над этим процессом существуют государственные механизмы, и именно эти механизмы и надо оптимизировать. Дополнительно необходимо усилить меры общественного контроля над этим процессом, в мире много примеров успешной реализации этой задачи, один из них – общественные советы.

3. Привлекаются ли представители гражданского общества к обсуждению новых законов, которые могут ограничить анонимность в интернете и использование средств шифрования? Как быстро вводятся данные законы?

Да, все вводимые нормы закона обсуждаются на портале legalacts.gov.kz и все имеют возможность участия в обсуждении. Другое дело, что не все стремятся, очень часто людям проще сидеть на диване и жаловаться на жизнь, чем делать. У нас очень пассивное гражданское общество, а жизнь не стоит на месте. Чиновники часто принимают неправильные решения и частично мы с вами

63. О компании «Царка»: https://www.cybersec.kz/ru/about-us

несем за это ответственность. По процедурам, проект документа обязан пройти общественные обсуждения не менее месяца и при наличии замечаний министерство юстиции требует веские аргументы для того, чтобы проигнорировать их. Мы знаем это не понаслышке, так как активно отстаивали свои вопросы этим путем, и готов ответственно заявить, что это рабочий механизм воздействия.

4. Расскажите подробнее о национальном сертификате безопасности. Какую опасность создает внедрение такого сертификата? Существуют ли на данный момент средства, которые позволяли бы оставаться анонимным, в случае повсеместного внедрения сертификата?

Корневой сертификат рассматривается государством как единственно доступный механизм фильтрации трафика без полной блокировки сервиса. Да, этот механизм рабочий, но опасный. Государство хочет получить «ящик Пандоры», обещает никогда его не вскрывать, а все должны поверить на слово. Вместе с тем, справедливости ради, можно признать, что пока других доступных механизмов государство не имеет и для решения этой задачи другим путем нужны годы.

Доступный механизм обхода сертификата – VPN, и такое мы уже видим в Таджикистане, где 100% населения использует VPN.

5. Были ли попытки в Казахстане обязать компании, мессенджеры раскрывать ключ шифрования вместо адресной расшифровки данных?

Насколько я знаю – нет. Нет задачи всеобщего доступа к данным, в первую очередь проблема именно с решением задач по борьбе с преступностью. Правоохранительные органы хотят получить механизм доступа к данным преступников и готовы обосновывать его, это ровно такие же права, как и у их западных коллег.

Западные же компании не хотят заниматься политикой, что вполне нормально, и требуют решение локальных органов для выдачи данных. Таким образом, техническая проблема эскалируется на геополитический уровень и должна в первую очередь быть решена там.

6. Как соблюдается закон в Казахстане о запрете анонимных комментариев в интернете? Известны ли вам случаи наказания владельцев сайта за нарушения данного закона?

Все новостные порталы реализовали функцию авторизации для доступа к комментированию, технически это несложно было сделать.

Случаев наказания за невыполнение этого требования я не слышал, думаю, в нашей стране такое маловероятно, так как в этом случае легко потерять лицензию – потерять бизнес.

7. В чем опасность законов об обязательной регистрации сим-карт и IMEI мобильных устройств связи для права на анонимность онлайн? В чем заключается цель введения подобных законов, по вашему мнению?

Честно говоря, я не понимаю излишний ажиотаж вокруг этой темы. Я часто путешествую, и, проведя несложный анализ, можно увидеть, что такие подходы сейчас применяются по всему миру.

Другой вопрос, каким образом обращаются с нашими данными, это действительно проблема, и тут мы возвращаемся к вопросу №2 – надзор за деятельностью госорганов, в том числе общественный.

Очень много данных теряется государством в ходе их обработки и использования, и нам, безопасникам, это кажется серьезной проблемой.

8. Какова проблема с законами о хранении персональных данных исключительно на серверах внутри страны и использовании национального домена для сайтов, размещенных на серверах внутри страны?

Требование по хранению персональных данных на территории страны – это хорошее и правильное требование, позволяющее контролировать процесс и применять некоторые санкции в случаях нарушения требований.

А вот вторая часть вопроса – это чистой воды протекционизм локального рынка, в том числе из соображений безопасности. Это не плохо и не хорошо, это мера, направленная на поддержку отечественного рынка хостинга. Мы не работаем на этом рынке, но, думаю, ему придет конец, если убрать это требование. Надо этот вопрос обсудить с компаниями PS, HOSTER и, конечно, Казахтелеком.

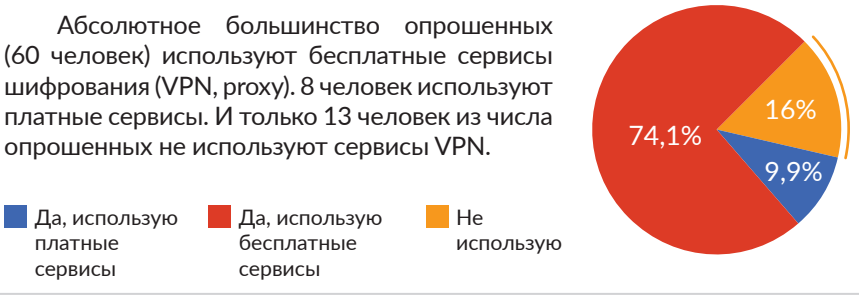
В принципе это требование не особо мешает развивать сайты доменной зоны kz, так как местные цены не сильно отличаются от мировых, зато позволяет концентрировать квалификацию вокруг этих компаний.

Если коротко, то это маленькое зло во имя большого добра.

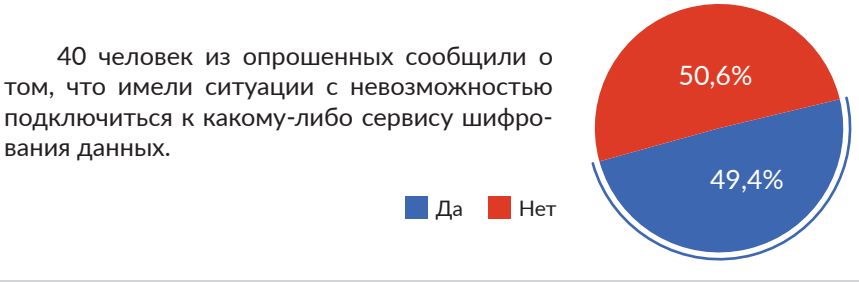
VIII. АНАЛИЗ АНКЕТИРОВАНИЯ

В ходе проведения опроса были получены ответы от 81 респондента, проживающего в Казахстане. Из них 16 человек проживают в г. Алматы, 24 – в г. Нур-Султане, 26 – в г. Караганде и 14 – в остальных городах Казахстана.

Абсолютное большинство опрошенных (60 человек) используют бесплатные сервисы шифрования (VPN, proxy). 8 человек используют платные сервисы. И только 13 человек из числа опрошенных не используют сервисы VPN.

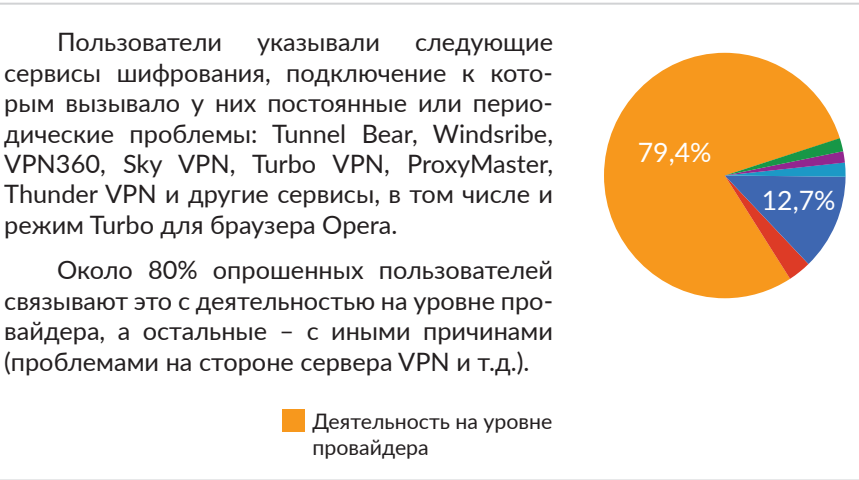


40 человек из опрошенных сообщили о том, что имели ситуации с невозможностью подключиться к какому-либо сервису шифрования данных.

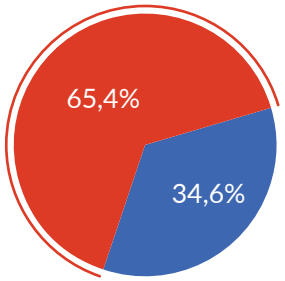


Пользователи указывали следующие сервисы шифрования, подключение к которым вызывало у них постоянные или периодические проблемы: Tunnel Bear, Windsribe, VPN360, Sky VPN, Turbo VPN, ProxyMaster, Thunder VPN и другие сервисы, в том числе и режим Turbo для браузера Opera.

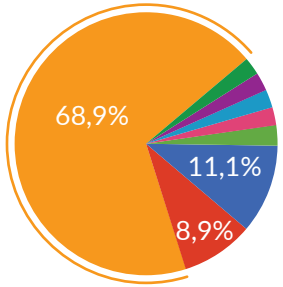
Около 80% опрошенных пользователей связывают это с деятельностью на уровне провайдера, а остальные – с иными причинами (проблемами на стороне сервера VPN и т.д.).



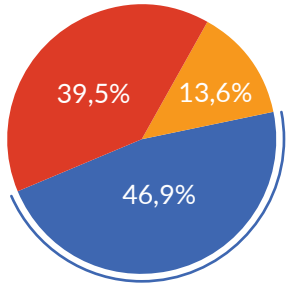
Большинство опрошенных (53 респондента) никогда не пользовались анонимными сетями, такими как Tor или I2P. 16 респондентов из числа пользователей анонимных сетей сталкивались с проблемами подключения к ним.



70% респондентов связывают свои трудности с подключением к анонимным сетям с блокировками на уровне провайдера.

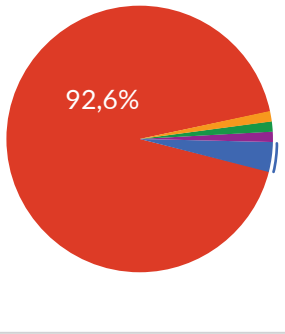


38 (47%) респондентов добровольно зарегистрировали IMEI-код своего мобильного устройства.

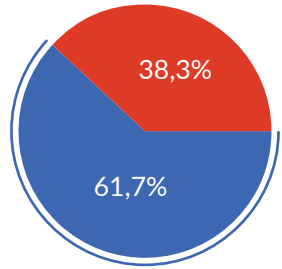


9 человек из числа опрошенных сообщили о потере возможности пользоваться сим-картой, номер которой не был связан с IMEI устройства из-за отсутствия регистрации.

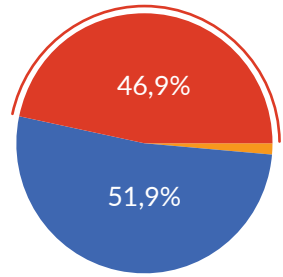
Только 3 человека из опрошенных 81 заявили о том, что добровольно установили сертификат безопасности Qaznet.



62% опрошенных знают о потенциальных проблемах с шифрованием данных, которые могут возникнуть при установке сертификата Qaznet.

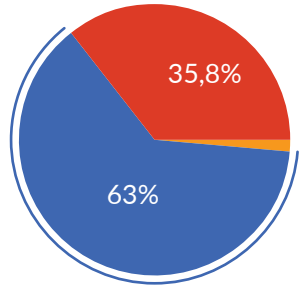


43 респондента заявили о том, что сталкивались за последний год с публичными точками доступа Wi-Fi, которые требовали аутентификацию через одноразовый пароль.

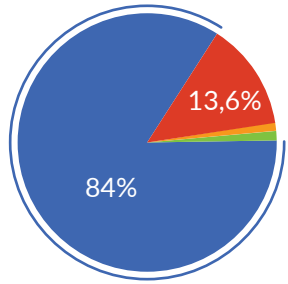


Места, в которых расположены точки, требующие аутентификации, с которыми сталкивались опрошенные, это торговые центры, железнодорожные и автовокзалы, аэропорты, кофейни, ВУЗы, сети Burger King, Starbucks.

64% опрошенных сообщили, что им известно о том, что они имеют право на анонимность и использование средств шифрования согласно международному законодательству.



84% опрошенных считают такие действия, как внедрение сертификата безопасности Qaznet, требование регистрации IMEI, блокировки и запреты средств шифрования (VPN, анонимных сетей и proxy-серверов), нарушением права на приватность и использование средств шифрования. 1% опрошенных считает нарушением все, кроме требований регистрации IMEI.



Как мы можем судить по результатам опроса, большинство респондентов используют средства шифрования. Из тех, кто их использует, – большая часть сталкивается с проблемами подключения. Особенно это касается пользователей анонимных сетей, таких как Tor и I2P. Большинство опрошенных связывают проблемы с подключением с блокировками анонимных сетей и некоторых сервисов VPN.

Около половины опрошенных добровольно зарегистрировали IMEI своего мобильного устройства, когда появилось требование. 9 опрошенных из числа тех, кто не производил регистрацию самостоятельно, столкнулись с невозможностью дальнейшего использования сети оператора.

Практически никто не устанавливал сертификат безопасности Qaznet из числа опрошенных и большинству известно о последствиях установки сертификата безопасности.

Больше половины опрошенных сталкивались за последний год с общественными точками доступа Wi-Fi, которые требовали у них аутентификацию через SMS-пароль.

Большая часть опрошенных знает о своем праве на анонимность и использование средств шифрования и абсолютное большинство считает недавние действия правительства нарушением своего права.

IX. ЗАПРОС В ГОСУДАРСТВЕННЫЙ ОРГАН

Запрос был направлен в Мажилис Парламента РК с целью выяснить, кем были инициированы законопроекты, какие комитеты их рассматривали, кто участвовал в рассмотрении, привлекались ли представители гражданского общества, НКО при рассмотрении законопроекта и как долго проводилось обсуждение следующих законов и законопроектов:

1. Проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информации и коммуникаций» (31 мая 2017 года);
2. Законопроект «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия экстремизму и терроризму» (31 августа 2016 г.);
3. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;
4. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

Полный ответ на запрос будет дан в приложении.

По ответу на данный запрос можно сделать вывод, что законы и законопроекты не принимались ускоренными процедурами, по данным законопроектам проводилось обсуждение с представителями различных НКО Казахстана. Но, к сожалению, это не помогло предотвратить принятие законов в таком виде, какие они есть сейчас, – не соответствующем рекомендациям о защите права на анонимность и использование средств шифрования.

X. АНАЛИЗ СОБРАННЫХ ДАННЫХ

Мониторинг включал в себя анализ международной практики, рекомендаций ООН, национального законодательства, сообщений национальных и международных СМИ, интервью с экспертом ЦАРКА, запрос в Мажилис Парламента, а также опрос пользователей интернета в Казахстане.

Сравнив рекомендации специального докладчика Давида Кайе касательно права на анонимность и использование средств шифрования с национальным законодательством, можно прийти к выводу, что рекомендации практически полностью не выполняются.

Да, проводятся слушания с участием широкого круга общественности законов, касающихся в том числе и ограничений права на анонимность и использование средств шифрования. Однако проводимые слушания не позволяют предотвратить принятие законов, которые прямо противоречат рекомендациям, касающимся защиты права на неприкосновенность частной жизни в интернете.

По остальным индикаторам мы видим явное несоответствие. Большая часть законов и мер, ограничивающих право на анонимность и использование средств шифрования, была принята после мая 2015 года, когда был впервые выпущен доклад Давида Кайе, что говорит об игнорировании его рекомендаций в полном объеме при принятии данных мер и законов.

Был принят целый ряд мер неизбирательного характера, противоречащих 4 пункту рекомендаций, таких как:

1) запрет на индивидуальное использование технологий шифрования и борьба с применением средств шифрования;
2) намеренное понижение степени эффективности шифрования;
3) запрет анонимных высказываний в интернете;
4) принуждение к регистрации сим-карт и мобильных устройств под настоящим именем для доступа в Интернет;
5) политика локализации хранения данных внутри страны и фиксация деятельности всех пользователей страны в интернете.

Это говорит о несоответствии индикаторам 1 и 2, которые были даны в начале этого исследования. Формальное выполнение в стране 3 пункта не способствует прекращению принятия законов, ограничивающих право на анонимность и использование средств шифрования.

Анализ сообщений СМИ подтверждает невыполнение рекомендаций. Принятие некоторых мер, таких как введение сертификата безопасности Qaznet, было отложено, однако остаются вопросы и опасения по поводу попыток введения этой меры в будущем.

Было проведено интервью с экспертом ЦАРКА, которое дало понимание неэффективности некоторых применяемых норм, распространенности подобных практик в мире. Эксперт советует наладить общественный контроль за деятельностью госорганов, так как принятые меры способны потенциально причинить вред праву на неприкосновенность частной жизни граждан Казахстана, в том числе и благодаря несанкционированному доступу и утечке данных.

Запрос в Мажилис Парламента подтвердил информацию о том, что по принятым законам и законопроектам, ограничивающим право на анонимность, было проведено слушание с привлечением неправительственных организаций Казахстана и законы не принимались ускоренными процедурами. Однако все же законы были приняты в том виде, который противоречит рекомендациям спецдокладчика.

Опрос пользователей дал информацию о том, что многие пользователи VPN и анонимных сетей в Казахстане испытывают проблемы с подключением к ним, что вкупе с сообщениями в СМИ о действиях по блокировке анонимных сетей и некоторых средств шифрования говорит о действительности неафишируемых блокировок некоторых средств шифрования в Казахстане. Также некоторые пользователи потеряли возможность пользоваться сим-картами, к которым не привязан IMEI-код регистрируемого мобильного устройства. Из опрошенных респондентов многие не знают о потенциальных опасностях внедрения сертификата безопасности, а небольшое число пользователей установили его. Большинство опрошенных отрицательно относятся к таким инициативам государства, как внедрение сертификата безопасности, считая их нарушающими их права.

Из всего этого можно сделать вывод о действительности нарушения права на анонимность в Казахстане на законодательном и практическом уровне. Невыполнение рекомендаций специального докладчика Дэвида Кайе носит повсеместный характер и производится практически в полном объеме.

XI. ВЫВОДЫ И РЕКОМЕНДАЦИИ

Исходя из проанализированных данных и полученного вывода о практически полном игнорировании рекомендаций специального докладчика Дэвида Кайе касательно анонимности в Интернете и применении средств шифрования, можно дать следующие рекомендации:

1. Начать проводить образовательные мероприятия, направленные на популяризацию среди граждан цифровой грамотности и средств обеспечения приватности, навыков безопасного использования интернета, распоряжения своими персональными данными для предотвращения случаев мошенничества, кибербуллинга и иных правонарушений.
2. Проводить обсуждение новых законов, которые потенциально могут ограничить анонимность онлайн и использование средств шифрования, привлекая широкие круги представителей гражданского общества, не принимая законы в ускоренном порядке.
3. Любые ограничения анонимности и шифрования в интернете применять исключительно на индивидуальной основе и в соответствии с требованиями законности, необходимости, соразмерности и правомерности их цели и только с санкции суда.
4. Отказаться от рассмотрения законов и применения мер, которые могли бы не избирательно, не на индивидуальном уровне, без соответствия требованиям законности, необходимости, соразмерности и правомерности их цели ограничивать анонимность и использование средств шифрования в интернете.
5. Отказаться от ограничений анонимности и использования средств шифрования, носящих абсолютный, неизбирательный характер, — принудительного снижения стандартов безопасности, ограничения на законодательном уровне анонимного общения онлайн, требований обязательной регистрации сим-карт, мобильных средств связи для доступа к услугам интернета, блокирования доступа к услугам средств шифрования (VPN, Tor, Proxy и т.д.), требований использования внутренних серверов для сайтов с национальным доменом .kz, требований компаниям хранить личные данные исключительно на серверах внутри страны, требований аутентификации пользователей при пользовании публичными точками доступа к интернету (Wi-Fi) и других подобных ограничений.

Выполнение данных рекомендаций требует всестороннего изучения рекомендаций и иностранных практик, применяемых для защиты права на неприкосновенность частной жизни и свободы выражения мнений. В первую очередь стоит отменить недавно внесенные изменения в законодательство, приведя его хотя бы в состояние до введения ограничений. Дальнейшее же совершенствование законодательства требуется для недопущения введения подобных ограничений неизбирательного характера в будущем.

Приложение 1

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ПАРЛАМЕНТІ МӘЖІЛІСІ
АППАРАТЫ БАСШЫСЫНЫҢ
ОРЫНБАСАРЫ

ЗАМЕСТИТЕЛЬ
РУКОВОДИТЕЛЯ АППАРАТА
МАЖИЛИСА ПАРЛАМЕНТА
РЕСПУБЛИКИ КАЗАХСТАН

Нұр-Сұлтан, Парламент Мәжілісі
№ _____

Нур-Султан, Мажилис Парламента
20 __ жылғы «___»_____
«___» _____ 20 __ года

Хлынцову А.С

Уважаемый Александр Сергеевич!

Рассмотрев Ваше обращение, касающееся предоставления информации по проектам законов Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информации и коммуникаций», «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия экстремизму и терроризму», «Об информатизации» и «О персональных данных и их защите», сообщаем следующее.

1. Проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информации и коммуникаций».

Постановлением Правительства РК от 31 мая 2017 № 316 названный законопроект поступил в Мажилис Парламента 7 июня 2017 года. Инициатором законопроекта являлось Правительство Республики Казахстан (Министерство информации и коммуникаций РК).

Головным определен Комитет по социально-культурному развитию Мажилиса Парламента. Для рассмотрения законопроекта была создана рабочая группа, в которую вошли депутаты Мажилиса Парламента, представители разработчика и заинтересованных государственных органов, а также Национального Банка, НПП Республики Казахстан «Атамекен», Национального информационно-коммуникационного холдинга «Зерде», ТРК «Казакстан», Агентства «Хабар», республиканских газет «Егемен Қазақстан» и «Казахстанская правда», неправительственных организаций («Әділ сөз», «MEDALIFE», «Интерньюс Казахстан», «Жер тағдыры», «Медиа альянс») и представители сотовых операторов.

По законопроекту проведены презентация и 14 заседаний рабочей группы.

В ходе работы над законопроектом рабочей группой было рассмотрено свыше 200 поправок.

В целях всестороннего обсуждения норм законопроекта Комитетом 23 октября 2017 года проведены круглый стол в Атырауской области и 2 ноября 2017 года в г. Астане – встреча с международными экспертами.

Законопроект одобрен в первом чтении на пленарном заседании Мажилиса Парламента 8 ноября 2017 года и 22 ноября 2017 года – во втором.

21 декабря 2017 года Сенатом Парламента названный Закон был одобрен, 28 декабря 2017 года подписан Президентом Республики Казахстан.

2. Проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия экстремизму и терроризму».

Постановлением Правительства РК от 31 августа 2016 № 490 данный законопроект поступил в Мажилис Парламента 1 сентября 2016 года. Инициатором законопроекта являлось Правительство Республики Казахстан.

Головным определен Комитет по международным делам, обороне и безопасности Мажилиса Парламента. Для рассмотрения законопроекта была создана рабочая группа, в которую вошли депутаты Мажилиса Парламента, представители разработчика и заинтересованных государственных органов, неправительственных организаций (Казахстанский институт стратегических исследований, Консалтинговая, аналитическая организация «Группа Оценки Рисков» (KRAG), Астанинский филиал Казахстанского международного бюро по правам человека и соблюдению законности (КМБПЧ), Хартия за права человека, Фонд развития парламентаризма в Казахстане, Ассоциация центров исследования религий и другие), религиозных организаций, партий, не входящих в состав Парламента, общественные деятели и эксперты.

По законопроекту проведены презентация и 13 заседаний рабочей группы.

Законопроект также обсуждался на круглом столе, семинаре Республиканского общества ветеранов Казахстана, заседании Ассоциации ветеранов войны в Афганистане, что позволило в более широком формате совместно с представителями гражданского общества рассмотреть предлагаемые меры противодействия экстремизму и терроризму.

В ходе работы над законопроектом рабочей группой было рассмотрено более 90 поправок.

Законопроект одобрен в первом чтении на пленарном заседании Мажилиса Парламента 5 октября 2016 года и 9 ноября 2016 года – во втором.

9 декабря 2016 года Сенатом Парламента названный Закон был одобрен, 22 декабря 2016 года подписан Президентом Республики Казахстан.

3. Проект Закона Республики Казахстан «Об информатизации».

Постановлением Правительства РК от 31 мая 2014 № 594 названный законопроект поступил в Мажилис Парламента 7 июня 2014 года. Инициатором законопроекта являлось Правительство Республики Казахстан (Агентство по связи и информации РК).

Головным определен Комитет по социально-культурному развитию Мажилиса Парламента. Для рассмотрения законопроекта была создана рабочая

группа, в которую вошли депутаты Мажилиса Парламента, представители разработчика и заинтересованных государственных органов, а также представители НПП Республики Казахстан «Атамекен», Национального информационно-коммуникационного холдинга «Зерде», акционерного общества «Национальные информационные технологии», неправительственных организаций («Правовой медиа-центр», «Интерньюс Казахстан», Казахстанская ассоциация IT-компаний) и представители сотовых операторов, интернет-изданий.

По законопроекту проведены презентация и 20 заседаний рабочей группы.

В ходе работы над законопроектом рабочей группой было рассмотрено свыше 450 поправок.

Законопроект одобрен в первом чтении на пленарном заседании Мажилиса Парламента 22 апреля 2015 года и 7 октября 2015 года – во втором.

29 октября 2015 года Сенатом Парламента названный Закон был одобрен, 24 ноября 2015 года подписан Президентом Республики Казахстан.

4. Проект Закона Республики Казахстан «О персональных данных и их защите».

Постановлением Правительства РК от 29 марта 2012 № 372 данный законопроект поступил в Мажилис Парламента 3 апреля 2012 года. Инициатором законопроекта являлось Правительство Республики Казахстан (Министерство внутренних дел РК).

Головным определен Комитет по законодательству и судебно-правовой реформе Мажилиса Парламента. Для рассмотрения законопроекта была создана рабочая группа, в которую вошли депутаты Мажилиса Парламента, представители разработчика и заинтересованных государственных органов, Верховного Суда, Генеральной Прокуратуры, Комитета национальной безопасности, Службы охраны Президента, Национального Банка Республики Казахстан, а также представители неправительственных организаций и эксперты.

По законопроекту проведено 27 заседаний рабочей группы, на которых были рассмотрены поступившие предложения.

Законопроект одобрен в первом чтении на пленарном заседании Мажилиса Парламента 14 ноября 2012 года и 6 марта 2013 года – во втором.

18 апреля 2013 года названный Закон был рассмотрен Сенатом Парламента, 21 мая 2013 года подписан Президентом Республики Казахстан.

Ж. Жугунисов

Исп. Кайргалиева Г.М., 74-68-51

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК