МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права

(наименование института полностью)

Кафедра «Конституционное и административное право»

(наименование кафедры полностью)

40.04.01 Юриспруденция

(код и наименование направления подготовки, специальности)

«Правовое обеспечение государственного управления и местного самоуправления»

(направленность (профиль)

# МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему Приватность в сети Интернет: конституционно-правовые вопросы

Студент С.А. Назаров _____
(И.О. Фамилия) (личная подпись)

Научный руководитель А.Н. Станкин _____
(И.О. Фамилия) (личная подпись)

Руководитель программы д.ю.н., профессор, Д.А. Липинский _____
(учёная степень, звание, И.О. Фамилия) (личная подпись)

« _____ » _____ 20 _____ г.

**Допустить к защите**

Заместитель ректора-директор к.ю.н., доцент С.И. Вершинина _____
(учёная степень, звание, И.О. Фамилия) (личная подпись)

« _____ » _____ 20 _____ г.

Тольятти 2018

**Оглавление:**

## Введение

Конституцией Российской Федерации провозглашаются права и свободы человека и гражданина, которые являются непосредственно действующими. Исходя из них осуществляется правосудие. Одним из ключевых личных прав выступает право на неприкосновенность частной жизни и тайну переписки. Данная работа посвящена праву на приватность в сети Интернет, – неотъемлемому атрибуту неприкосновенности частной жизни, его конституционно-правовой основе, структуре и вопросам реализации.

Актуальность исследования заключается как в стремительном развитии технологий Интернет-коммуникации, охватывающих нашу повседневную жизнь, так и в растущем интересе их правового регулирования, границы которого являются по-прежнему достаточно дискуссионными. При этом подобное регулирование со стороны государства может как защищать ключевые права и свободы, включая приватность и неприкосновенность частной жизни, свободу мысли и слова, так и наоборот вступать с ними в конфликт.

Новые средства коммуникации, работающие через сеть Интернет, позволяют вести общение с собеседником из любого конца света. При этом, несмотря на частое утверждение «мне нечего скрывать», пользователи сети Интернет оставляют множество «следов», что нередко может повлечь нарушение их прав и свобод в будущем. Многие пользователи мессенджеров и социальных сетей так же уверены и в конфиденциальности своих сообщений, что зачастую может быть далеко не так. Причиной тому может быть множество факторов: как беспечность со стороны самих пользователей, так и небрежность операторов данных сервисов, а также противоправная деятельность третьих лиц. Особый интерес в контроле Интернет-приватности могут иметь и различные государственные структуры. Вместе с тем та самая грань, когда государственное вмешательство с целью защиты прав и свобод переступает через эти самые права и свободы по-прежнему остаётся дискуссионной.

В частности, раскрытие бывшим сотрудником Агентства национальной безопасности (АНБ) США Эдвардом Сноуденом программы глобальной слежки как за гражданами самих Соединённых Штатов, так и иностранными гражданами, породило очередной виток ожесточённых дебатов об обоснованности данной политики. Тем не менее указанный случай мог быть далеко не единичным, получив столь яркое освещение во многом лишь благодаря своей глобальности. На практике возможно множество локальных, менее освещаемых прецедентов. Стоит понимать, что само по себе правовое регулирование может проявляться в различных формах: как защищать непосредственно конвенционные и конституционные права, гарантируя их соблюдение, так и наоборот переступать через них под тем или иным предлогом.

Целью данной работы, в первую очередь, выступает нахождение необходимого баланса, позволяющего максимально обеспечить реализацию и защиту конституционных прав и свобод, а также предотвратить в отношении них возможные противоправные действия и злоупотребления.

Для осуществления поставленной цели необходимо выполнить ряд задач**.** Во-первых, на основании анализа формирования и развития института неприкосновенности частной жизни, становления международного и внутригосударственного законодательства в указанной сфере дать определение приватности в сети Интернет, её особенностей и элементов, соотнести её с положениями Конституции Российской Федерации. Во-вторых, определить сферы и общественные отношения, охватывающие данные положения. В-третьих, проанализировать сложившуюся на данный момент ситуацию, выделить имеющиеся проблемы и предложить оптимальные варианты их решения, соответствующие ценностям, провозглашённым международными соглашениями и Конституцией Российской Федерации. В-пятых, сделать соответствующие выводы на основании приведённых в исследовании данных.

Объектом исследования выступает непосредственно приватность в сети Интернет как составная часть права на неприкосновенность частной жизни и тайны сообщений в целом. В свою очередь предметом являются конституционно-правовые вопросы, возникающие в процессе реализации и защиты права на приватность в сети Интернет. При этом решение данных вопросов выступает одной из руководящих задач исследования.

В процессе исследования были использованы такие методы, как анализ существующего законодательства и текущей правовой доктрины, синтез полученной в процессе исследования информации, сравнение международных соглашений и нормативно-правовых актов Российской Федерации и зарубежных стран. Также были учтены такие приёмы и методы, как сравнительный, правовой, исторический, формально-юридический, технико-юридический и прочие.

Выявленные в процессе исследования положения обладают существенной теоретической, научной и практической значимостью. Определение приватности в сети Интернет, её концепция, особенности и элементы должны дополнить институт неприкосновенности частной жизни, изучаемый наукой Конституционного права, открывая новую сферу теоретической и концептуально-правой разработки в указанной сфере. Практическая же значимость должна выражаться в качественных, научно и технически обоснованных нормативно-правовых актах, преследующих цели обеспечения реализации и защиты конвенционных и конституционных прав и свобод человека и гражданина.

На защиту выносятся следующие теоретические выводы и практические предложения:

1. Определено, что под приватностью в сети Интернет следует понимать атрибут права на неприкосновенность частной жизни, общественные отношения, возникающие при реализации человеком его права на конфиденциальную переписку

и общение через средства Интернет-коммуникации, и (или) его стремлении сохранить своё пребывание в сети Интернет тайным от посторонних глаз.

2. Установлено, что элементами Интернет-приватности являются тайна Интернет-сообщений и Интернет-анонимность. Под тайной Интернет-сообщений подразумевается реализация человеком права на конфиденциальность его общения и переписки через средства Интернет-коммуникации. В свою очередь Интернет-анонимность включает в себя стремление сохранить в тайне непосредственно своё пребывание в сети Интернет, инструментами реализации которого выступают различного рода средства анонимизации.

3. На основании современной международной практики регулирования сферы Интернет-приватности были выделены два подхода: социальный и государственный, выявлены их руководящие принципы. Социальный, к приверженцам которого в большей степени можно отнести страны Европейского Союза, представляет из себя комплекс принципов и норм, сочетающих в себе прозрачность хранения личных данных и максимальную их доступность для владельцев. В свою очередь государственному, приверженцами которого в большей мере можно назвать Китай и ближневосточные страны, присущ больший уровень вмешательства в отношения сервиса и клиента, меньшая степень прозрачности, а также принципиально доминирующие государственные интересы в отношении правового регулирования данной сферы. Таким образом, социальному подходу соответствуют принципы верховенства прав человека и гражданина, общественной прозрачности, демократичности, а государственному, в свою очередь, – принципы верховенства государственных интересов (в том числе выдаваемых за общественные или коллективные) над правами личности, закрытости, недемократичности принятия решений. Можно также выделить и переходную категорию, прибегающую к методам и принципам обоих подходов, к приверженцам которой можно, например, отнести как Российскую Федерацию, так и США.

4. Был выявлен круг основных проблем Интернет-приватности. Ключевой среди них выступает дискуссионность пределов вмешательства государства в сферу приватности, где на одной чаше весов мы видим такие категории, как неприкосновенность частной жизни, тайна переписки и сообщений, а на другой – необходимость борьбы с преступностью, обеспечение прав и свобод личности, а также благополучия общества. Проблемным является и вопрос этичности мониторинга общего потока пользовательских сообщений, сбора их и хранения, а также соответствия данной практики требованиям безопасности. Кроме того, существенной проблемой выступает вопрос обоснованности и безопасности передачи организаторами распространения информации ключей шифрования правоохранительным органам. Стоит также выделить отсутствие должного нормативного определения электронного наблюдения, несмотря на уже фактически сложившиеся отношения и ресурсы для его осуществления, а также расплывчатое нормативное регулирование использования средств кодирования (шифрования) физическими лицами. Отдельного внимания заслуживает и проблема общей безопасности хранения пользовательских данных как со стороны частных компаний, так и со стороны государственных структур.

5. В целях обеспечения права граждан на Интернет-приватность необходимо внести в законодательство следующие изменения и дополнения. В частности, статьи 10.1 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также 46 федерального закона № 126-ФЗ «О связи» следует дополнить нормой, обязывающей организатора распространения информации в случае обнаружения утечки, а равно иной виновной компрометации личной информации пользователей, переписок и их содержания уведомить пострадавшую сторону немедленно (либо в кратчайшие сроки) после обнаружения указанной компрометации. Необходимо и дополнение главы 13 КоАП РФ составом: «Сокрытие должностным (юридическим) лицом факта утечки (компрометации)

личной информации». Также в федеральный закон № 144-ФЗ от 12.08.1995 «Об оперативно-розыскной деятельности» обосновано включение «электронного наблюдения» в список оперативно-розыскных мероприятий, поскольку фактически данные отношения уже сложились, но ещё не закреплены нормативно. При этом в целях обеспечения прозрачности необходимо внесение в Уголовно-процессуальный кодекс Российской Федерации или федеральный закон «Об оперативно-розыскной деятельности» чёткой классификации тех преступлений, при расследовании которых может применяться электронное наблюдение, либо же конкретных случаев, когда это оправдано или необходимо. Заслуживают законодательного закрепления и рамки проведения электронного наблюдения с обязательным уведомлением оператора связи. Представляет важность и внесение поправок в норму статьи 13.6. КоАП РФ, уточняющих о запрете передачи через несертифицированные средства кодирования (шифрования) исключительно сообщений и сведений, составляющих государственную тайну, а также отражение в новой формулировке статьи или отдельном правовом акте информации об отсутствии обязательной сертификации средств кодирования (шифрования) массово применяемых для защиты сведений, не составляющих государственную тайну. Кроме того, как минимум заслуживают пересмотра и нормы статьи 64 федерального закона «О связи», обязывающие операторов связи хранить Интернет-трафик абонентов, до разработки более прозрачного и безопасного механизма реализации, не вступающего в конфликт с конвенционным и конституционным правом на приватность. Представляет интерес и положение статьи 10.1 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» о передаче организаторами распространения информации ключей шифрования, заслуживающее значительного пересмотра, либо полной отмены в связи с выявленными рисками и этическими проблемами, а также технической невозможностью реализации в определённых случаях. Так, передача ключей шифрования третьим лицам может быть

потенциально небезопасна для всех пользователей сервиса, либо организатор распространения информации может вовсе не иметь доступа к сообщениям на устройстве из-за технических особенностей используемых им технологий. Отдельно стоит обратить внимание и на политику блокировок Интернет-ресурсов, не преследующих преступных целей и готовых к сотрудничеству с правоохранительными органами в плане пресечения противоправного публичного контента. Предлагается практика по внесению Интернет-ресурсов, не соответствующих в полней мере государственным стандартам, в публичный реестр «сомнительных» сервисов при сохранении к ним доступа, но наложения некоторых ограничений, вроде отказа от каких-либо налоговых послаблений или их государственной финансовой поддержки. В противовес этому Интернет-ресурсам, в полной мере соответствующим государственным стандартам, предлагается их одобрение в виде выдаваемых электронных сертификатов, а также возможности некоторых налоговых послаблений, либо финансовой господдержки, если Интернет-ресурс является отечественным. Таким образом, обеспечивается баланс между ограничением доступа к Интернет-ресурсам, действительно, преследующим противоправные цели, и сохранением за пользователем выбора в условиях справедливой конкуренции. Говоря о порядке функционирования такого инструмента как VPN, обоснованным решением стал бы пересмотр нормы о запрете доступа с иностранных VPN-серверов к ограниченным на территории РФ Интернет-ресурсам в связи с нахождением и функционированием указанных серверов в иностранной юрисдикции, а также сомнительной возможностью реализации данных норм из-за особенностей функционирования данной технологии. В свою очередь со стороны VPN-провайдеров, чьи серверы физически расположены на территории РФ и дают возможность выхода в сеть Интернет от российского IP-адреса, взаимной мерой стало бы соблюдение ими действующего российского законодательства. При использовании же зарубежных VPN-серверов достаточной мерой может выступить

предупреждение пользователей о возможной доступности Интернет-сайтов с содержанием, признанным в их стране нахождения незаконным, и о возможной юридической ответственности за противоправные действия, совершаемые с помощью данных сервисов. Помимо перечисленного выше, в связи с достаточно частым применением положения статьи 138.1 УК РФ в отношении лиц, не имеющих умысла нарушать право приватности других, и мнением Конституционного суда РФ, подчёркивающим руководящую роль умысла в составе указанного преступления, должной мерой стал бы пересмотр положений данной нормы и легализация исключительно бытовых сценариев использования указанных инструментов. Говоря о киберпреступлениях, результатом которых стала незаконная эксплуатация чужих IP-адресов для совершения правонарушений, необходимой мерой может стать выделение из статей 272 (неправомерный доступ к компьютерной информации) и 273 (создание, использование и распространение вредоносных компьютерных программ) УК РФ отдельного состава правонарушения, предусматривающего юридическую ответственность за незаконное использование IP-адреса другого лица. Данная мера может быть полезна в связи с размытостью вышеуказанных составов, а также стремительным технологическим развитием, ушедшим значительно вперёд с момента введения данных составов. В целях гуманизации, допустимо разделение данного состава на административный и уголовный. Административный, наказываемый штрафом, возможно оставить на случаи, когда отсутствует конечный ущерб, либо же он незначителен. Уголовный состав, в свою очередь, должен иметь место в случае совершения от лица жертвы правонарушения, что опорочило её доброе имя, а также причинение этими действиями существенного вреда. «Незаконное» использование, в данном случае, должно предполагать использование IP-адреса без ведома и согласия лица путём применения вредоносного программного обеспечения, либо уязвимостей, а равно путём обмана или подбора пароля.

Результаты исследования были апробированы при участии во Всероссийском конкурсе молодёжи образовательных и научных организаций на лучшую работу «Моя законотворческая инициатива», а также на Международных научно-практических конференциях «Актуальные проблемы правотворчества и правоприменительной деятельности в Российской Федерации» и «Актуальные вопросы современного права. Пути теоретического и практического решения проблем».

По теме диссертационного исследования были опубликованы следующие работы:

1. Назаров С.А. IP-адрес как идентификатор при расследовании правонарушений [Текст] / С.А. Назаров // Сборник статей Международной научно-практической конференции «Актуальные проблемы правотворчества и правоприменительной деятельности в Российской Федерации. Часть 2» (Самара, 01.11.2017 г.). – Уфа: Аэтерна, 2017. – С. 40-44.
2. Назаров С.А. Концепция Интернет-приватности / С.А. Назаров // Сборник статей Международной научно-практической конференции «Актуальные вопросы современного права. Пути теоретического и практического решения проблем» (Уфа, 01.03.2018 г.). – Уфа: Аэтерна, 2018. – С. 130-133.
3. Назаров С.А. Правовая охрана тайны сообщений в Российской Федерации / С.А. Назаров // Сборник тезисов работ участников XI Всероссийского конкурса молодёжи образовательных и научных организаций на лучшую работу «Моя законотворческая инициатива» (II том). – М.: Государственная Дума ФС РФ, НС «ИНТЕГРАЦИЯ», 2016. – С.119-120.

Диссертация состоит из 3-х глав, 7 параграфов и 130 страниц.

# Глава 1. Приватность в сети Интернет как проявление конституционного права на неприкосновенность частной жизни

## 1.1. Формирование и развитие института неприкосновенности частной жизни

Неприкосновенность частной жизни, будучи общечеловеческим личным правом, имеет крайне важное значение. Существенное ограничение данного права либо его игнорирование может выступать одним из ярких признаков авторитарных и тоталитарных политических режимов. В связи с этим неприкосновенность частной жизни нередко определяется исследователями как своего рода «линия сопротивления» между опытом тоталитаризма и требованиями правового государства [26, с. 34]. Любое демократическое, стремящиеся к идеалу правового государство предусматривает данное право в своём законодательстве, и, что не менее важно, – способствует его реализации своими гражданами. Особую роль это играет для России, где за последний век не единожды менялись политический режим и его правовая ориентация.

Обратившись к истории формирования и развития права на неприкосновенность частной жизни, можно заметить самые первые его зачатки ещё на позднем этапе общинно-родового строя. Ключевым этапом его возможного зарождения выступает выделение семьи от общей стаи, благодаря изобретению индивидуального очага. Если у раннего человека возможность реализации своей потребности в частной жизни была едва ли осуществима, поскольку он не мог выжить вне общины, то возникшая после возможность обособления стала одним из ростков индивидуализации. Вместе с тем ещё продолжительное время какого-либо концептуального или правового закрепления неприкосновенности частной жизни не возникало. Одним из ключевых этапов теоретического формирования права на неприкосновенность частной жизни выступает публикация в 1890 году двумя известными американскими юристами Сэмюэлом Уорреном и Луи Брендайсом

статьи «Право быть оставленным в покое» [21], где, наконец, была сформулирована начальная концепция неприкосновенности частной жизни. Ими был так же выведен принцип равной и полной защиты не только права собственности, но и личных прав. Кроме того, были определены правила, регулирующие судебные разбирательства в сфере защиты «права быть оставленным в покое». В частности, сведения, которые индивид сделал достоянием общественности лично, либо дал на то согласие не подпадают под защиту как охраняемая законом тайна. Также авторы отмечали, что правдивость публикуемой информации об индивиде, а равно наличие или отсутствие негативного настроя в отношении него не играют роли, если имело место нарушение его права на неприкосновенность частной жизни. В свою очередь не противоречащими праву на неприкосновенность частной жизни были определены публикации, отвечающие государственным или общественным интересам.

Названные авторы также отмечали, что неприкосновенность частной жизни выступает одним из древнейших прав человека, поскольку её зачатки в виде признания личностных прав в целом встречались во многих древних законах. Данная точка зрения выглядит вполне оправданной. Обратившись, к примеру, к древнерусским правовым источникам, мы так же увидим данные зачатки личностных прав. Например, «если кто у кого вырвет бороду или ус, то платить ему за обиду 12 гривен» – говорится в «Законе судном людем» [33, с. 95]. Подобное, свидетельствует о достаточно сильном развитии на Руси представлений о личности, так как заметное обезображивание, способное причинить и существенные нравственные страдания, ценилось дороже, чем незаметное увечье. При этом представление о вреде чести и достоинства пострадавшего, входящие и в современное понятие неприкосновенности частной жизни, выражались древнерусскими законодателями в так называемой «обиде», которая была серьёзнее ряда увечий, как, например, отрубленный палец, оцениваемый, в частности, лишь в 3 гривны.

Вместе с тем развитие права на неприкосновенность частной жизни в России заметно отличалось от стран Запада. Закрепляя основные права человека, государственные законы должным образом не определяли их гарантии и механизмы реализации. Значительную роль сыграли и нередкие смены политического курса. Так, после Октябрьской революции 1917 года советское правительство приняло решение, что в социалистическом государстве не может быть индивидуального права, а допустимы лишь коллективные права. Данная позиция отразилась в дальнейшем и в Конституции РСФСР 1918 года, которая провозглашала свободу совести, однако лишала граждан личной свободы, превращая право на труд в обязанность. Конституции СССР 1924 и РСФСР 1925 года так же практически не уделяли никакого внимания личным правам граждан. Основной приоритет отдавался социально-экономическим правам. Не было как таковой и «всеобщности»: все провозглашенные права закреплялись лишь за трудящимися.

Заметные новшества появились лишь в Конституция 1936 года, которая впервые провозгласила право на неприкосновенность частной жизни. Однако, в него входили лишь неприкосновенность личности, жилища и тайна переписки. Полностью отвергалось право частной собственности. Существует мнение, что таким образом советский законодатель привел личные права в соответствие с социалистическим устройством государства [26, с. 35]. Также имел место конфликт, заключающийся в провозглашении Конституцией личных прав, и их отрицанием советской идеологией. Объяснить подобный феномен можно, в частности, тем, что социализм предполагал отсутствие различий между личностью и обществом, а правовой статус личности, в свою очередь, связывался прежде всего с природой государства и общества.

Конституция уже 1977 года оставила заметный след закреплением института «личной жизни». При этом впервые говорилось именно о «личной жизни», а не о частной. Правоведами тех лет личная жизнь определялась как совокупность

взаимоотношении граждан, обусловленных их личными привязанностями, чувством симпатии, любви и дружбы. Содержание личной жизни включало в себя те категории, оглашение которых граждане по тем или иным причинам могли считать нежелательными: тайна завещаний, усыновления, врачебных диагнозов, дневниковых записей, денежных вкладов, фотографии и прочих. В данном случае мы так же можем видеть аналогичный конфликт. В силу своей идеологии СССР не мог дать советским гражданам право на «частную жизнь», поскольку слово «частное» несло негативную окраску необщественного, антисоциалистического. По этой причине при переводе «Международного пакта о гражданских и политических правах» произошла определённая подмена понятии, когда слово «privacy» было переведено как «личный», а не «частный». Учитывая, что понятие «частного» значительно шире понятия «личного», такая подмена понятии не могла не сказаться на конечном правоприменении. Несмотря на положительный сдвиг в области частных прав, Конституция СССР 1977 года по-прежнему оставалась коллективисткой, ставя интересы общества и государства над интересами отдельного человека, и позволяя гражданам реализовывать свои права и свободы исключительно в рамках социалистической идеологии. Только 22 ноября 1990 года Верховным Советом Российской Федерации была принята «Декларация прав и свобод человека и гражданина», которая закрепляла право на неприкосновенность частной жизни. Под влиянием Декларации была принята новая редакция Конституции РСФСР 1978 года, в тексте которой, наконец, появилась норма о частной жизни. В новой редакции впервые получила своё воплощение и новая концепция прав человека. В разделе «Государство и личность» были выделены две главы: «Права и свободы человека и гражданина» и «Обязанности граждан Российской Федерации», что в некоторой степени предвещало переход к новому правовому курсу.

В ныне действующей Конституции РФ 1993 года государство выступает представителем общества, в обязанности которого входит признание, соблюдение и защита прав и свобод человека и гражданина. Личные интересы приобретают для государства приоритетное значение перед публичными. Также Конституция признает права и свободы человека и гражданина неотчуждаемыми и принадлежащими каждому от рождения. Сохранилась и тенденция в сторону защиты прав и свобод человека и гражданина, что выразилось, в частности, в статье 23, предусматривающей право на неприкосновенность частной жизни, личную и семейную тайну, а также защиту чести и доброго имени. Гарантируется право и на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Вместе с этим допускается и ограничение этого права, которое, однако, может быть исключительно на основании судебного решения.

Что касательно отечественной доктрины, то вопросы толкования понятия «частной жизни» ей не игнорируются. В частности, М.В. Баглай отмечает, что содержание частной жизни «составляют те стороны личной жизни человека, которые он в силу своей свободы не желает делать достоянием других. Это своеобразный суверенитет личности, означающий неприкосновенность её «среды обитания» [23, с. 219]. Содержание частной жизни отражает естественное стремление каждого человека иметь собственный мир интимных и деловых интересов, скрытый от чужих глаз. Вместе с этим автор отмечает, что тайна не должна прикрывать какую-либо антиобщественную и противоправную деятельность. Вмешательство в частную жизнь должно происходить только на основании норм закона при наличии веских основании для подозрения или обвинения лица в совершении преступления, т.е. при возбуждении уголовного дела. В остальных же случаях частная жизнь неприкосновенна.

Своеобразно трактует термин «частная жизнь» Е.Г. Тарло, под которым он понимает некое качество жизни, определяемое реальной возможностью человека

осуществлять автономию и свободу в тои сфере жизни, которая может быть названа «частной» [35, с. 119]. В свою очередь выражаться оно может в виде права человека на автономию и свободу, права на защиту от вторжения других людей, органов власти или каких-либо общественных организации и государственных институтов. При этом лишь сам человек или в крайнем случае закон и суд, соответствующие требованиям правового, демократически организованного государства, могут разрешить такое вторжение.

Весьма интересной представляется концепция правоведа и действующего судьи Конституционного суда РФ Л.О. Красавчиковой, которая даёт развёрнутое понятие частной жизни, разбирая несколько её сторон. По её мнению, частная жизнь проявляется по-разному и имеет множество граней. Она складывается из «интимной стороны», определяющей индивидуальность личности и её привычки, «семейной стороны» – складывающиеся отношения в семье, «организационной стороны» – установление распорядка дня, избрания места учёбы или работы, «оздоровительной стороны» – поддержание здоровья, «стороны досуга» – отдых и развлечения, «коммуникативной стороны» – установление личных контактов с друзьями, знакомыми и т.д [22, с. 91].

Право на неприкосновенность частной жизни имеет и свои признаки. В частности, Э.Р. Аберхаев [22, с. 92] выделяет следующие:

А) Право на неприкосновенность частной жизни принадлежит конкретному гражданину в силу закона, неотчуждаемо и непередаваемо им другим лицам иным способом, кроме как в случаях, предусмотренных законом.

Б) Оно является абсолютным. Управомоченному лицу противостоит неопределённый круг лиц, обязанных воздержаться от нарушения его права.

В) Для данного права характерно наличие двух правомочий: возможности управомоченного лица требовать от неопределённого круга обязанных лиц

воздерживаться от нарушения его права и его возможность прибегнуть к установленным законом мерам защиты в случае нарушения его права.

Нельзя не отметить, что и в праве Совета Европы проблемам частной жизни уделяется серьезное внимание. При этом во многом современное понимание частной жизни сформировалось не без его непосредственного влияния. Так, праву на уважение частной и семейной жизни посвящена статья 8 Конвенции о защите прав человека и основных свобод от 4 ноября 1950 г. Согласно её положениям каждый имеет право на уважение его личной и семейной жизни, а также жилища и корреспонденции. Конвенцией 1950 г. не допускается и вмешательство со стороны публичных властей в осуществление этого права. Вместе с тем ей предусматриваются исключения, когда, в частности, такое вмешательство предусмотрено законом и необходимо в интересах национальной безопасности, общественного порядка, экономического благосостояния страны, а также в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности, или защиты прав и свобод других лиц [2].

Имеются в праве Совета Европы и свои особенности толкования частной жизни. В частности, как отмечает Европейская комиссия по эффективности правосудия, для многочисленных англосаксонских и французских авторов данное право — это право лица жить как хочется, не опасаясь огласки. Однако, оно не ограничивается только этим. Право на уважение частной жизни включает в себя и право на установление и поддержание отношений с другими людьми, особенно в эмоциональной сфере, в целях развития и реализации собственной личности. Впоследствии эта позиция была подтверждена и Европейским судом по правам человека в решении от 16 декабря 1992 г. по делу «Нимитц против Германии», в котором было установлено, что нельзя ограничивать частную жизнь только интимным кругом, где каждый может жить так, как он хочет, и тем самым полностью исключать внешний мир из этого круга. Было отмечено, что уважение

частной жизни до некоторой степени включает так же право устанавливать и развивать отношения с другими людьми. В решении от 22 февраля 1994 г. по делу «Бургхарц против Швейцарии» Европейский Суд по правам человека также обратил внимание на тот факт, что частная жизнь распространяется и на отношения с другими людьми в профессиональной области и в сфере бизнеса, и не исключает публично правовые аспекты. Стоит отметить, что на этом расширительное толкование данного вопроса правом Совета Европы не останавливается. В частности, отмечается, что право на уважение жилища не случайно содержится именно в ч.1 ст. 8 Конвенции 1950 г. рядом с правом на уважение личной и семейной жизни и тайны переписки [35, с. 120]. Данная точка зрения обуславливается тем, что жилище так же выступает и своего рода «хранилищем» личных тайн граждан. Кроме того, практика Европейского Суда по правам человека свидетельствует о том, что одним из элементов права на частую жизнь является так же и право человека на благоприятную окружающую среду. Несмотря на то, что сам текст Конвенции 1950 г. не содержит положений об экологических правах, указанные права в последние годы получили защиту в ряде постановлении Европейского Суда по правам человека, выводящих их из иных прав, содержащихся в Конвенции и, прежде всего, из права на уважение частной и семейной жизни, закрепленного в восьмой статье [35, с. 121]. Подобное подчёркивается, в частности, решением от 9 июня 2005 г. по делу «Фадеева против Российской Федерации», где Европейский Суд по правам человека сделал вывод о том, что государство не сумело найти справедливый баланс между интересами общества и эффективным удовлетворением прав заявителя на уважение её дома и частной жизни, что выражалось в непредставлении заявителю никакого эффективного решения, способствующего её переезду из загрязнённого района, ставшего опасным из-за нарушающей природоохранное законодательства деятельности предприятия. Вызывает интерес также и толкование понятия «корреспонденция» в праве Совета Европы. Первоначально данный термин

толковался Европейским Судом по правам человека в буквальном смысле, означая отправку сообщения в виде письма. Однако, по мере возникновения новых прецедентов, толкование «корреспонденции» стало расширяться. В частности, в особом мнении судьи сэра Джеральда Фицмориса по делу «Голдер против Соединенного Королевства» (решение Европейского Суда по правам человека от 21 января 1975 г.) имела место позиция, заключающаяся в том, что термин «корреспонденция» обозначает письменную корреспонденцию, которая включает, возможно, и телеграммы или сообщения по телексу, но не устную коммуникацию от человека к человеку по телефону или при помощи знаков либо сигналов. Также, важным этапом стал и охват понятием «корреспонденции» не только отосланных, но и неотправленных писем что, несомненно, расширило сферу действия данного права. Несколькими годами позже, уже в 1978 году, в деле «Класс против Германии» Европейский Суд по правам человека впервые дал расширительное толкование термина «корреспонденция», отметив, что, хотя телефонные разговоры конкретно не указаны в п. 1 ст. 8 Конвенции 1950 г., такие разговоры входят в понятие «личная жизнь» и «корреспонденция». Аналогично Европейский Суд по правам человека расширял понятие «корреспонденции» и в дальнейшем.

Таким образом, мы видим, что формирование и развитие института неприкосновенности частной жизни как в мире, так и в России было непростым. Вместе с этим прослеживается заметная глобальная либерализация и направление в сторону защиты прав и свобод человека и гражданина, что в итоге затронуло и Россию, даже несмотря на осложнённое многими факторами развитие данного института в её правовой системе.

### 1.2. Понятие тайны переписки и иных сообщений

«Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» – провозглашается Конституцией РФ. Чтобы дать понятие права на тайну переписки и иных сообщений, следует прежде

всего определить, что включает в себя само понятие «тайны», а также виды переговоров и сообщений, которые она охватывает.

В российской юридической науке разработкой теоретико-правового понятия «тайна», как отмечает С.А. Куликова [25, с. 225], активно занимаются специалисты в области информационного права и информационной безопасности, в работах которых мы можем встретить две концепции. В рамках первой «тайна» рассматривается в виде информации, доступ к которой ограничен. Под «тайной» в данном случае понимаются сведения, не являющиеся общеизвестными или общедоступными, разглашение которых может причинить вред чьим-либо интересам, и их обладатель, в свою очередь, принимает меры по охране этих сведении□. Вторая концепция рассматривает «тайну» с другого угла, характеризуя её как особый правовой режим информации, не отождествляя с самой информацией или сведениями как таковыми. Особый правовой режим, в свою очередь, включает в себя комплекс правовых средств в виде взаимодействующих между собой дозволении□, запретов и обязательств, способствующих ограничению доступа и распространения определенных видов информации. Похожий двойственный подход, но в ином теоретико-правовом аспекте, просматривается и во многих работах конституционно-правовых исследователей. С одной стороны, «тайна» рассматривается ими в качестве самостоятельного права – «права на тайну». В частности, это может означать предоставление лицу возможности контролировать информацию о самом себе, препятствовать разглашению сведении□ личного или интимного характера, которые оно не желает делать достоянием третьих лиц, либо общественности. С другой стороны, «тайна» рассматривается уже в качестве гарантии реализации права, обеспеченной обязанностями, возложенными на уполномоченные органы и лица. Грани охраняемой указанными субъектами тайны определяются, в свою очередь, законодателем.

Таким образом, понятие «тайны» является сложным и многоаспектным. С одной стороны, она может рассматриваться как круг информации, доступ к которой ограничен, а также как право лица на выбор ограничения распространения информации о себе. С другой же – как особый правовой режим, включающий в себя систему обязанностей, запретов и дозволений, способствующих ограничению доступа и распространения определенных видов информации.

Говоря о видах переговоров и сообщений, стоит отметить, что если «телефонные переговоры», «почтовые и телеграфные сообщения» не нуждаются в каком-то отдельном толковании, то так называемые «иные сообщения» страдают отсутствием точной определённости. В частности, могут возникать вопросы по поводу отнесения электронных сообщений и писем, а также аудио- и видео-переговоров к тому или иному из перечисленных видов. Тем не менее, данные формы связи должны быть отнесены к категории «иных сообщений», поскольку в отличие от аналоговых телеграфных, телефонных или почтовых сообщений, где общий алгоритм функционирования в целом общеизвестен, они действуют по иному, цифровому протоколу, сохраняя при этом основную цель – передачу личной информации, и могут основываться как на закрытых, так и открытых общественности моделях. Единственное, но не обязательное, что может их объединять – это использование сети Интернет для связи. Однако, в некоторых случаях и подключение к Интернету может быть не обязательным. Определёнными приложениями могут использоваться сети Wi-Fi или связь по протоколу Bluetooth, объединяющие находящиеся рядом мобильные устройства в альтернативную сеть, способную функционировать даже при отсутствии сигнала сотовых сетей. Ярким примером можно выделить использование мессенджера FireChat во время протестов в Гонконге в 2014 году [81]. Несмотря на попытки властей нарушить каналы связи протестующих путём отключения сотовых сетей, последними использовался данный сервис, не требующий сети Интернет для полноценного функционирования.

Используя протоколы передачи Wi-Fi и Bluetooth мессенджер устанавливает прямое соединение между двумя мобильными устройствами на расстоянии до 70 м. При этом большое скопление пользователей не перегружает сеть, а только расширяет её радиус.

Возвращаясь к электронным сообщениям, следует отметить, что существует ряд проблем по защите права на тайну переписки в указанной форме. В частности, Е.В. Митин [27, с. 272] выделяет среди них: отсутствие правового регулирования использования электронных почтовых ящиков, недостаточный опыт судебной практики в указанной сфере, а также недостаточную квалификацию сотрудников правоохранительных органов, в том числе следственных, в области функционирования систем электронного общения. Стоит отметить, что на данный момент произошёл определённый сдвиг в плане нормативного регулирования. В частности, был принят ряд законов, регулирующих работу сервисов электронных сообщений, возложивших на их организаторов определённые обязательства. Вместе с этим, указанные нормативные акты, сохранили ряд конфликтов и недочётов, о которых будет так же изложено в данном исследовании.

### 1.3. Приватность в сети Интернет: понятие, особенности и элементы

Рассмотрев основные этапы формирования права на неприкосновенность частной жизни, а также охарактеризовав такие его атрибуты как тайна переписки, телефонных переговоров и иных сообщений можно сделать вывод, что право на приватность в сети Интернет по мере развития технического прогресса так же становится её неотъемлемой частью. В подтверждение этого можно выделить многие общие, родственные черты данных отношений: в частности, личная коммуникация между лицами, способная выражаться через специальные средства, которые, меняя своё устройство и применяемые технологии на протяжении времён, не утрачивали свою основную суть – передачу конфиденциальной информации: письма, телефон, SMS.

Схожим образом на замену аналоговым средствам приходят цифровые: сеть Интернет и средства Интернет-коммуникации (мессенджеры, аудио- и видеосвязь, социальные сети и другие). Общественные отношения в указанной сфере за последние годы получили настолько обширное развитие, что игнорирование их становится невозможным. Вместе с этим, сложность указанных отношений, их срастание с повседневностью, а также их техническое обеспечение говорят о необходимости максимально осторожного подхода к их регулированию. Отдельно стоит отметить, что само понимание Интернет-приватности может быть достаточно дискуссионным из-за её субъективного понимания. Имеет место и недостаточная доктринальная разработанность данной сферы, без обращения к которой, к сожалению, страдает и качество нормотворчества. В стремлении закрыть имеющиеся проблемы современной доктрины, на основе анализа приведённой информации можно дать следующее определение Интернет-приватности:

Под Интернет-приватностью следует понимать атрибут права на неприкосновенность частной жизни, общественные отношения, возникающие при реализации человеком его права на конфиденциальную переписку и общение через средства Интернет-коммуникации, и (или) его стремлении сохранить своё пребывание в сети Интернет тайным от посторонних глаз [29, с. 132].

Как мы видим, указанное определение включает в себя два элемента, которые возможно определить, как тайну Интернет-сообщений и Интернет-анонимность.

Под тайной Интернет-сообщений следует понимать реализацию человеком права на конфиденциальность его общения и переписки через средства Интернет-коммуникации: как правило мессенджеры, сервисы аудио- и видеосвязи, а также личные сообщения в социальных сетях.

Под Интернет-анонимностью, в свою очередь, – стремление сохранить в тайне своё пребывание в сети Интернет в целом. Инструментами реализации последнего

могут выступать VPN – виртуальные частные сети, различного рода анонимайзеры, сервис Tor и аналогичные ему.

Стоит отметить, что указанные элементы могут как коррелировать друг другу, так и сосуществовать в раздельности. Например, человек может не ставить целью сокрытие своего Интернет-трафика как такового, а лишь желает конфиденциальности исключительно своей Интернет-переписки. В свою очередь иной пользователь может желать, как сохранности в тайне самой переписки, так и всего трафика, включая посещаемые им веб-сайты. Цели же сокрытия подобного рода информации могут быть различны. Например, нежелание сбора различными сервисами каких-либо данных о пользователе. Так, многие крупные Интернет-компании осуществляют круглосуточную слежку за пользователями, собирая так называемые «Большие данные» (Big Data), которые используются в рекламных и иных целях. При этом в последние может входить обширный перечень сведений: IP-адрес, поисковые запросы, характеристики устройства и его операционной системы и многое другое, благодаря которому формируется общий электронный образ каждого из пользователей, на основании анализа которого может, к примеру, предлагаться целевая реклама. В частности, человек, интересующийся автомобилями или спортом, вводящий соответствующие поисковые запросы и посещающий тематические веб-сайты, будет видеть тематические рекламные блоки, подсказки или видеоролики, даже, порой, не подозревая об истинной причине таких совпадений. С одной стороны, конечно, указанные вещи можно даже назвать полезными и стимулирующими, однако, подобный расклад может и многих не устраивать даже при условии некоторого обезличивания вышеперечисленных данных. Этичность подобного сбора личной информации, что важно, – без уведомления пользователя, по-прежнему сохраняет свою дискуссионность.

Кроме того, не утихло по-прежнему и эхо прецедента Эдварда Сноудена, – бывшего сотрудника Агентства национальной безопасности (АНБ) США,

раскрывшего программу глобальной слежки американских спецслужб как за своими, так и иностранными гражданами, и нашедшего на данный момент своё пристанище на территории Российской Федерации [74]. Средства анонимизации выступают в данном случае одним из средств защиты от подобного рода шпионажа. Также далеко не каждый готов делиться своими личными данными и со своим Интернет-провайдером, который может осуществлять их сбор и хранение в различных целях, в том числе и в коммерческих, собирая «Большие данные» своих абонентов.

Стоит отметить, что, порой, данными средствами пользуются и для противоправных целей, что, очевидно, не может подпадать под защиту законом. Вместе с этим, умаление прав добросовестных пользователей является так же недопустимым, что требует, в свою очередь, должной осторожности при вмешательстве в данную сферу. При этом указанные инструменты анонимизации сами по себе не могут расцениваться как исключительно преступные орудия, поскольку, как и многие другие объекты, вроде автомобилей, мобильных телефонов и даже столовых приборов, могут использоваться как во благо, так и для совершения различных правонарушений.

Таким образом, мы видим, что Интернет-приватность, будучи одной из составных частей права на неприкосновенность частной жизни, является в то же время неоднородной и по-своему уникальной категорией, включающей в себя элементы, способные как коррелировать друг другу, так и сосуществовать в раздельности. Вместе с этим указанные элементы – тайна Интернет-сообщений и Интернет-анонимность выступают в том числе и уникальными признаками приватности в сети Интернет, которые аналогично могут говорить о ней как в совокупности, так и при наличии хотя бы одного из них. В следующей главе нами будут рассмотрены подробнее вышеуказанные элементы приватности в сети Интернет, выявлены пределы вмешательства в данную сферу и определены общие проблемы в их реализации.

# Глава 2. Проблемы реализации права на приватность в сети Интернет

## 2.1. Пределы вмешательства государства в тайну Интернет-сообщений

Одной из ключевых проблем реализации права на приватность в сети Интернет, определённо, можно назвать дискуссионность пределов вмешательства государства в сферу приватности, в том числе касательно тайны Интернет-сообщений, под которой следует понимать реализацию человеком права на конфиденциальность его общения и переписки через средства Интернет-коммуникации. На одной чаше весов мы видим такие категории, как неприкосновенность частной жизни, тайна переписки и сообщений, на другой же – необходимость борьбы с преступностью, обеспечение прав и свобод личности, а также общественного благополучия.

Стоит отметить, что зачастую дискуссия касательно данного вопроса сводится к превалированию одной из позиций и умалению другой. Данный подход создаёт дисбаланс, поскольку лишь противопоставляет публичные и приватные интересы друг другу. С одной стороны, отсутствие какого-либо контроля в данной сфере может стимулировать рост правонарушений, создавая иллюзию полной безнаказанности, с другой же – тотальный контроль и массовая слежка нарушают право на неприкосновенность частной жизни и тайну переписки добропорядочных граждан, способствует их необоснованной самоцензуре даже в конфиденциальном общении.

Как отмечает Ю. В. Шкудунова [36, с. 68], несмотря на сложность и различия концептов публичности и приватности, необходим баланс личных и общественных интересов, с чем сложно не согласиться. Пользовательская переписка может содержать очень много информации о личности как самого пользователя, так и его собеседников, и даже третьих лиц. Потому любые субъекты, будь то сам пользователь или сервис Интернет-коммуникации должны пропорционально

разделять ответственность за её сохранность и конфиденциальность. Если на плечах сервиса лежит ответственность за общую безопасность от атак злоумышленников, и сохранность личных данных в целом, то пользователю, в свою очередь, так же не стоит забывать о должных мерах предосторожности для обеспечения своей конфиденциальности.

Зачастую именно беспечность и пренебрежение самыми простыми правилами безопасности со стороны пользователя становятся причиной возникновения множества неприятных ситуаций для него самого, либо его собеседников. Так же играет немаловажную роль в данном вопросе и государство, которое, с одной стороны, должно способствовать возможности реализации гражданами их права на неприкосновенность частной жизни, не создавая им в этом препятствий, а с другой обеспечивать безопасность личности и общества, состоящего из совокупности этих личностей, в целом. Любое вмешательство государства должно быть обоснованным и нести цель защиты прав и законных интересов его граждан.

Одним из негативных примеров такого вмешательства можно назвать, в частности, многоизвестную историю Эдварда Сноудена, – бывшего сотрудника Центрального разведывательного управления (ЦРУ) и Агентства национальной безопасности (АНБ) США, нашедшего убежище на территории Российской Федерации. По раскрытой им информации миру стало известно о программе глобальной международной слежки спецслужбами США за частной жизнью как граждан страны, так и за иностранными гражданами в 60 странах мира. Сноуденом была так же обозначена возможность американских спецслужб просматривать электронную почту, прослушивать голосовые и видеочаты, просматривать фотографии, видео, отслеживать пересылаемые файлы, а также узнавать другие подробности из социальных сетей. Перехватывались телефонные звонки, в том числе иностранных политиков и чиновников. История Эдварда Сноудена оставила глобальный отпечаток на иллюзии всеобъемлющей приватности в сети Интернет и

вызвала множество споров. Многие добропорядочные пользователи, опасающиеся за свою приватность, принялись за поиск оптимальных вариантов защиты своих законных прав.

Стоит отметить, что отдельную ветвь споров вызвал сам факт разглашения со стороны Эдварда Сноудена подобной информации. Данная этическая проблема вызвала заметный интерес среди зарубежных правоведов. В частности, как отмечает Д. Хайс [20, с. 12], поступок Сноудена можно рассматривать с двух подходов. С точки зрения первого Сноуден выступает героем, поскольку проявил храбрость и предпринял попытку изменить безнравственное положение дел, выступая против одной из крупнейших организаций, существовавших когда-либо в истории человечества: правительства США. Проявляя принципиальность, он демонстрировал аморальность данной государственной программы слежки в ущерб собственной безопасности и свободе в пользу информирования мира о секретных правительственных программах, которые функционируют без общественного согласия. С другой точки зрения Сноуден рассматривается как правонарушитель, нарушивший трудовой договор, а также разгласивший сведения, составляющие государственную тайну. При этом, как отмечает М. Фридман [19, с. 23], раскрытие государственной тайны Сноуденом потенциально могло нанести большой ущерб государственным структурам, а также подвергнуть опасности лиц, осуществляющих свою деятельность в указанной сфере. Вместе с этим, автор замечает, что американские законы не допускают каких-либо обстоятельств, в которых информаторы могли бы легально сообщать о незаконной деятельности общественности.

Касательно самих средств Интернет-коммуникации, то многие из них учли данные запросы и постарались адаптировать свой продукт под нужды максимального объёма аудитории, стараясь сочетать удобство и приватность. Кроме того, на фоне резкой волны интереса выросла и категория особо защищённых

мессенджеров, ставящих исключительно в свой главный приоритет и даже идеологию защиту конфиденциальности переписки своих пользователей. На фоне остальных они выделяются усиленными методами шифрования данных, минимальным набором необходимых данных пользователя при его регистрации, нахождением серверов на территории государств, лидирующих в рейтингах свободы слова, Интернета и печати, и прочими особенностями.

Стоит отметить, что, в частности, Конституцией РФ в статье 23 предусматривается защита тайны переписки пользователя, как и в любом демократическом правовом государстве: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений». При этом, как Конституцией РФ, так и международными актами предусматривается законное ограничение этого права, например, на основании судебного решения. Основанием же для вынесения подобного решения может выступать совершение лицом преступления и соответствующая необходимость извлечения доказательств из его личной переписки. Однако, здесь мы можем увидеть назревающий конфликт. С одной стороны, в ряде случаев такие данные, действительно, могут помочь в расследовании, но с другой – вопрос границ вмешательства в тайну переписки, пусть и потенциального правонарушителя, может быть достаточно дискуссионным. Также возможен риск должностных злоупотреблений в случае необоснованного обвинения лица. Кроме того, далеко не каждый преступник будет непосредственно обсуждать свои преступные планы через сеть Интернет, либо же может их «маскировать» под обычную житейскую, либо иную отвлечённую беседу. Последнее, как правило, делает извлечённый текст переписки с точки зрения доказывания совершенно бесполезным. Кроме того, в ряде случаев преступниками и вовсе не используются какие-либо средства шифрования. В частности, во время террористических атак в Париже в 2015 году преступниками использовались одноразовые мобильные телефоны с сим-картами, оформленными на третьих лиц. Какие-либо шифрованные

электронные сообщения или чаты террористы не использовали. Единственный аккаунт электронной почты, привязанный к одному из устройств террористов, как было установлено правоохранительными органами, был пуст и так же не использовался для связи или координации действий [37].

Другой аспект данного конфликта заключается том, что несмотря на сотрудничество многих участников рынка с правоохранительными органами в расследовании преступлений, не все из них готовы идти на это в полной мере. Некоторые из них могут, в частности, аргументировать это тем, что не находятся в юрисдикции государства, правоохранительные органы которого осуществили запрос, а также и вовсе заявлять, что приватность и сохранность любых данных их клиентов для них является высшей ценностью. Отдельный дискурс может вызвать и понимание правомерности разными сторонами. В частности, к сервису могут поступать запросы от государственных органов авторитарных или тоталитарных государств, либо прочих стран, чьи нравы могут не совпадать с ценностями сервиса. В подобных случаях у сервиса возникает нелёгкий морально-финансовый выбор: либо сотрудничать по каждому из запросов, но предать свои идеалы, либо продолжать следовать своим ценностям, рискуя оказаться под запретом и лишиться рынка вышеуказанных стран. Так, в 2010 году по подобной причине компания Google была вынуждена покинуть рынок Китайской Народной республики, в связи с отказом заниматься дальнейшей цензурой поисковых запросов [46]. Данная проблема, возможно, выступает одной из ключевых в отсутствии консенсуса между государством и сервисами. В конечном итоге главными пострадавшими в подобном противостоянии остаются пользователи, которых лишили привычных и удобных им сервисов, а также выбора на основе справедливой конкуренции.

Также стоит отметить, что при использовании определённых видов шифрования организаторы средств Интернет-коммуникации могут вовсе не иметь доступ к переписке своих пользователей, поскольку она шифруется

индивидуальным ключом и хранится только на устройствах собеседников. Доступ к ней правоохранительных органов возможен лишь в случае попадания устройства в их руки. Однако, даже в этом случае возможность её извлечения не является стопроцентной [30, с. 119]. Невозможность правоохранительными органами извлечь необходимую информацию, в свою очередь, уже стало объектом множества обсуждений во многих странах. В частности, со стороны бывшего директора ФБР США Джеймса Коми подверглись резкой критике такие компании, как Google и Apple за их наработки средств шифрования смартфонов, из-за которых сотрудники правоохранительных органов не могли легко получить доступ к информации, хранящейся на устройствах даже при наличии судебного ордера. Ещё более жёсткую критику выразил Джон Эскаланте, – главный детектив департамента полиции Чикаго, выразивший обеспокоенность в том, что, в частности, средства шифрования компании Apple стимулируют правонарушителей использовать именно их устройства [44]. Данная проблема способна вызывать долгие проволочки и разбирательства, не приводящие в итоге ни к чему благоприятному. Итогом же, как правило, становится либо блокировка Интернет-ресурса и иные запреты, либо же просто пустая трата времени в целом. При этом, как было отмечено выше, уже в первом случае нарушаются права добропорядочных пользователей, не использующих сервис или устройство в преступных целях.

В качестве рекомендации по решению данного конфликта можно предложить совместную выработку государствами и участниками рынка единой, прозрачной и понятной всем политики в данной сфере. Так, в рамках выступления на ежегодном форуме Всемирной встречи на высшем уровне по вопросам информационного общества о необходимости разработки конвенции в сфере регулирования Интернета под эгидой ООН заявил замминистра связи и массовых коммуникаций РФ Рашид Исмаилов [97]. Что касательно возможных вариантов подхода к данному вопросу, в частности, возможна выработка подходов, выражающихся в сохранении

неприкосновенности личных переписок пользователей, но в блокировке публичных страниц, аккаунтов, групп или чатов, пропагандирующих терроризм и иную преступную деятельность, а также выявлению их создателей и, по крайней мере, активных участников для дальнейших разбирательств. Организация и существование подобного рода чатов или каналов не подпадает под защиту какой-либо из охраняемых тайн, а являются вполне публичной категорией, нарушающей как частные, так и общественные интересы, представляя существенную опасность. Помимо нарушения требований закона, подобная деятельность всегда противоречит и условиям пользовательского соглашения практически любого сервиса, запрещающего использовать сервис в преступных целях. Например, в октябре 2017 года, согласно отчёту главы сервиса «Telegram» Павла Дурова, было заблокировано более 8500 каналов, связанных с терроризмом [54], что можно назвать одним из результатов подобного компромиссного сотрудничества. Тем не менее, отказ сервиса в предоставлении ключей шифрования личных переписок пользователей привёл в конечном итоге к блокировке сервиса в РФ по решению суда [103]. Что касательно последнего, то стоит осознавать вероятность технической невозможности передачи подобных данных при использовании сервисами определённых видов шифрования (например, при хранении индивидуального ключа шифрования исключительно на устройстве), а также безопасности передачи подобной информации лицам, не имеющим отношения к функционированию сервиса. Стоит понимать, что сам факт наличия ключа шифрования от каждой личной переписки, а тем более расширение круга лиц им обладающего, не скажутся на уровне безопасности сервиса в целом. Кроме того, с этической стороны данный подход фактически уравнивает добропорядочных пользователей, чьи личные сообщения охраняются законной неприкосновенностью, и правонарушителей, тайна переписки которых может быть ограничена по решению суда, поскольку с передачей ключей шифрования предоставляется доступ к сообщениям как тех, так и других

одновременно. На фоне этого куда более этичным выглядит расшифровка самим сервисом отдельных сообщений по решению суда, либо при невозможности этого по той или иной причине – передача метаданных о контактах, продолжительности аудио- или видеозвонков, времени отправки сообщений. Последние, к слову, могут представлять достаточно ценную информацию при расследовании, давая установить сам факт и время связи участвующих в деле лиц. Однако и здесь, отдельным интересным моментом выступает то, что некоторые сервисы или программное обеспечение (ПО) могут разрабатываться и поддерживаться собственным сообществом (например, «открытое ПО» с особой лицензией), а не каким-либо конкретным разработчиком, что затрудняет даже потенциальные запросы правоохранительных органов, не говоря о реагировании на них.

Дискуссионным выступает и вопрос о допустимости мониторинга общего потока пользовательских сообщений, сбора их и хранения. На одной чаше весов здесь тезис о безосновательности опасений добросовестных граждан, чьи сообщения могут так же мониториться и храниться. В противовес же данной точке зрения можно выделить факт потенциальной небезопасности данных мер, особенно в части их хранения. Кроме того, сам мониторинг, если он не осуществляется исключительно самим же организатором распространения информации (мессенджеры и прочие Интернет-сервисы), может предполагать стороннее вмешательство в его трафик, пусть и со стороны правоохранительных органов, что уже выступает его фактической компрометацией. Принятие подобных спорных инициатив без должного информирования населения и учёта его мнения может лишь расколоть доверительные отношения между обществом в целом, его отдельных групп и государством. Так, в марте 2018 года в Нидерландах прошел референдум, фактически расколовший общество на два лагеря [96]. Жителям страны предлагалось выразить свое отношение к закону, расширяющему полномочия спецслужб и дающему им возможность отслеживать Интернет-трафик граждан,

прослушивать телефонные переговоры, взламывать электронные устройства подозреваемых, и, что немаловажно, предоставлять собранные сведения зарубежным спецслужбам. Даже несмотря на предусмотрение проектом закона такой формы контроля, как разрешение министра внутренних дел, результаты референдума показали, что сопротивление его принятию оказалось намного выше, чем ожидали власти. Победа противников закона, пусть и с минимальным перевесом, дала властям сигнал о существенном неприятии обществом подобной инициативы. Хотя и результат данного референдума не имеет обязательной силы, премьер-министр страны Марк Рутте, будучи сам сторонником закона, обещал со всей серьезностью отнестись к голосованию.

Возвращаясь к мониторингу пользовательских сообщений и трафику, отдельным вопросом выступает его законодательная обоснованность, а также соответствие принципу соблюдения прав и свобод человека и гражданина. В частности, статьёй 23 Конституции Российской Федерации допускается ограничение права на тайну сообщений только на основании судебного решения. Таким образом, не может допускаться слежка в отношении неопределённого круга граждан, когда законодательством государства предусматривается возможность ограничения подобного права исключительно на основании решения суда и в отношении конкретного лица или определённой группы лиц, имеющей отношение к рассматриваемому делу.

Таким образом, нами было рассмотрено право на тайну Интернет-сообщений как элемент приватности в сети Интернет, являющейся неотделимой частью конституционного права на неприкосновенность частной жизни. Нами были рассмотрены и пределы вмешательства государства в тайну Интернет-сообщений, а также даны рекомендации, наиболее сочетающие, на наш взгляд, личные и общественные интересы, касательно подхода к правовому регулированию в данной сфере.

## 2.2. Анонимность в сети Интернет и проблемы её реализации

Рассмотрев первый элемент приватности в сети Интернет, – тайну Интернет-сообщений, необходимо обратить внимание так же и на второй – Интернет-анонимность, её особенности и проблемы реализации.

Под анонимностью в сети Интернет, как было определено ранее, понимается стремление лица сохранить в тайне своё пребывание в сети Интернет. В свою очередь инструментами реализации могут выступать VPN – виртуальные частные сети, различного рода анонимайзеры, сервис Tor и сервисы, аналогичные ему. Необходимость же в этом может возникать в различных ситуациях. В частности, для ухода от слежки со стороны международных Интернет-корпораций, собирающих «Большие данные» пользователей в рекламных и иных целях. Далеко не каждому может быть приятно осознавать, что его поисковые запросы, списки посещаемых Интернет-сайтов, а в некоторых случаях и более персональные данные были использованы, а то и вовсе переданы третьим лицам для использования в рекламных и иных целях. При этом, нередко пользователь может вовсе не иметь представления о данных, которыми он делится с сервисом, а также конкретных случаях их использования. В частности, Интернет-компанией Google в очередной из редакций пользовательского соглашения было сообщено о намерении использовать в рекламе имена и фотографии своих пользователей [45]. Стоит отметить, что самой компанией при этом была дана возможность отключить сбор и использование подобных сведений, однако, далеко не все компании могут быть достаточно лояльны, в том числе и касательно уведомления об изменении пользовательского соглашения в одностороннем порядке. Вместе с этим круг собираемой информации о пользователях может быть значительно широк, и зачастую пользователю необязательно даже иметь аккаунт какого-либо из сервисов. Чтобы осознать примерный масштаб мы можем обратиться к Интернет-сайту той же компании Google [83]. Помимо самой поисковой системы, компанией осуществляется сбор

данных о действиях пользователей и на её дочерних сервисах, как, например, YouTube. Среди указанных данных фигурируют, в частности, поисковые запросы, список всех посещаемых сайтов и просматриваемых видео, а также местоположение пользователей, их IP-адреса и даже данные с их устройств, конкретный перечень которых компанией не раскрывается.

При использовании аккаунтов глобальных международных сервисов к перечисленным ранее сведениям добавляются и содержание электронных писем, контакты, загруженные фотографии, видеозаписи и документы. Поступают в распоряжение компании и такие личные данные, как имя, пол, дата рождения, номер телефона и т.д. Аналогичный перечень в виде персональных данных пользователей, а также их IP-адрес и конфигурацию компьютера собирает компания Яндекс [91]. Что касательно обоснования сбора и хранения столь обширного круга персональных данных, компаниями, как правило, приводятся аргументы в виде улучшения работы и точности оказываемых ими услуг, персонализированные рекомендации контента, в том числе рекламного характера. С одной стороны, публикация сведений о собираемых данных крупными Интернет-компаниями создаёт определённую атмосферу прозрачности данных взаимоотношений, предупреждая пользователя ещё до, либо на этапе его регистрации. Однако, с другой стороны, пользователям, не желающим делиться таким перечнем сведений о себе, приходится использовать указанные сервисы в связи с отсутствием вменяемых альтернатив, либо же вовсе фактической монополии компаний в определённых сферах, даже и не регистрируя там свою учётную запись. При этом на Интернет-ресурсах далеко не всех компаний могут быть настройки конфиденциальности для неавторизированных пользователей. Побуждение же к регистрации влечёт за собой передачу компании ещё большего круга личных данных. Возникновение подобной ситуации фактически вынуждает пользователя прибегать к инструментам анонимизации для сокрытия, либо «разбиения» и «перемешивания» своих данных ради невозможности их

использования, наподобие действия шредера. В качестве если не решения, то хотя бы минимизации вышеуказанной проблемы, было бы крайне желательно обеспечение со стороны как можно большего числа Интернет-сервисов возможности настройки передаваемых им данных со стороны неавторизированных пользователей, а также наглядного уведомления с полным перечнем собираемых компанией данных. Также должно учитываться согласие пользователя на передачу указанных данных, пусть даже и в обезличенном виде.

Важным моментом выступает и прозрачность операторов связи касательно собираемой ими информации в процессе предоставления услуг связи. Особенно это важно при ознакомлении с пользовательским соглашением. Однако, нередко данная информация может быть недостаточно доступна для пользователей. Так, экспертами правозащитных организаций «Роскомсвобода» и «Общество защиты Интернета» было проведено исследование «Рейтинг открытости мобильных операторов», направленное на оценку политик и практик деятельности четырех крупнейших российских операторов мобильной связи (Теле2, Билайн, Мегафон, МТС). Одним из ключевых параметров оценивая оказались доступность пользовательских соглашений и политики конфиденциальности. Экспертами было установлено, что все рассмотренные операторы мобильной связи размещают на своих официальных сайтах в публичном доступе для широкого круга лиц собственные Правила и Политику. При этом экспертами было отмечено, что формат представления данной информации достаточно сложный. Документы, размещенные в открытом доступе, написаны нередко языком юридического канцелярита, отличаются большим объемом и трудностью восприятия. В некоторых случаях указанные документы достаточно сложно найти на сайте и получить для ознакомления в удобном виде [24, с. 14].

Кроме того, стоит понимать, что никакие, даже очень крупные компании, заверяющие о должной защите персональных данных своих клиентов, не

застрахованы от их утечек по собственной вине, либо внешним факторам. Так, в марте 2018 года компания и одноимённый сервис Facebook оказались в центре крупного скандала в связи с утечкой данных порядка 50 миллионов человек. Одним из ключевых участников скандала оказалась и британская аналитическая компания Cambridge Analytica, которая совместно с сотрудником Кембриджского университета распространяла в данной соцсети якобы исследовательское приложение, способное делать предсказания на основе анализа личностных черт пользователя [90]. Как выяснилось позднее, данные пользователей использовались с нарушениями, и оказались доступны не только разработчику, но и компании Cambridge Analytica, что противоречило запрету соцсети на передачу данных третьим лицам. Несмотря на немедленное удаление приложения и заявление всех вовлечённых в инцидент сторон об уничтожении полученных ими персональных данных пользователей было установлено, что далеко не все данные были удалены, а приложение получало ещё и доступ к информации друзей пользователя, установившего его. В результате случившегося компания Cambridge Analytica получила несанкционированный доступ к данным порядка 50 миллионов человек, а сервис Facebook, несмотря на прекращение сотрудничества с ней, пережил серьезный финансовый и репутационный ущерб.

Возможен также и риск несанкционированного сбора данных пользователей. Так, новозеландским разработчиком Диланом Маккеем было установлено, что социальная сеть Facebook собирает информацию, которую ей не следует знать, а именно: историю телефонных разговоров, а также метаданные об отправленных и полученных SMS [42]. В ответ на это компания Facebook заявила, что все контакты, звонки и SMS собирались исключительно с согласия пользователей, и при первом входе в аккаунт после установки приложения с целью поиска контактов пользователю предлагается загрузить на сервер содержимое его телефонной книжки, а также историю звонков и SMS-сообщений. Однако, на справочной странице

сервиса, посвященной тому, какую информацию он собирает о пользователях, метаданные звонков не упоминаются. Тем не менее пользователям компании доступна возможность выключения синхронизации контактов и удаления с серверов содержимого своей телефонной книжки.

Во время интервью одним из представителей Facebook было рассказано и о сканировании личных сообщений пользователей для проверки их на предмет оскорбительного контента [43], что так же могло стать для многих большой неожиданностью. При сканировании личных сообщений, по словам представителя, применяются те же инструменты, что и в публичных постах. Под анализ попадают как сами тексты сообщений, так передаваемые изображения и ссылки. Что касательно мотивов такой политики со стороны компании, то со слов её представителей таковыми выступают противодействие оскорбительному поведению, распространению незаконных материалов с несовершеннолетними, а также разжиганию ненависти и насилия. Аналогичные моменты прослеживается и во вступающем в силу с 1 мая 2018 года пользовательском соглашении компании Microsoft, владеющей в том числе таким крупным сервисом как Skype, где пунктом 3, включая личные сообщения, был закреплён запрет на использование оскорбительной лексики [100] под угрозой блокировки учётной записи. При расследовании же указанных нарушений компанией было оставлено за собой право пересматривать содержимое сообщений с целью разрешения возникшей ситуации. Стоит отметить, что вопрос этичности подобных мер и их границ остаётся дискуссионным. Так, модерация подобного содержания в личном пространстве может столкнуться со множеством проблем, как, например, смысловое содержание сообщений. В частности, контент, формально подпадающий под критерий разжигания насилия и ненависти, на деле может иметь обратный, саркастический смысл, либо быть простым цитированием, что понять без смыслового анализа всей ветви сообщений, особенностей взаимоотношения пользователей может быть крайне

затруднительно. Стоит также отметить, что если в случае публичного разбирательства дела о разжигании ненависти к расследованию могут быть привлечены соответствующие эксперты, то риск ошибки модерирующего личные сообщения машинного алгоритма может быть гораздо выше. Кроме того, все личные сообщения подпадают и под защиту права на их тайну, что должно препятствовать несанкционированной утечке их содержания, под критерий которой может подпадать в том числе и анализ сообщений сторонними службами и лицами.

Заметным фактором, несущим угрозу конфиденциальности пользователей, выступает и отсутствие необходимых обновлений программного обеспечения для персонального компьютера (ПК) или смартфона, исправляющего возможные ошибки и уязвимости. Так, достаточно распространённое мнение «если работает, то лучше не обновлять» может привести к использованию злоумышленниками неисправленной уязвимости того или иного программного обеспечения (ПО) для кражи персональных и платёжных данных пользователя. Аналогичный риск представляет и использование нелицензионных копий программ, сам факт взлома которых уже говорит о пробоине в защите и потенциальной опасности установки и использования. Однако, в ряде случаев недобросовестное отношение производителя электроники может представлять потенциальную опасность для пользователя. В частности, в апреле 2018 года исследовательской компанией Security Research Labs (SRL) был опубликован отчёт, проясняющий халатное отношение многих известных производителей смартфонов к обновлениям безопасности своих устройств [53]. В ходе анализа ПО 1200 устройств под управлением операционной системы Android было установлено отсутствие исправлений уязвимостей и ошибок, о которых заявлялось производителем. Проблема была зафиксирована на устройствах таких производителей как Samsung, Sony, Google, ZTE, TCL и многих других. По итогам исследования представителями компании Google было принято решение о совместном изучении сложившейся проблемы, а также, отмечено, что некоторые

устройства, участвовавшие в исследовании, предположительно, не были сертифицированы, что означает невозможность применения к ним стандартов безопасности Google.

Существенной проблемой также выступает и определённая беспечность многих пользователей при принятии решения о предоставлении своих данных тому или иному сервису. Так, на фоне популярности мобильного приложения GetContact, предоставляющего возможность узнать под каким именем сохранен ваш номер у людей из списка контактов, Роскомнадзором было высказано предостережение о потенциальной опасности подобных сервисов, собирающих информацию о контактах для своего функционирования [94]. Тем не менее, в России только за февраль 2018 года приложение было установлено около 200 тысяч раз. Существенным аспектом в данной ситуации является факт передачи пользователем не только своих персональных данных, но и данных всех людей из его контактной книги. При этом многие не задумываются о том, дали бы их знакомые на то личное согласие, и для каких целей может использоваться переданная сервису информация.

Одной из причин, побуждающих к обеспечению пользователями своего права на Интернет-анонимность, выступает безопасность их персональных, а также платёжных данных от посягательств правонарушителей. Посещая веб-страницы либо используя мобильные приложения без протокола шифрования трафика SSL (англ. Secure Sockets Layer), будучи при этом подключённым к общественной или малозащищённой беспроводной точке доступа к сети Интернет, пользователь существенно рискует. Имея необходимое программное обеспечение, а также оборудование, злоумышленник способен перехватывать незашифрованный трафик, используя незаконно-полученные данные в своих целях. Наиболее опасным подобное становится при использовании банковских Интернет-ресурсов, где помимо самих персональных данных, злоумышленнику становятся доступны и денежные средства жертвы. Согласно исследованию, проведённому Лабораторией

Касперского, по состоянию на конец 2016 года только в одной Москве 47% точек беспроводного доступа в сеть Интернет слабо защищены и могут представлять потенциальную опасность для пользователей. При этом, 16% из них не имеют никакого шифрования, а, следовательно, даже самой минимальный защиты. Вместе с этим, как отмечают в Лаборатории Касперского, в целом по Российской Федерации защищенных шифрованием беспроводных подключений почти на 8% выше, чем в среднем в мире, и составляет 72%. Лишь в относительно немногих странах Европы результаты выше. В частности, 83% сетей защищено шифрованием в Германии [95]. Тем не менее, по-прежнему значительное число беспроводных точек доступа в сеть Интернет остаются в зоне риска. Как сообщает Лаборатория Касперского, нередко злоумышленники создают псевдо-точки доступа в кафе и иных общественных места, заманивая посетителей в свои сети, либо же компрометируют уже имеющиеся [99]. Получив доступ ко всему трафику подключившихся жертв, злоумышленникам может стать доступна любая информация с незашифрованных соединений, в том числе и банковские данные. К счастью, в последнее время любой заботящийся о своей безопасности банк уже обзавёлся SSL-шифрованием (которое, как правило, проверяется в наличии зелёного «замочка» в адресной строке Интернет-браузера), однако, под угрозой могут оставаться клиенты мелких онлайн-банков, либо покупатели недобросовестных Интернет-магазинов, халатно относящихся к безопасности приёма платежей. Также помимо платёжных данных, аналогично могут быть скомпрометированы и аккаунты иных Интернет-ресурсов, не использующих SSL-шифрования при регистрации и авторизации, в том числе и сервисов электронной почты, социальных сетей. Завладев последним, правонарушитель может использовать полученные данные в любых противоправных целях, действуя фактически от лица жертвы. Говоря о мерах предотвращения подобных случаев, помимо желательного избегания небезопасных точек доступа в сеть, альтернативной может выступать использование VPN – виртуальной частной

сети, шифрующей входящий и исходящий трафик на устройстве и делающей его недоступным кибер-преступникам. Вместе с этим, пользователям необходимо с умом подходить и к выбору самого VPN, поскольку в данном случае весь незашифрованный Интернет-трафик будет проходить через VPN-провайдера и, соответственно, сможет им просматриваться. Также ему могут передаваться и другие данные пользователя, вроде характеристик его устройства, местонахождения, адресов посещаемых веб-сайтов. При этом в пользовательском соглашении, которое принимает клиент, могут быть оговорены такие моменты, как порядок хранения его трафика, ведение журнала соединений и т.д. При этом со стороны многих Интернет-ресурсов существенно сократить многие риски могло бы использование ими шифрования трафика, как минимум, в момент обработки персональных данных и, как максимум, полный переход на зашифрованное соединение. Актуальность данной проблемы подчёркивается, в частности, и недавним обнаружением крупной уязвимости со стороны оператора Wi-Fi в московском метро. Было установлено, что как минимум на протяжении года дыра в безопасности позволяла любому получить номера телефонов всех подключившихся пассажиров поезда, а затем и прочитать хранившийся в незашифрованном виде цифровой портрет каждого из них, включающий примерный возраст человека, пол, семейное положение и достаток, а также станции метро, на которых человек живет и работает [79].

Нельзя не затронуть и растущий интерес как со стороны общества, так и государства к теме криптовалют, многие из которых дают возможность совершать анонимные покупки в сети Интернет. Стоит отметить о двоякой сущности данного феномена, поскольку с одной стороны не все товары, полученные таким обменом, могут иметь незаконный характер, в отличии от, например, наркотиков или оружия. Также, как правило, невозможна и необоснованная блокировка криптовалютных счетов в связи с отсутствием регулирования как такового, что может создавать представление о надёжности среди некоторых участников данных проектов. Однако,

в то же время анонимность финансовых транзакций создаёт плодородную почву для отмывания преступных доходов и коррупционных схем, а вероятные сбои систем, нестабильность курса, либо неосторожность самих пользователей способны за мгновение лишить их всех хранящихся средств. В связи с ещё становлением данной сферы сложно предусмотреть какие-либо конкретные рекомендации по её правовому регулированию, однако можно обратить внимание на успешный международный опыт. Так, в Японии, в апреле 2017 года был принят закон о виртуальной валюте, позволивший использовать криптовалюты для взаиморасчётов на территории страны [107]. Вместе с этим японские власти сохранили позицию в отношении строгого регулирования данной сферы с целью предотвращения отмывания незаконных доходов [106]. К обменным пунктам, в свою очередь, были установлены строгие требования по уставному капиталу, защищённой компьютерной системе и аудиту.

Отдельное место, говоря об Интернет-анонимности, занимают слежки за пользователями со стороны государств, что подтверждает уже ранее упоминаемая история бывшего сотрудника ЦРУ и АНБ США Эдварда Сноудена, раскрывшего миру программу массовой международной слежки спецслужбами США за частной жизнью как граждан, так и за иностранными граждан в 60 странах мира. Стоит отметить, что данная тенденция становится всё более популярной и в других странах мира. При этом, зачастую преследуя вполне благие цели, в конечном итоге данные меры могут иметь сомнительную эффективность. Так, в июле 2015 года, практически за 5 месяцев до крупного парижского теракта, Конституционным советом Франции был одобрен новый закон о слежке, предоставляющий спецслужбам страны широкие полномочия для слежки за гражданами. Среди них, в частности, возможность запроса персональных данных граждан у Интернет-провайдеров и операторов сотовой связи, а также осуществление прослушки переговоров без решения суда подозреваемых в терроризме. Данный закон подвергся жесткой критике со стороны Комитета по правам человека ООН, который

в своём отчете отмечал, что закон дает слишком широкие полномочия спецслужбам для навязчивого контроля с плохо обозначенными целями [78].

Что касательно Российской Федерации, то заметную критику вызвал ещё на стадии законопроекта комплекс инициатив депутата Государственной Думы РФ И.А. Яровой и сенатора В.А. Озерова о борьбе с террористической угрозой. Одним из ключевых аспектов критики выступало и продолжает выступать повышение срока хранения информации о фактах приема, передачи сообщений, а также хранение самого Интернет-трафика, его содержимого и голосовой информации операторами связи. Принятие данного пакета законов вызвало заметное общественное обсуждение и обеспокоенность его возможными последствиями.

Таким образом, мы рассмотрели основы Интернет-анонимности, – стремления лица сохранить в тайне своё пребывание в сети Интернет. Являясь одним из элементов права на приватность в сети Интернет, Интернет-анонимность выступает так же составной частью конституционного права на неприкосновенность частной жизни, гарантируемого статьёй 23 Конституции Российской Федерации. Нами были выделены основные инструменты анонимности в сети Интернет. Кроме того, были определены наиболее встречающиеся проблемы реализации Интернет-анонимности. В следующей главе нами будет рассмотрено соотношение приватности в сети Интернет и законодательства Российской Федерации, основные проблемы последнего в указанной сфере, а также международный опыт по регулированию и обеспечению данного права.

# Глава 3. Проблемы правового регулирования Интернет-приватности в отечественном и зарубежном законодательстве

## 3.1. Проблемы Интернет приватности в российском законодательстве

Рассмотрев понятие приватности в сети Интернет, её элементы и общие проблемы их реализации, стоит проанализировать и действующую юридическую практику, имеющую выражение как в действующем законодательстве, так и непосредственно в судебной практике. Данный вопрос, ввиду его многогранности, следует рассматривать с нескольких сторон: как со стороны российского законодательства, так и со стороны международного опыта. На основании же приведённых данных должны быть сделаны соответствующие выводы.

Сфера Интернет-приватности в Российской Федерации ещё до недавнего времени не была столь ярко освещена вниманием. Достаточно долго данный вопрос казался малоинтересным как гражданам, так и законодателю. Однако, по мере развития Интернет-инфраструктуры и всё большему охвату ею повседневной жизни, вопросы и предложения по её регулированию стали выражаться всё чаще. На данный момент среди источников нормативного регулирования данной сферы можно выделить такие, как Конституция РФ, Уголовно-процессуальный кодекс, федеральные законы, в частности, № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», № 152-ФЗ от 27.07.2006 «О персональных данных», № 144-ФЗ от 12.08.1995 «Об оперативно-розыскной деятельности», № 126-ФЗ от 07.07.2003 «О связи», № 40-ФЗ от 03.04.1995 «О Федеральной службе безопасности», № 3-ФЗ от 07.02.2011 «О полиции», № 2202-1 от 17.01.1992 «О прокуратуре Российской Федерации». Данный перечень так же нельзя назвать исчерпывающим, поскольку он может бесконечно дополняться и подзаконными актами правительства и его ведомств, а также иными принятыми в

ближайшем будущем нормативными актами, в связи с нарастающим интересом законодателя к указанному вопросу.

Начало же регулированию приватности в сети Интернет было положено ещё введённой в 1996 году Системой оперативно-розыскных мероприятий (СОРМ-1). Однако, первая её версия была заточена исключительно на прослушивание телефонных переговоров. Уже начиная со второй версии, организованной в 2000 году, – СОРМ-2, целью контроля выступали непосредственно сеть Интернет и перехват электронных сообщений. Как отмечает О.Ю. Стороженко начиная с 2009 года постепенно создается и вводится в эксплуатацию ещё более комплексный проект анализа информации – СОРМ-3. При этом новое поколение СОРМ может включать в себя системы сплошного аудиомониторинга жилых помещений с использованием бытовых электронных приборов учета воды и уличных камер видеонаблюдения, а также специализированные базы паспортных, налоговых, банковских и голосовых данных. В конечном итоге, новое поколение СОРМ, по словам О.Ю. Стороженко, должно аккумулировать структурированную информацию о любом человеке (его номерах телефонов, звонках, контактах, перемещениях, темах разговоров дома, посещаемых сайтах и иных данных) [34, с. 69]. Однако, стоит отметить, что утверждение В.Ю. Теплышева [63] об аудиомониторинге жилых помещений с использованием приборов учета воды в рамках СОРМ 3, на которое ссылается О.Ю. Стороженко, не находят какого-либо авторитетного источника подтверждения, что можно интерпретировать как сомнительную информацию. Кроме того, подобная практика негласного сбора информации без санкции суда являлась бы грубым нарушением российского законодательства. Вместе с тем записи и метаданные телефонных переговоров, Интернет-трафика, системы уличных камер видеонаблюдения, паспортных, налоговых и банковских данных объективно уже на данный момент могут аккумулироваться в единую структуру в рамках СОРМ. Стоит также отметить, что условием получения лицензии на оказание услуг

связи выступает обязательство оператора предоставлять правоохранительным органам помещение и оборудование для проведения законного перехвата информации коммуникационных сетей. Так, согласно статьи 64 федерального закона «О связи» на операторов связи возлагаются обязанности, а на пользователей ограничения при проведении оперативно-розыскных мероприятий, а также мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий [8].

Касаясь нормативного регулирование СОРМ, в частности, можно выделить приказ Министерства информационных технологий и связи Российской Федерации от 16.01.2008 № 6 «Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий» [15]. Так, среди требований, предъявляемых к операторам связи, можно выделить, в частности, передачу на пункт ОРМ всей необходимой информации, выявленной в процессе контролируемого соединения, включая местонахождение абонента, а также декодирование данной информации при наличии шифрования. СОРМ предполагает и фактически полный доступ к базе данных абонентов, информации о конкретных пользователях и их номерах. Особый интерес вызывает пункт 9 требований, согласно которому в сетях связи обеспечивается исключение возможности обнаружения участниками контролируемого соединения или участниками передачи сообщений электросвязи факта проведения оперативно-розыскных мероприятий. Таким образом, даже сам оператор связи может не знать о проведении в отношении кого-либо из его абонентов оперативно-розыскных мероприятий. Вместе с этим, в приказе отмечается, что должна быть предусмотрена и защита от несанкционированного доступа персонала, обслуживающего сеть связи. С одной стороны, данные положения сочетаются с принципами конспирации и сочетания гласных и негласных методов и средств наблюдения, установленными федеральным законом «Об оперативно-розыскной деятельности». С другой стороны, в процессе проведения

данных оперативных мероприятий осуществляется пусть и легальное, но вторжение в инфраструктуру оператора связи, который, стоит отметить, в подавляющем числе случаев выступает третьей, незаинтересованной стороной. Следовательно, обоснованность подобного тайного легального вторжения может служить отдельным предметом для дискуссии. Подобная практика способна как существенно ускорить процесс расследования и его эффективность в одном случае, так и необоснованно внести закрытость в отношения, не нуждающиеся в этом.

Необходимые технические средства ОРМ, обеспечивающие доступ к столь массивному объёму данных, размещаются непосредственно на узлах связи сети связи оператора в соответствии с Планом мероприятий по внедрению технических средств для проведения оперативно-розыскных мероприятий.

В систему ОРМ входят следующие виды оперативно-розыскных мероприятий:

1. Наблюдение (п.6 ст.6 ФЗ «Об оперативно-розыскной деятельности»;
2. Контроль почтовых отправлений, телеграфных и иных сообщений (п.9 ст.6 ФЗ «Об оперативно-розыскной деятельности»);
3. Прослушивание телефонных разговоров (п.10 ст.6 ФЗ «Об оперативно-розыскной деятельности»);
4. Снятие информации с технических каналов связи (п.11 ст.6 ФЗ «Об оперативно-розыскной деятельности»);
5. Поиск на каналах электрической связи и в почтовых отправлениях (ч.3 п.4 ст.11 ФЗ «О противодействии терроризму»);

Кроме того, как отмечает С.И. Семилетов [32, с. 192], среди видов оперативно-розыскной деятельности с должной степенью уверенности можно выделить и «электронное наблюдение», которое, однако, законодателем на данный момент должным образом не закреплено и требует отдельного внимания. Так, касательно сущности «электронного наблюдения», с развитием Интернет-технологий оно может проявляться во множестве форм: анализ сетевого трафика, в том числе посещаемых

веб-сайтов, используемых сервисов и приложений на компьютере или смартфоне, определение местонахождения с достаточно высокой точностью. Могут извлекаться и данные о здоровье, вроде частоты сердцебиения, что способны считывать современные фитнес-устройства. Благодаря развитию так называемого «Интернета-вещей», – концепции единой сети физических предметов, взаимодействующих друг с другом или с окружающей средой, электронное наблюдение с той или иной стороны способно принять глобальные масштабы. Фактически любой умный чайник или термометр, имеющий выход в сеть Интернет, способен выполнять роль инструмента наблюдения, в том числе и в недобросовестных руках. Отсюда следует, что необходимо нормативное закрепление понятия электронного наблюдения, а также официальное включение его в список оперативно-розыскных мероприятий, пусть и под видом классифицирующего признака, включающего указанные выше моменты. Стоит отметить, что фактически данные меры могут уже осуществляться и применяться на практике, но, как видно на примере того же федерального закона «Об оперативно-розыскной деятельности», чёткое их определение отсутствует, как и должная регламентация процедур иных видов оперативно-розыскных мероприятий, без которых может развиться почва для злоупотреблений должностными полномочиями и иных правонарушений. С определёнными трудностями сталкиваются и операторы, среди которых, можно выделить, в частности, некорректную работу самого оборудования СОРМ, расплывчатость технического задания по его установке, а также непосредственную дороговизну реализации и эксплуатации. Затягивание внедрения оборудования СОРМ нередко может обходиться оператору существенно дешевле, поскольку штрафы в размере 30–40 тысяч рублей могут быть значительно меньше, чем проценты по кредитам за столь дорогостоящее оборудование и последующую его эксплуатацию [66].

Касаясь наиболее очевидных пробелов, связанных с реализацией СОРМ, в частности, можно выделить возникновение сложности с соотнесением его

применения с действующим уголовным законодательством. В Уголовно-процессуальном кодексе, а также федеральном законе «Об оперативно-розыскной деятельности» нет чёткой классификации тех преступлений, при расследовании которых может применяться электронное наблюдение, либо же конкретных случаев, где это может быть оправдано или необходимо. Расплывчатые либо фрагментированные формулировки могут выступать потенциальным инструментом злоупотреблений со стороны должностных лиц, и лиц, имеющих доступ к системе ОРМ. Кроме того, специфика того или иного состава может быть различной, что может предполагать наличие, либо отсутствие необходимости в осуществлении перехвата Интернет-трафика конкретного лица, либо группы лиц. Отсюда следует необходимость в составлении единого и понятного общественности классификатора преступлений, либо конкретных случаев, которые могут служить законным основанием проведения тех или иных оперативно-розыскных действий, включая электронную слежку.

Аналогичного подхода требует и установление рамок, по которым электронное наблюдение может осуществляться с обязательным уведомлением оператора связи. Сам вопрос целесообразности использования подобной закрытой процедуры заслуживает отдельного рассмотрения. Будучи не заинтересованным лицом, оператор связи не имеет каких-либо мотивов препятствования законному расследованию, подкреплённому справедливым решением суда. Отсюда следует, что подобное тайное вторжение зачастую может быть не обоснованным. При этом, в качестве исключения можно выделить, например, расследования, связанные с государственной тайной. Однако, и в данном случае сам факт доступа к инфраструктуре ОРМ оператора связи ещё не может говорить о раскрытии охраняемой законом тайны. В подобной ситуации возможно заключение договора о неразглашении, либо принятие решения компетентным судебным органом о возложении необходимых информационных ограничений. Таким образом,

предлагаемое законодательное регулирование должно исходить не из презумпции недоверия к оператору связи, а из полагания его заинтересованности в исключительно законном использовании его сервиса.

Отдельного внимания заслуживает и порядок хранения сведений личного характера, полученных в результате электронной слежки и не имеющих отношения к расследуемому делу. В частности, обоснованной мерой может служить их уничтожение, на что обращает внимание Е.Н. Поперина [31, с. 44]. Так, статью 6 федерального закона «О Федеральной службе безопасности», в которой законодателем отмечается, что «Полученные в процессе деятельности органов федеральной службы безопасности сведения о частной жизни, затрагивающие честь и достоинство гражданина или способные причинить вред его законным интересам, не могут сообщаться органами федеральной службы безопасности кому бы то ни было без добровольного согласия гражданина, за исключением случаев, предусмотренных федеральными законами» [11], можно дополнить положением об уничтожении указанных сведений по достижению поставленной цели.

Касаясь столь нашумевших летом 2016 года антитеррористических поправок, можно выделить несколько моментов. В частности, отдельные положения федерального закона № 374-ФЗ [10], касающиеся Интернет-сферы, вызвали особо жаркое общественное обсуждение. Так, статьями 13 и 15 на операторов связи была возложена обязанность хранить в течении трёх лет на территории Российской Федерации информацию о фактах приёма, передачи, доставки или обработки, а также непосредственно сами текстовые и иные сообщения, голосовую информацию, изображения, звуки, видео до шести месяцев. Аналогичные обязательства были возложены и на организаторов распространения информации в сети Интернет. Обязанность хранения информации о фактах приема, передачи, доставки или обработки для организаторов распространения информации была установлена сроком на один год, а сами текстовые и иные сообщения сообщения пользователей,

их голосовую информацию, изображения, звуки, видео сроком до шести месяцев с момента окончания их приема, передачи, доставки или обработки. При этом, установка порядка, сроков и объема хранения данной информации в обоих случаях были возложены на Правительство Российской Федерации.

Стоит отметить, что если термин «оператор связи» не вызывает особого недопонимания, то «организатор распространения информации» заслуживает более детального рассмотрения. Согласно статье 10.1 федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» организатором распространения информации в сети Интернет выступает лицо, осуществляющее деятельность по обеспечению функционирования информационных систем или программного обеспечения, которые предназначены для приема, передачи, доставки или обработки электронных сообщений [6]. Таким образом, организатором распространения информации фактически выступают любые сервисы, предоставляющие возможность обмена электронными сообщениями: мессенджеры, социальные сети, форумы и прочие.

Говоря же о самом факте хранения пользовательских сообщений и трафика, то стоит на этом остановиться подробнее. Реализация указанной нормы сталкивается с рядом различных вопросов и трудностей. В частности, это непосредственная безопасность хранения. Пользовательский Интернет-трафик может содержать достаточно личную информацию, охраняемую неприкосновенностью частной жизни, а также платёжные и иные ценные данные. Утечка подобной информации способна нанести существенный ущерб как материального, так и репутационного характера. Отсюда следует, что владение подобной информацией может стать целью номер один для различного рода правонарушителей, видящих в ней удобный инструмент для вымогательства, шантажа и прочих запрещённых законом деяний. Как было установлено специалистами по Интернет-безопасности компании InfoWatch, лишь только за первую половину 2017 года вследствие 925 крупных

инцидентов была зафиксирована утечка 7,78 млрд записей с персональными и платежными данными по всему миру, что составило восьмикратный рост по сравнению с прошлым годом [87]. В свою очередь при 520 официально зафиксированных инцидентах виновниками выступили сами компании и государственные структуры, ответственные за безопасное хранение пользовательских данных, что составило абсолютное большинство. В 384 случаях фактором утечки выступило внешнее вмешательство. Не менее интересным выступает и факт того, что причину 21 крупного инцидента в конечном итоге установить не удалось. Стоит отметить, что по мнению специалистов InfoWatch, реальный охват данного отчёта может составлять не более 1% от всех случаев утечек данных, поскольку он основан на анализе публичной информации, а компаниями, в свою очередь, по понятным причинам, подобные инциденты раскрываются крайне неохотно.

Заслуживает внимания и стремительный рост утечек конфиденциальных данных непосредственно на территории РФ. Так, в 2016 году Россия заняла второе место по числу утечек конфиденциальной информации, уступив место лишь США [98]. Кроме того, за данный период на территории страны был зафиксирован 80% рост утечек по сравнению с предыдущим, что вовсе сделало её лидером по ежегодному приросту. Одной из возможных причин столь резкого роста, как отмечают специалисты, может выступать развитие сервисов, обрабатывающих персональные данные, и, соответственно, увеличение объёмов, обрабатываемых данных. Как и на общемировом уровне абсолютное большинство случаев утечек (61,8%) происходило по вине внутреннего нарушителя, – бывших и настоящих сотрудников компаний, а также их подрядчиков. Однако, в результате действий извне (например, хакерских атак) было спровоцировано 34 из 44 наиболее крупных утечек пользовательских данных. Как отмечают эксперты по кибербезопасности, количество утечек в России и Европе в реальности может быть существенно выше,

поскольку значительная часть информации может просто не доходить до аналитиков. При этом, специалистами подчёркивается важность отчётности, позволяющей составить более реальную картину текущего положения, анализ которой мог бы способствовать выработки более эффективной политики по дальнейшему предотвращению указанных инцидентов. Так, если в законодательстве США имеются положения, обязывающие компании и организации отчитываться о фактах утечки информации, то в России, а также многих странах Европы подобные нормы в законодательстве отсутствуют, что затрудняет анализ.

На основании приведённой информации следует, что хранение личных пользовательских данных, особенно в столь крупных масштабах, сопряжено со значительной долей рисков. Как показывает статистика, наибольшее число нарушений безопасности пользовательских данных происходит именно по вине субъектов, ответственных за их сохранность, т.е. внутреннего фактора. При этом наибольшая масштабность ущерба связана непосредственно со внешними факторами, вроде хакерских атак, поскольку, как правило, причиной внутренних утечек выступает желание бывших либо действующих сотрудников отомстить работодателю или использовать ценную информацию в личных интересах. В подобных случаях утечки не являются столь массовыми, и сводятся к краже небольшого объёма данных, однако это не умаляет серьёзности вероятного ущерба для конкретного пострадавшего лица. Особенно серьёзный ущерб могут нанести утечки из баз данных государственных структур. Так, в сентябре 2016 года в СМИ сообщалось об утечке со стороны ныне расформированной Федеральной службы по контролю за оборотом наркотиков (ФСКН) всероссийской базы данных ВИЧ-инфицированных, пациентов психоневрологических диспансеров, алко- и наркозависимых, а также склонных к суициду граждан. «Рекламные» объявления о продаже секретных баз данных, по словам журналиста Сергея Канева, появились на Интернет-форумах силовиков ещё в середине августа того же года [60]. Стоит

отметить, что сообщения о подобных случаях неоднократно всплывают на протяжении многих лет. Так, в 2017 году ЕСПЧ коммуницировал жалобу 46-летнего москвича, обнаружившего в 2011 году в открытом доступе на Савеловском рынке базу ГУВД Москвы, в которой содержались данные, что заявитель – носитель ВИЧ-инфекции и дважды судим. При этом во второй половине 2011 года правоохранительными органами были проведены рейды по рынкам и были изъяты более 2500 дисков с базами данных. В процессе изучения судом дела уполномоченный России в ЕСПЧ, замминистра юстиции Михаил Гальперин отметил, что МВД обеспечивает защиту информации от несанкционированного доступа, а приобретенная заявителем на рынке база не является подлинной, поскольку в базах МВД отсутствуют сведения о состоянии здоровья лиц, состоящих на оперативном учете. Замминистра юстиции также заявил, что не располагает информацией о фактах несанкционированного доступа к базам данных МВД. В свою очередь документы и учетные карточки Управления собственной безопасности (УСБ), касающиеся проведённых в 2011 году рейдов, были уничтожены ещё в 2016 году в связи с истечением их срока хранения [75]. Несмотря на отрицание властями утечки персональных данных со стороны МВД, трудно не согласиться, что источником утечки указанных данных о здоровье граждан могли быть иные государственные структуры, либо медицинские учреждения. Не менее интересно и недавнее уголовное дело, возбуждённое в отношении бывшего следователя одного из столичных райотделов полиции, обвиняемого в незаконном получении у операторов сотовой связи детализаций телефонных соединений абонентов по поддельным судебным решениям. За нужную им информацию клиенты, по данным следствия, платили ему и посредникам от 45 до 100 тысяч рублей. В материалах расследования отмечается, что обвиняемый за два года успел оформить порядка 300 поддельных судебных решений о предоставлении данных детализации телефонных переговоров, а также информации о самих абонентах у основных операторов

сотовой связи [64]. Таким образом, учитывая рост сервисов и служб, а также государственных и медицинских структур обрабатывающих персональные данные, ожидаем и закономерный рост возможных нарушений и злоупотреблений как внутри компаний, госструктур, учреждений и их подрядчиков, так и в результате внешних факторов, как хакерские атаки. Вследствие того, что данные Интернет-трафика и содержание сообщений могут представлять из себя существенный пласт ценной информации по конкретной личности, ожидаем ещё больший интерес к их заполучению и перехвату со стороны правонарушителей. Следовательно, переход к сбору и хранению подобной информации без определения должных правил и требований к их безопасности, может быть связан с существенными рисками её компрометации.

В свою очередь, для предотвращения возможных утечек информации и минимизации ущерба произошедших необходимо законодательное закрепление обязанности операторов связи, организаторов распространения информации, а также государственных структур и учреждений в уведомлении пострадавшей в результате утечки стороны в максимально короткие сроки после факта обнаружения таковой. Способ уведомления, при этом, может быть различным: как через официальное электронное уведомление, так и через публичное обнародование. Наиболее же эффективным из них может быть комбинированный, включающий в себя как персональное уведомление каждой из пострадавших сторон, так и публичное заявление о случившимся на случай, если по какой-либо причине личное уведомление может не дойти до адресата. Важным условием в данном случае выступает непосредственная вина оператора связи, организатора распространения информации и иных отвечающих за хранение и обработку персональных данных структур в данной утечке, поскольку, определённо, они не могут быть ответственны за компрометацию данных пользователем по его собственной вине. В целом подобная практика должна дисциплинировать указанных субъектов в плане

отношения к безопасности данных своих пользователей, стимулируя бережное и ответственное к ним отношение. В свою очередь, возможные репутационные риски на случай компрометации должны быть определённым сдерживающим фактором, не дающим забывать об этом.

Таким образом, статьи 10.1 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также 46 федерального закона N 126-ФЗ «О связи» следует дополнить нормой:

«…в случае обнаружения утечки, а равно иной виновной компрометации личной информации, сообщений и их содержания, обязан незамедлительно (либо в кратчайшие сроки) уведомить пострадавшую сторону».

Соответствующие положения, касающиеся обязанности уведомления пострадавшей стороны в случае утечки какой-либо его персональной информации, следует внести и в Федеральный закон № 152-ФЗ «О персональных данных».

Кроме того, эффективной мерой могло бы выступить введение административной ответственности для должностных и юридических лиц на случай утаивания информации о совершённой утечке пользовательских данных. Так, возможно дополнение главы 13 КоАП РФ, касающейся непосредственно связи и информации, составом: «Сокрытие факта утечки (компрометации) личной информации». Сама же норма может представлять из себя следующее:

«Сокрытие должностным (юридическим) лицом факта виновной утечки (компрометации) личной информации, переписок, аудио-, видео- и иных сообщений…влечёт наложение административного штрафа в размере…»

Необходимость административной ответственности за сокрытие факта компрометации личной информации обуславливается во многом тем, что незнание пользователями о случившемся инциденте и непринятие ими каких-либо срочных действий по минимизации рисков (например, смена пароля учётной записи, блокировка скомпрометированных кредитных карт и т.д.) может увеличить

дальнейший конечный ущерб. Возлагает данная мера и большую ответственность на плечи должностных лиц, в ведении которых находится обеспечение безопасности пользовательских данных.

Не менее важной выступает защита прав пользователей, пострадавших вследствие подобных утечек. Основным направлением государственного регулирования в данной сфере должна выступать выработка у компаний ответственности и должной дисциплины в области хранения пользовательских данных. Так, обеспечение должной защиты своей инфраструктуры должно быть экономически выгоднее, чем халатное к ней отношение. Конечно, в случае утечки конфиденциальной информации пользователей компании несут репутационные риски, однако это едва ли может компенсировать уже причинённый ущерб. В некоторых случаях, нанесённый ущерб может быть и вовсе непоправим. Так, в августе 2015 года сообщалось о самоубийствах пользователей взломанного Интернет-сайта, специализирующегося на тайных знакомствах людей, находящихся в браке [65]. Аналогичные последствия могут вызвать и утечки личных сообщений из мессенджеров, социальных сетей и прочих сервисов, предоставляющих услуги Интернет-коммуникации. Согласно исследованию российской национальной системы мониторинга Роскачество существенная часть сервисов онлайн-знакомств, действующих в РФ, не соответствует минимальным требованиям безопасности [84]. В ряде из них отсутствует шифрование текстовой информации, в других же не шифруются передаваемые изображения. Кроме того, было установлено, что некоторые приложения вовсе передают персональные данные в незашифрованном виде. В случае перехвата трафика злоумышленниками могут быть скомпрометированы все личные данные клиентов, что не может не вызывать обеспокоенность. Таким образом, мы видим, что проблема халатного отношения к персональным данным клиентов стоит особенно остро. Для минимизации же потенциально-возможного ущерба необходима законодательная выработка системы

компенсаций пострадавшей в случае утечки стороне. При этом, стоит учитывать, что для обхода или минимизации потерь многие компании, особенно крупные, могут изначально предусматривать часть средств на данные компенсации, продолжая игнорировать требования безопасности. Следовательно, наиболее разумным будет расчёт размера компенсаций исходя из годовой выручки компании. Сам же компенсационный процент выручки, требует более подробного согласования. Однако, с одной стороны, он должен быть достаточно существенным, чтобы необходимые меры безопасности были выгоднее компаниям, чем разовый «откуп» в случае каждого происшествия, с другой же, – целью как таковой выступает не разорение провинившейся стороны, а стимулирование её ответственного обращения с пользовательскими данными. Отдельного внимания заслуживают монополисты и недобросовестные компании, способные в случае возложения на них ответственности, компенсировать расходы за счёт своих же пользователей, – той самой пострадавшей стороны, путём поднятия тарифов и т.д. Подобные способы обхода ответственности должны должным образом пресекаться со стороны Федеральной антимонопольной службы и других уполномоченных органов.

Не менее важным вопросом выступает и финансовая основа реализации норм, касающихся хранения пользовательского Интернет-трафика и содержания сообщений. Так, по оценке ФСБ и Минкомсвязи затраты, возложенные на операторов связи, могут составить до 4,5 трлн рублей, что практически в три раза больше оборота всей отрасли за 2016 год [105]. Оценили свои предварительные расходы и сами операторы связи. Так, по расчетам оператора «Мегафон», вероятные затраты по закупке и модернизации необходимого оборудования составят приблизительно от 672 млрд до 1 трлн рублей. В компании «ВымпелКом» (бренд «Билайн») предварительная оценка представила расходы так же в районе 1 трлн рублей. Стоит учитывать, что поскольку данные цифры не включают траты на последующую эксплуатацию и модернизацию оборудования, то реальные конечные

цифры могут оказаться значительно выше. Указанные суммы, даже после их определённой коррекции, являются чрезвычайно затратными. Для понимания этого, выручка компании Мегафон за 2016 год всего составила около 316 млрд рублей. Стоит осознавать, что столь существенные затраты могут на годы замедлить развитие сетевой инфраструктуры в стране, поскольку, помимо непосредственного обеспечения связью, существенные затраты операторов уходят и на поддержание в рабочем состоянии и развитие собственных сетей. Последнее, в данной ситуации, может оказаться слишком затратным, и значительно сбавить обороты. В конечном итоге компенсация возложенных затрат может быть возложена и на абонентов в форме существенного подорожания услуг связи.

Отдельной проблемой реализации нормы по хранению сетевого трафика пользователей сети Интернет выступает и сам его объём. Так, на ранних этапах разработки и принятия данной нормы предполагалась хранение операторами связи по 1 петабайту на каждый 1 Гбит/сек, что в конечном итоге за один 2018 год способно достигнуть 30 эксабайт, и 60 с 2019 года [89]. Стоит понимать, что среди столь фантастического объёма данных фактически полезными, например, для расследования какого-либо правонарушения, могут быть лишь единичные фрагменты. Последнее обуславливается в том числе и ростом числа Интернет-сайтов, использующих SSL-шифрование. Так, по состоянию на январь 2018 года более 70% загружаемых веб-страниц в браузере Mozilla Firefox используют SSL [47]. При посещении пользователем Интернет-сайта, использующего шифрование, оператору связи не известны его действия на данном Интернет-ресурсе, хотя и факт его посещения, а также время могут фиксироваться. Аналогичный результат может быть при использовании средств анонимизации, как VPN или Tor. Однако, в данном случае от глаз оператора связи могут быть скрыты и фактически посещаемые Интернет-ресурсы. Отдельное место может занимать различный «файловый мусор», к которому можно отнести воспроизводимые потоковые видео- и аудиозаписи, IP-

телевидение, торренты, и прочие тяжелые и бесполезные для хранения и обработки материалы, которые, тем не менее, могут быть едва ли не основной частью Интернет-трафика и занимать наибольший объём данных. Стоит отметить, что последнее было всё же принято Минкомсвязи во внимание, которое допустило сокращение требуемых объёмов хранения, с учётом исключения избыточной информации, до 10 раз [82]. Также постановлением правительства от 12.04.2018 № 445 был установлен ближайший порядок реализации хранения трафика пользователей. Так, операторы связи должны будут обеспечивать хранение голосовой информации и текстовых сообщений пользователей в полном объёме в течении 6 месяцев с даты окончания их приёма, передачи, доставки и обработки. А с 1 октября 2018 года на операторов связи было возложено и обязательство по хранению в полном объёме трафика, отправленного и полученного пользователями за 30 суток, предшествующих дате ввода технических средств накопления информации в эксплуатацию. При этом ёмкость последних должна будет увеличиваться ежегодно на 15% в течении 5 лет с даты ввода их в эксплуатацию. На оператора связи было возложено и обеспечение защиты технических средств накопления информации от несанкционированного доступа в соответствии с требованиями Министерства связи и массовых коммуникаций РФ. Не обошёл законодатель и вопрос порядка удаления хранящейся информации. Удаление из технических средств накопления информации их содержимого должно будет осуществляться в автоматическом режиме по окончании 6 месяцев с даты их приёма, передачи, доставки и обработки [14]. Тем не менее, указанное не исключает необходимости выработки со стороны ответственных за хранение указанных данных должных алгоритмов фильтрации, сжатия, и шифрования, отвечающих принципам безопасности, соблюдения прав человека и гражданина, и в целом соответствующих требованиям законодательства.

Заслуживает внимания так же и знание пользователей того, какую информацию о них собирают, и что конкретно в данном случае хранят на установленный законом срок. Особенно это касается операторов связи, способных фиксировать буквально каждое перемещение своего абонента. Незнание пользователем данной информации, и невозможность с ней ознакомиться не делает вышеуказанную норму о хранении Интернет-трафика прозрачной для общества, и может создавать почву для возможных злоупотреблений. Если каждый ответственен за свои действия в сети Интернет, то, соответственно, за ним должно быть закреплено и право ознакомления с тем, за что он ответственен. Следовательно, должной мерой может выступать создание инструмента, дающего пользователю возможность ознакомиться с его сетевым трафиком. Одним из ключевых факторов в данном случае, несомненно, должна выступать безопасность, поэтому доступ к данной информации должен обеспечиваться особо надёжными способами верификации и авторизации, например, через Интернет-портал Госуслуг. Однако, имеется у данной услуги и обратная сторона, касающаяся обеспечения неприкосновенности частной жизни в случае проживания на одной территории нескольких человек или использования единой точки выхода в сеть Интернет. Сокрыть в данном случае свою Интернет-активность от посторонних возможно лишь используя средства анонимизации, шифрующие сетевой трафик с конкретного устройства. Также возможна и разработка такого стандарта выхода в сеть Интернет, когда одна общая точка доступа может делиться на несколько «колен» в зависимости от привязки к устройству, информация о трафике которого не доступна без надлежащего разрешения субъекта. Возможна реализация подобного и через процедуру письменного согласия всех лиц, использующих данную точку доступа. Тем не менее, данная проблема осложняется ещё множеством факторов, помимо технических. В частности, ключевым остаётся вопрос, как стоит поступать с Интернет-трафиком несовершеннолетних, не нарушая их право на частную жизнь,

либо в случае использования общественных Wi-Fi сетей. Стоит признать, что однозначного решения указанных проблем на данный момент нет, а цена ошибки будет слишком высока. Какое-либо поспешное принятие мер может привести к непредсказуемым последствиям, включая даже рост правонарушений или злоупотреблений.

Таким образом, стоит понимать, что массовый тайный сбор какой-либо информации о гражданах без их явного на то согласия сложно назвать этичной мерой. Решение же указанной проблемы, в независимости от его философского подхода, может привести к непредсказуемым последствиям из-за технической или социальной составляющей. На основании этого возникает закономерный вопрос о целесообразности осуществления подобной политики сбора и хранения информации в целом, по крайней мере на этапе, когда ещё отсутствуют какие-либо технические и правовые инструменты прозрачности и предотвращения возможных злоупотреблений и утечек. Наиболее оптимальным вариантом в сложившейся ситуации мог бы стать полный пересмотр норм статьи 64 федерального закона № 126-ФЗ «О связи» [8], касающихся сбора и хранения пользовательского трафика и сообщений, либо перенос их вступления в силу до момента проработки наиболее прозрачного и безопасного варианта реализации, не вступающего в конфликт с конвенционным и конституционным правом на приватность.

Интересным так же выступает содержание постановления Правительства Российской Федерации № 21 от 18.01.2018, регулирующее порядок сотрудничества участников реестра организаторов распространения информации с уполномоченными органами. В пункте 6 отмечается, что организатор распространения информации при взаимодействии с уполномоченными органами обеспечивает в соответствии с законодательством Российской Федерации неразглашение любой информации о конкретных фактах и содержании такого взаимодействия третьим лицам [13]. Данное положение является достаточно

расплывчатым, поскольку, в частности, возникает вопрос о запрете разглашения сотрудничества как такового, или же о неразглашении конкретных эпизодов. В указанном случае возникает вопрос о соответствии данной меры деянию, в совершении которого подозревается лицо. С одной стороны, порой указанная мера может быть логически обоснована, поскольку в ряде ситуаций раскрытие указанной информации может побудить подозреваемое лицо к попытке уничтожения улик либо иным способом скрыться от правосудия. Тем не менее, с другой стороны, особенностью многих сервисов онлайн-коммуникации, а также сети Интернет в целом, выступает крайняя сложность сокрытия каких-либо данных. Так, метаданные всех действий со стороны пользователя в большинстве случаев могут быть доступны оператору распространения информации, среди которых можно выделить в том числе и факты изменения, либо удаления информации, а также резервные копии её предыдущих версий. История изменения содержания той или иной Интернет-страницы может содержаться и в кэше поисковиков, как Яндекс или Google. Следовательно, во многих случаях такие меры явно чрезмерны, за исключением, когда правонарушитель заинтересован скрыться от следствия, либо раскрытие подобной информации представляет существенную угрозу расследованию на данный момент. Полное же сокрытие даже самого статистического факта сотрудничества в публичной отчётности не содействует прозрачности работы с пользовательскими данными и вере общества в справедливость и законность расследования правонарушений. Последствием этого могут быть различные практики обхода подобных непрозрачных норм со стороны компаний, обеспокоенных своей репутацией. Так, в ряде западных стран, как США, на практике сложилось такое явление, как «свидетельство канарейки», представляющее из себя способ передачи информации о слежке через молчание или отрицание её факта. Для лучшего понимания данного термина стоит кратко обратиться к его этимологии. Исторически канарейки, благодаря их чувственной остроте,

использовались в угольных шахтах в качестве рецептора концентрации угарного газа. Замолкая, птица давала понять шахтёрам о надвигающейся опасности [55]. Аналогично сложилась практика, когда компания, несмотря на запрет разглашения факта ордера на слежку, вправе обойти этот запрет, не нарушая закон, уведомив пользователя о том, что за ним в определённый момент времени не велось скрытого наблюдения.

Отдельного внимания заслуживает и следующее положение, касающееся шифрования пользовательских данных. Так, статьёй 10.1 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» на организатора распространения информации возложена обязанность предоставлять в уполномоченный государственный орган информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых или обрабатываемых электронных сообщений [6]. Важно понимать, что любой уважающий безопасность своих пользователей сервис осуществляет передачу и приём входящих и исходящих сообщений используя те или иные протоколы шифрования. Последние, в свою очередь, могут быть как собственной разработкой компании, так и быть использованными на основании текущей лицензии. В некоторых случаях шифрование сообщений может осуществляться индивидуальными ключами на устройствах пользователей, что делает информацию недоступной для организатора распространения информации. Извлечение данных в таких случаях возможно исключительно с самого устройства, если самим владельцем не использованы дополнительные меры шифрования. При этом важно понимать, что какое-либо разглашение ключей шифрования третьим лицам, в том числе и правоохранителям, со стороны организаторов распространения информации может расцениваться как мера потенциально-небезопасная. И у данных опасений присутствует вполне обоснованная почва, если обратиться даже к статистике по утечкам, упомянутой выше. Кроме того, раскрытие декодирующей информации третьим лицам может

потенциально поставить под удар всех пользователей, поскольку фактически в распоряжение правоохранителей или спецслужб передаётся «ключ от всех дверей». Несмотря на обязательство исключительно законного использования указанной информации, никто не может дать стопроцентной гарантии, что однозначно исключён прецедент злоупотребления положением со стороны данной категории лиц. Трудно не заметить и этическую проблему, заключающуюся в возможном предоставлении ключей шифрования от личных сообщений всех пользователей при решении суда лишь в отношении конкретных граждан. Данный сценарий фактически предполагает угрозу приватности неограниченного числа лиц, не имеющих какого-либо отношения к расследуемому делу. Соответственно, подобная ситуация предполагает и отсутствие судебного решения в отношении каждого лица из неопределённого круга пользователей. В случае же самостоятельной расшифровки и передачи личных сообщений организатором распространения информации, пусть и на основании решения суда, возникает иная этическая проблема, касающаяся его полномочий на осуществление данных действий, особенно, если в пользовательском соглашении за ним не были закреплены правомочия доступа к личным сообщениям пользователей. Так, при наличии законного решения суда формально может нарушаться соглашение со всеми остальными пользователями, для которых обязательство сервиса о полной неприкосновенности личных сообщений могло быть ключевым при заключении данного соглашения. Вместе с этим, если сервис оставил за собой подобное право, и пользователи выразили на то безоговорочное согласие, вышеуказанная этическая проблема может отпасть. Таким образом, положение статьи 10.1 федерального закона № 149-ФЗ о передаче ключей шифрования заслуживает значительного пересмотра, либо полной отмены в связи с выявленными рисками и этическими проблемами, а также технической невозможностью реализации в определённых случаях. Так, передача ключей шифрования третьим лицам может быть

потенциально небезопасна для всех пользователей сервиса, либо организатор распространения информации и может вовсе не иметь доступа к сообщениям на устройстве из-за использования им сквозного шифрования, при котором ключи дешифровки хранятся исключительно на устройствах пользователей. Вместе с этим данное решение не предполагает создания помех правоохранительным органам, поскольку содействие следствию организаторами распространения информации может заключаться и в виде санкционированной судом передачи общих метаданных об адресатах, времени отправки сообщений, продолжительности аудио- или видеозвонков, которые так же могут оказать существенную помощь расследованию. В случае же установления факта невозможности получения каких-либо данных вовсе, работу по их извлечению из устройства остаётся возлагать на компетентные правоохранительные службы, обладающие надлежащими знаниями и оборудованием.

Касаясь политики блокировок и запрета сервисов, придерживающихся осторожности в плане сотрудничества с властями того или иного государства, более эффективной мерой мог бы стать поиск компромиссов в случае, если площадка не осуществляет поддержку противоправной деятельности и готова идти на сотрудничество, не затрагивающее безопасность, права и свободы её добросовестных пользователей. Таковыми, как упоминалось ранее, могли бы стать выявление и блокировка публичных страниц, групп и каналов, пропагандирующих и обеспечивающих террористическую и иную противоправную деятельность. Блокировки же в большей мере создают проблемы именно добросовестным пользователям, привыкшим к удобной им площадке, и вынужденным искать либо доступные альтернативы, либо средства обхода возложенных ограничений. В последнем случае возрастает и угроза безопасности пользовательских данных, поскольку сложившаяся ситуация может использоваться злоумышленниками для распространения вредоносного ПО среди невнимательных или неподкованных в

информационной безопасности граждан под видом средств обхода блокировок и альтернативных клиентов сервиса. Риск такой технической возможности был подтверждён специалистами и в ходе одного из опубликованных в сети Интернет экспериментов, показавшего достаточную лёгкость создания и распространения подобного псевдо-клиента [104]. Кроме того, как было установлено, преступниками могут использоваться сервисы и инструменты, вовсе не использующие какие-либо средства шифрования, что, в частности, и подтвердилось во время террористических атак в Париже.

Таким образом, рациональными могли бы стать пересмотр законодателем действующего законодательства в отношении блокирования Интернет-ресурсов, и изъятие из числа запрещённых веб-сайтов Интернет-площадок, готовых к сотрудничеству с правоохранительными органами в отношении публичного недопустимого контента. Если же имеются основания полагать о присутствии угрозы пользовательским данным при использовании того или иного сервиса, обоснованным могло бы стать внесение его в список «сомнительных», ведение которого можно поручить Роскомнадзору. Данный статус мог бы налагать на сервис определённые ограничения, вроде невозможности его государственной финансовой поддержки, отсутствия налоговых послаблений в случае осуществления коммерческой деятельности на территории РФ. При этом ресурсам, полностью соответствующим нормам Интернет-безопасности, могли бы выдаваться соответствующий цифровой сертификат, и полагаться некоторые стимулирующие преимущества, недоступные «сомнительным» сервисам, как, например, финансовая господдержка, если сервис является отечественным. Вместе с этим, допустимо было бы сохранение доступа к данным ресурсам при условии отсутствия поддержки с их стороны противоправной деятельности и сотрудничества в плане модерации публичного неприемлемого контента. При этом статус «сомнительного ресурса» стимулировал бы владельцев данных сайтов лучше соблюдать государственные

стандарты о персональных данных с целью исключения из данного списка, а у пользователей, в свою очередь, сохранился бы выбор: продолжать пользоваться удобным для них сервисом, осознавая личную ответственность за своё решение, либо выбрать Интернет-ресурс в полной мере соблюдающий действующее законодательство, к которому нет каких-либо вопросов со стороны государства. Интересным является и факт того, что блокировка сервисов в некоторых случаях способна даже увеличить их популярность, пусть и лишь на первое время после блокировки. Так, специалистами сервисов аналитики Telegram-каналов Combot, TGStat и Telemetr было отмечено, что активность в мессенджере после блокировки в России заметно увеличилась [101]. В частности, дневной охват просмотров вырос со 175 до 211 млн, что составило 20%, а прирост подписчиков на каналы вырос на 39%, составив 336 против 240 тысяч до блокировки. Впрочем, закономерно ожидать и определённое падение охвата в будущем за счёт тех пользователей, для которых сервис не представлял особой важности. Однако, среди действительно преданной аудитории вряд ли стоит ожидать существенного падения интереса к любимому сервису. Возвращаясь к предложенному подходу, можно отметить, что, с одной стороны, он позволяет исключить чрезмерные сетевые ограничения, нарушающие права добросовестных граждан, с другой же – сохраняет запрет Интернет-ресурсов, действительно, преследующих противоправные цели и представляющих реальную общественную опасность.

Стоит также вернуться к особенностям функционирования такого инструмента анонимизации как VPN, и прояснить некоторые детали. С 1 ноября 2017 года вступил в силу закон, обязывающий владельцев VPN и анонимайзеров ограничивать доступ к сайтам и сервисам с запрещённой информацией [67]. Основной же проблемой в большей мере выступает факт того, что как правило расположенные в той или иной стране серверы VPN-провайдера действуют согласно законодательству страны местонахождения. Так, подключаясь к серверу, расположенному в США или

Нидерландах, пользователь, соответственно, соглашается перед VPN-провайдером соблюдать американское или нидерландское законодательство, виртуально перемещаясь на территорию другого государства. Следовательно, более логичным было бы соблюдение российского законодательства со стороны серверов VPN-провайдеров, находящихся на территории Российской Федерации, поскольку, их физическое нахождение в её юрисдикции накладывает и обязательство по соблюдению российского законодательства. Блокировка же запрещённых в РФ сайтов серверами, находящихся на территории зарубежных государств, может быть как сложнореализуемой технически, так и ущемлять право на доступ к информации всех пользователей данного VPN-провайдера, независимо от их гражданства и фактического местонахождения, поскольку Интернет-сайт, запрещённый в одном государстве, может быть доступен и разрешён в другом. При этом с высокой вероятностью ограничения могут быть реализованы лишь введением их для всех без исключения, поскольку точечно определить гражданство каждого подключающегося к серверу пользователя практически невозможно, как крайне сложно и в общем соотнести IP-адрес и конкретную личность. О последних, при этом, известно может быть лишь оператору связи, и то не во всех случаях. Кроме того, требуя подобных ограничений для иностранных серверов, возможно создать прецедент в виде ответной реакции и со стороны иностранных государств на блокировку запрещённых на их территории сервисов и сайтов к российским властям и Интернет-провайдерам, что может толковаться как вмешательство во внутренние дела и нарушение государственного суверенитета. Фактически VPN-сервисы можно по аналогии отнести к международному транспортному сообщению через относительно открытые виртуальные границы. Данным инструментом даётся возможность перемещения в виртуальное пространство другого государства, где аналогом визы или иного подтверждающего документа выступает присвоенный IP-адрес того или иного государства. Хотя и VPN сам по себе не является исключительно средством

обхода запрещённых Интернет-сайтов, а выступает средством анонимизации и сетевой безопасности, однако, по своему существу он предполагает и подобные возможности. Стоит отметить, что в практически любом пользовательском соглашении того или иного VPN-провайдера предусмотрено соблюдение пользователем действующего законодательства как своей страны, так и страны, где располагается выбранный им сервер. Соответственно, при совершении пользователем правонарушения, используя IP-адрес VPN-провайдера, ему могут грозить как санкции со стороны своего государства, так и государства, в виртуальном сегменте которого им было совершено правонарушение. Пользователя может также ожидать и риск судебного разбирательства с самим VPN-провайдером за фактическую дискредитацию его сервиса и нарушение пользовательского соглашения. Таким образом, использование VPN-сервиса не даёт основания для совершения и сокрытия правонарушений. Более того, на плечи пользователя возлагается большая ответственность в виде соблюдения как местного законодательства, так и законодательства страны расположения подключаемого сервера VPN. Также пользователь может нести и гражданско-правовую ответственность в зависимости от его соглашения с VPN-провайдером. При этом стоит отметить, что вопрос использования заблокированных в стране Интернет-сайтов или сервисов через VPN по-прежнему достаточно дискуссионный. Однако, это не делает данные ресурсы общедоступными, поскольку бесплатные версии VPN, как правило, имеют множество ограничений, в том числе и по количеству трафика, а также скорости подключения. Стоимость платного подключения может так же представлять существенную сумму, что в любом случае способно существенно сократить посещаемость заблокированного ресурса. Кроме того, как таковое использование заблокированных сервисов со стороны населения и посещающих страну туристов не запрещается российским законодательством. Статья 29 Конституции РФ предоставляет каждому право свободно искать, получать,

передавать, производить и распространять информацию любым законным способом, за исключением сведений, составляющих государственную тайну. Использование средств обхода заблокированных ресурсов становится необходимостью и для выезжающих за рубеж государственных представителей. Так, заместитель руководителя Минкомсвязи Алексей Волин подтвердил отсутствие запрета использования средств обхода блокировок для граждан и признался, что зачастую ему самому приходится прибегать к использованию VPN в зарубежных поездках для обращения к привычным ему сервисам [71]. Таким образом, обоснованным решением стал бы пересмотр нормы о запрете доступа с иностранных VPN-серверов к ограниченным на территории РФ Интернет-ресурсам в связи с нахождением и функционированием указанных серверов в иностранной юрисдикции, а также сомнительной возможностью реализации данных норм из-за особенностей функционирования указанной технологии. При этом со стороны VPN-провайдеров, чьи серверы физически расположены на территории РФ и дают возможность выхода в сеть Интернет от российского IP-адреса, взаимной мерой стало бы соблюдение ими действующего российского законодательства. Кроме того, VPN-провайдерам следовало бы предупреждать пользователей о возможной доступности Интернет-сайтов с содержанием, признанным в их стране нахождения незаконным, и о возможной юридической ответственности за противоправные действия, совершаемые с помощью данных сервисов.

Стоит обратить внимание и на ситуации, в которых возможное недопонимание как со стороны рядовых граждан, так и должностных лиц способно приводить к необоснованным волнениям. В частности, стоит обратиться к положению части первой статьи 13.6. КоАП РФ, предусматривающий административное наказание за использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям [4]. Гипотеза в данном случае звучит следующим

образом: «Использование в сетях связи несертифицированных средств связи или несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет, если законодательством предусмотрена их обязательная сертификация» [4]. Проблема данной нормы заключается главным образом в её расплывчатой формулировке. Рядовому гражданину довольно трудно понять её истинное назначение. Во-первых, не совсем чётко определены сами как таковые «несертифицированные средства связи». В данном случае закон отсылает к Постановлению Правительства РФ от 25.06.2009 № 532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации [12]. Однако, практически любого рядового гражданина, не обладающего должными техническими познаниями, данный перечень может ввести в заблуждение. Например, термины «международные телефонные станции» или «комбинированные телефонные станции» могут вызвать ассоциации со всеми смартфонами или мобильными телефонами в целом. При этом их трактовка может отличаться от представлений обывателя. Особенно актуальным это является для тех, кто, например, приобрёл устройство для личного использования в заграничной поездке или в онлайн-магазине, не имея никаких преступных целей. При этом о необходимости сертификации устройства гражданин может просто не предполагать.

Вторым аспектом положения данной статьи КоАП РФ выступает проблемное толкование понятия «несертифицированных средств кодирования (шифрования)». Прежде всего не стоит забывать о статье 23 Конституции РФ, провозглашающей тайну переписки и иных сообщений. Средства шифрования в данном случае как раз и защищают переписку пользователей от несанкционированного доступа с какой-либо стороны. Кроме того, при использовании определённых видов шифрования владельцы мессенджеров никаким образом сами не могут иметь доступ к переписке своих пользователей, поскольку она шифруется индивидуальным ключом и хранится только на устройствах собеседников. Доступ к ней правоохранительных органов

возможен лишь в случае попадания устройства в их руки, и то возможность её извлечения даже в этом случае не является стопроцентной. Также многие пользователи выражали обеспокоенность тем, что формулировка статьи 13.6. КоАП РФ может дать добро злоупотреблениям со стороны государства. Например, возможное введение обязательной сертификации шифрования для тех же мессенджеров, в том числе и разработанных или собранных для личных нужд, никак не отразится на содержании самой статьи 13.6. КоАП РФ, что многих рядовых пользователей может ввести в заблуждение, однако компетентные органы, в свою очередь, уже будут вправе привлекать граждан, заботящихся о конфиденциальности своей личной переписки, к административной ответственности.

Тем не менее, обратившись за позицией государства, имеющей своё официальное выражение в «Извещении по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети „Интернет“», опубликованном на официальном сайте Федеральной Службы Безопасности (ФСБ), можно обнаружить интересную деталь. В данном извещении отмечается, что: «Законом Российской Федерации „О государственной тайне“ [7] обязательная сертификация средств шифрования и других средств защиты информации определена только для средств, предназначенных для защиты сведений, содержащих государственную тайну (ст. 28). Обязательной сертификации средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети „Интернет“, массово применяемых для защиты сведений, не составляющих государственную тайну, в том числе в абонентских устройствах и базовых станциях мобильной связи, компьютерах, оборудовании информационно-телекоммуникационной сети „Интернет“, на соответствие требованиям по безопасности информации не требуется» [16].

Таким образом, обязательная сертификация средств кодирования (шифрования) необходима только для средств, предназначенных для защиты сведений, содержащих государственную тайну, а не, например, мессенджеров, используемых рядовыми пользователями для частной переписки. Тем не менее, формулировка статьи 13.6. КоАП РФ не обладает чёткостью и определённостью, чем способна ввести в заблуждение граждан, не обладающих должными правовыми знаниями. На основании приведённой информации, помимо указанных выше положений, необходимым будет внесение поправок в норму статьи 13.6. КоАП РФ, а именно в её гипотезу путём уточнения о передаче исключительно сообщений и сведений, содержащих государственную тайну. Также в примечании к новой формулировке статьи или в отдельном правовом акте полезно было бы и отразить, что обязательная сертификация средств кодирования (шифрования) массово применяемых для защиты сведений, не составляющих государственную тайну не требуется. Данный подход должен максимально чётко обозначить сферу применения данной нормы, – защиту сведений, составляющих государственную тайну, а также подчеркнуть заботу государства об обеспечении права граждан на тайну сообщений, и исключить вопросы и недопонимания с их стороны. При этом нельзя не отметить, что защита сведений, содержащих государственную тайну, является крайне важной, поскольку их утечка может сильно ударить по государственной безопасности. В данном случае обязательная сертификация средств связи и шифрования для передачи и хранения подобного рода сведений является более чем оправданной. В свою очередь большинство мессенджеров являются коммерческими проектами. Регистрируясь в них, пользователь заключает соглашение с владельцем мессенджера, содержащее ряд взаимных прав и обязанностей с обеих сторон. Конечно, пользователь в данном случае частично несёт и сам ответственность за сохранение своих данных, утечка которых может быть вызвана и с его стороны, как, например, установленное на его устройстве вредоносное программное обеспечение,

попадание пароля в руки третьих лиц по его вине и т.д. Но за сохранность пользовательских данных на серверах в большей мере всё же несёт та компания, с которой пользователь и заключил соглашение. При этом за утрату пользовательских данных по вине компании для неё самой, а также её должностных лиц может быть предусмотрена юридическая ответственность. Например, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) – ст. 13.11. КоАП РФ. При этом обязательная сертификация средств шифрования для передачи и хранения государственной тайны позволяет государству максимально контролировать сам процесс и не доверять столь важные сведения в руки частных компаний, занимаясь этим самостоятельно. Аналогично можно понять и разработку властными структурами специализированных операционных систем и программного обеспечения, обрабатывающих государственные секреты.

Представляют интерес и периодически всплывающие случаи уголовных дел по статье 138.1. УК РФ [5], устанавливающей ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации. Однако, практически любое современное мобильное устройство может обладать возможностью негласного сбора информации, а потому, исходя из данных положений, и гражданин, обладающий современным смартфоном, может выступать потенциальным правонарушителем. Решением подобной проблемы могли бы стать, с одной стороны, более чёткая формулировка и расширенное толкование законодателем технических терминов в постановлении № 532, с другой же – пересмотр в целом нормы статьи 138.1 УК РФ в плане купли и использования в лично-бытовых нуждах оборудования, формально подходящего под средства негласного сбора информации. Несмотря на принятое в 2011 году решение Конституционного суда РФ [92], допускающее бытовое использование указанных средств при условии отсутствия умысла на их противоправное применение, по

словам экспертов, правоохранительные органы и суды продолжают применять положение статьи 138.1 УК буквально. Необходимость пересмотра данной нормы находила поддержку и среди некоторых депутатов Государственной Думы, согласных с недопустимостью привлечения к уголовной ответственности за бытовое использование спецсредств негласного получения информации [57]. Таким образом, хотя и относящиеся к статье 138.1 предметы (ручки с микрофонами, различные трекеры местоположения и т.д.) могут выступать орудиями нарушения неприкосновенности частной жизни, так же осуществимо их использование и в быту, в том числе для обеспечения безопасности личного имущества. При этом существенной опасности для окружающих, как огнестрельное оружие, данные предметы не представляют. Ответственность же за их использование должна наступать не иначе как по факту правонарушения, т.е. при использовании данных предметов в качестве орудия преступления.

Стоит отметить, что в последнее время технологии Интернет-анонимизации стали играть немаловажную роль непосредственно и в процессе расследования и доказывания по делам о правонарушениях. В частности, согласно статьи 26.2. КоАП РФ доказательствами принято считать любые фактические данные, полученные с соблюдением порядка, установленного законом [4]. При этом нередко одним из доказательств виновности лица стали выделять IP-адрес – уникальный сетевой адрес пользователя в сети Интернет. Тем не менее, на практике далеко не всегда исключительно он способен служить прямым доказательством виновности лица, которому он принадлежит, а современные технологии сокрытия IP-адреса способны и вовсе завести расследование в тупик. Могут так же иметь место и случаи, когда расследование выходит на конкретное лицо, которое, однако, может быть не причастно к противоправному деянию, либо иметь косвенную связь. Подобной ситуации могут способствовать различного рода обстоятельства. В частности, когда злоумышленником путём неправомерного доступа использовалось беспроводное

подключением лица (сеть Wi-Fi), либо с учётом согласия лица, но путём введения его в заблуждение о своих истинных намерениях (социальная инженерия). Помимо указанных вариантов, возможен и ещё один, пусть и достаточно новый для правоприменительной практики: когда, используя определённое программное обеспечение, лицо могло как добровольно, так и по своему незнанию дать возможность неопределённому кругу лиц иметь способность доступа в сеть Интернет от лица своего IP-адреса. В данном случае истинный владелец IP-адреса может даже не подозревать об этом, либо же всё осознавать, но предполагать исключительно добросовестное использование со стороны третьих лиц.

Возвращаясь к варианту с неправомерным доступом со стороны третьих лиц, можно с уверенностью говорить о том, что, используя уязвимости программного или аппаратного обеспечения, злоумышленникам нередко удаётся получить контроль над точками (в том числе беспроводными) доступа в сеть Интернет жертвы. При этом использовать как сам доступ в сеть от лица жертвы, так и полученные в результате данные последние могут в абсолютно любых целях, в том числе для совершения от её лица правонарушений, либо шантажа или угроз, если полученные данные имеют особо личный характер. Указанный способ неправомерного доступа уже не является чем-то новым для судебной практики, обращаясь к которой мы можем видеть множество примеров. В частности, в Приговоре Новотроицкого городского суда Оренбургской области от 9 августа 2011 г. [93] отмечается, что осуждённый, обладая достаточными познаниями в области компьютерной техники и навыками работы в сети Интернет, просканировал IP-адреса 20-ти близлежащих точек доступа. После взлома их защиты осуждённый проник в настройки самих ADSL-модемов и без согласия законных пользователей получил полный контроль над данными устройствами. В результате указанных действий осуждённому стали доступны охраняемые законом данные потерпевших. Опасность же данных действий выражается в полном контроле над точками доступа потерпевших, используя

которые осуждённый мог выходить в сеть Интернет и совершать любые действия, в том числе противоправные, фактически от их лица, поскольку помимо самого IP-адреса был способен перехватывать их данные авторизации на различных веб-сайтах. Вместе с этим, стоило бы отметить, что зачастую сами пользователи имеют слабые представления о компьютерной безопасности, что выражается в использовании слабых паролей к точкам доступа, установке сомнительного программного обеспечения, в том числе нелицензионного, либо же вовсе в отказе от какой-либо защиты со своей стороны, делая свою точку доступа открытой для неопределённого круга лиц. Отдельным фактором может выступать и безответственное отношение производителя сетевого и компьютерного оборудования к качеству и поддержке своего товара. Не выпуская программных обновлений безопасности для своих устройств, производитель ставит безопасность пользователей под угрозу, поскольку в случае отсутствия «заплаток» от программных или аппаратных уязвимостей любые, даже самые строгие меры предосторожности со стороны пользователя, могут не дать никакого результата при хакерской атаке злоумышленника. Беспечное отношение пользователя к обновлениям безопасности так же может сыграть с ним злую шутку.

Отдельного внимания заслуживают и случаи добровольного использования лицами программного обеспечения для сокрытия своих реальных данных в целом, а также оказания данного рода безвозмездных услуг, и соотношение указанных действий с Российским законодательством. Причины, как было отмечено ранее, могут быть совершенно различными, в том числе и вполне благородными, – например, содействие в использовании права на приватность и неприкосновенность частной жизни, гарантируемых статьёй 23 Конституции Российской Федерации [3].

Вместе с этим, стоит учитывать, что воспользоваться подобного рода услугой могут и недобросовестные пользователи, преследующие противоправные цели. В таких случаях, подобные лица способны не только воспользоваться добродушием

некоторых граждан, но и поставить в конечном итоге их самих под удар. Интересным случаем здесь выступает громкое дело Дмитрия Богатова [80] — московского математика и Интернет-активиста, ставшего обвиняемым по таким преступлениям как призывы к осуществлению террористической деятельности и приготовление к организации массовых беспорядков. Несмотря на то, что указанные действия были совершены с IP-адреса Богатова, он и его защита продолжали настаивать на невиновности, ссылаясь на наличие алиби, а также, что обвиняемый, будучи Интернет-активистом и не имея противоправных целей, предоставлял при помощи программного обеспечения сети Tor возможность посещать Интернет-ресурсы от лица своего IP-адреса неограниченному кругу лиц. Кроме того, в качестве одного из доказательств в пользу невиновности обвиняемого отмечалось, что, несмотря на его задержание и заключение под стражу, у аккаунта, осуществлявшего призывы к массовым беспорядкам, продолжалась наблюдаться активность, а его истинный владелец даже выходил на связь с журналистами [58]. Заметное место играет и личностная характеристика обвиняемого, не одобряющего вменяемые ему деяния, и выразившего желание сотрудничать со следствием. Несмотря на уголовно-правовую сущность дела Богатова, подобная ситуация вполне реалистична и при расследовании административных правонарушений. В частности, используя описанные выше средства анонимизации, неустановленное лицо, либо группа лиц способны распространять экстремистские материалы, что квалифицируется по статье 20.29. КоАП РФ, либо разглашать информацию с ограниченным доступом согласно статье 13.14. КоАП РФ.

Возвращаясь к статусу лица, чей IP-адрес использовался для совершения правонарушения, и которое не давало на то прямого одобрения, то его деяние нельзя квалифицировать как противоправное, поскольку само лицо в силу специфики указанной технологии может не знать о личности правонарушителя и его истинных целях, подразумевая исключительно правомерное использование. Презумпция и

обязательство исключительно законного использования указанных инструментов могут быть оговорены и в их пользовательском соглашении, с которым автоматически соглашаются все пользователи при установке данного программного обеспечения. Вместе с этим, стоит учитывать, что лицо, чей IP-адрес был так скомпрометирован, может обладать какими-либо полезными для расследования сведениями в качестве свидетеля, а также иметь на своём персональном компьютере локальный журнал деятельности со стороны его IP-адреса, который может вести данное программное обеспечение. В случае, если IP-адрес лица был скомпрометирован противоправным путём (взлом, подбор пароля, использование уязвимостей и т.п.), то правоохранительными органами должен быть осуществлён комплекс мер по защите и восстановлению его нарушенных прав [28, с. 42]. Если же с IP-адресов VPN-провайдера или прокси-сервера была зафиксирована противоправная деятельность, то те, как правило, выступая заинтересованными в справедливом расследовании происшествия, на основании вынесенного решения суда могут предоставить всю имеющуюся у них информацию по запросу правоохранительных органов.

Таким образом, мы видим, что упование исключительно на IP-адрес во многих случаях способно как запутать расследование, так и в более худшем варианте создать множество проблем для лица, чей адрес был скомпрометирован. Касаясь решения либо минимизации указанной проблемы возможно, в частности, нормативно закрепить факт невозможности прямого отождествления личности и закреплённого за ней Интернет-провайдером IP-адреса, поскольку, в связи со множеством факторов, фактически с него может заходить неограниченное количество лиц. Вместе с этим и какую-либо борьбу с подобными сервисами анонимизации, их блокировку сложно назвать обоснованными, поскольку, во-первых, это нарушает конституционное право добросовестных граждан на защиту неприкосновенности своей частной жизни и вытекающего из неё права на Интернет-

анонимность, а, во-вторых, даже при блокировке или отсутствии данных сервисов злоумышленники могут продолжить использовать какие-либо уязвимости в Интернет-протоколах, программном и аппаратном обеспечении, либо же просто брать на вооружение иные, более узкоспециализированные и менее известные общественности сервисы. Также возможно выделение из нынешних в отдельный состав такого правонарушения, как «незаконное использование IP-адреса другого лица». Под «незаконным» в данном случае следует понимать использование IP-адреса без ведома и согласия лица путём применения вредоносного программного обеспечения или уязвимостей, а равно путём обмана или подбора пароля. В целях гуманизации, возможно разделение данного состава на административный и уголовный. Административный, наказываемый штрафом, возможно оставить на случаи, когда отсутствует конечный вред, либо же он незначителен. Уголовный состав, в свою очередь, должен иметь место в случае совершения от лица жертвы правонарушения, что опорочило её доброе имя, а также причинение этими действиями существенного вреда. Данная мера может быть полезна в связи с размытостью составов статей 272 (неправомерный доступ к компьютерной информации) и 273 (создание, использование и распространение вредоносных компьютерных программ) УК РФ, а также стремительным технологическим развитием, ушедшим значительно вперёд с момента введения данных составов. Стоит понимать, что использование чужого IP-адреса может быть и добросовестным, в частности, при согласии его владельца. Однако, данное использование не должно быть сопряжено с целью совершения противоправных действий.

Что касательно организации деятельности правоохранительных органов, то при проведении расследования им прежде всего следует учитывать подобные особенности и оценивать состоятельность предъявляемых обвинений по совокупности выявленных ими фактов. К сожалению, правоприменитель не всегда

обладает должными знаниями при квалификации и расследовании правонарушений, тесно связанных с Интернет-технологиями. Поэтому, в дополнение к сказанному, оптимальным решением стало бы проведение курсов повышения квалификации в данной сфере. Альтернативой может выступать передача ведения расследования подобных дел лицам, изначально обладающим должными познаниями и опытом.

Кроме того, заметно более значимое место в подобных случаях занимают такие элементы состава правонарушения, как мотив и цель, их состоятельность. Возрастает роль и личностной характеристики подозреваемого, присутствие или отсутствие административной наказанности либо судимости по подобного рода правонарушениям или преступлениям, поскольку в особых случаях только они могут говорить о невиновности лица в связи с техническими и иными особенностями указанных дел.

Таким образом, учёт указанных выше особенностей позволит максимально обеспечить права и свободы человека, усовершенствовать качество законодательства в данной сфере в целом, а также повысить эффективность и профессионализм правоохранительных органов при расследовании правонарушений, связанных с деятельностью в сети Интернет, и защите законных интересов пострадавшей стороны.

### 3.2. Международная практика по регулированию приватности в сети Интернет

Рассмотрев правовое регулирование Интернет-приватности в Российской Федерации, а также сопутствующие ей проблемы, необходимо обратить внимание и на международную практику по данному вопросу. Анализ действующей международной практики, выявление её позитивных и негативных сторон могут способствовать совершенствованию и российского законодательства в дальнейшей перспективе.

Начиная с наиболее высшего уровня, – Организации объединённых наций (далее ООН), то, в частности, в мае 2015 года Советом по правам человека был

представлен отчёт заседания, посвящённого анонимности и шифрованию в сети Интернет [52]. По итогу заседания Советом был сделан вывод о необходимости признания составной частью прав человека анонимного использования сети Интернет, а также шифрования личных данных и средств коммуникации. В документе отмечалось, что инструменты анонимизации и шифрования необходимы для свободы выражения своего мнения в цифровую эпоху. Совет по правам человека ООН так же напомнил, что данные средства могут использоваться как злоумышленниками для совершения преступлений, так и во благо. Вместе с этим, принятие запретов на шифрование и анонимность в угоду борьбы с преступным меньшинством может нарушать права гораздо большего числа добросовестных пользователей. В результате указанных действий в уязвимом положении могут оказаться как простые граждане, заинтересованные в безопасности своих данных и доступности их сообщений непосредственным адресатам, так и журналисты, общественные организации и активисты, подвергаемые необоснованным гонениям.

Схожую позицию выразил и Европейский суд юстиции 21 декабря 2016 года. Суд счёл противоречащим нормам Европейского Союза (далее ЕС) требование к Интернет-провайдерам о накоплении и складировании ими личной информации и электронной переписки пользователей (в том числе удалённой), а также данных их геолокации [102]. В пояснении судом было отмечено, что массовое хранение Интернет-трафика и геолокационной информации пользователей позволяет получать точные данные о частной жизни граждан. Судом были приняты во внимание аргументы правозащитных организаций, касающиеся неэффективности использования колоссальных массивов накопленной информации для системного предотвращения террористических атак, а также наличия широких возможностей различного рода злоупотреблений в отношении Интернет-пользователей. Данное решение Европейского суда юстиции фактически освободило компании от

необходимости исполнения законов стран-членов ЕС, касающихся массового хранения Интернет-трафика пользователей.

Указанное решение в определённой мере можно назвать логичным продолжением складывающейся правовой практики ЕС в данной сфере. В частности, принятый ещё весной 2016 года новый закон о защите персональных данных – «Генеральный регламент о защите персональных данных» (в англ. сокр. GDPR) довольно чётко определил границы и дальнейшие перспективы развития права ЕС в области Интернет-приватности. Закон, вступивший в силу в мае 2018 года, предъявляет к компаниям, хранящим персональные данные граждан ЕС, ряд строгих требований [72]. Во-первых, компании обязали быть готовыми предоставить гражданам сведения о распоряжении их персональными данными, а также порядком обработки указанных сведений. В законе был так же определён и порядок хранения самих персональных данных. В частности, компании должны хранить их так, чтобы в случае необходимости их можно было легко перезаписать, предоставить в структурированном виде, либо удалить. В свою очередь, информационные системы предприятий, согласно, данному закону, должны быть настроены таким образом, чтобы данные, включая архивные, можно было удалить безвозвратно. Новый закон так же требует от компаний и повышения прозрачности использования персональных сведений граждан. Были ужесточены правила получения согласия на обработку личной информации, а за пользователем было закреплено право в любой момент отозвать своё согласие. Компании обязали также обозначать цели использования персональной информации пользователей и раскрывать сведения о третьих лицах, которым они передают эти данные. Кроме того, на компании была возложена ответственность и за использование личных сведений граждан третьими лицами, если они поручат им обработку данной информации. Важным моментом выступает обязательство компаний в течение 72 часов предупредить регулятора и всех пострадавших в случае кражи персональных данных. Стоит отметить, что

обязанность исполнения вышеперечисленных требований возлагается на все компании, работающие на территории ЕС, в том числе и российские. Указанные правила максимально закрепили право европейских граждан на управление личными данными, дав возможность затребовать безвозвратного удаления сведений о себе в случае, если они более не желают их дальнейшего хранения и обработки. В свою очередь, изучение и реализации данной практики российским законодателем смогли бы в большей мере обеспечить права граждан РФ на защиту и контроль их личных данных.

Однако, указанная тенденция по усилению защиты персональных данных не является общемировой. Отдельные позиции на данный счёт, в частности, имеют такие государства, как Россия, США, Китай и Казахстан. При этом подход к регулированию в указанных странах может так же разниться.

Так, весной 2017 года в США были утверждены окончательные правила, касающиеся распоряжения Интернет-провайдерами персональными данными пользователей. Палатой представителей Конгресса США было принято решение отменить норму, предписывающую Интернет-компаниям обеспечивать максимальную безопасность личных данных пользователей, и запрещающую их продажу третьим лицам без специального разрешения пользователей [62]. Решение конгресса было поддержано новоизбранным президентом США Дональдом Трампом, которым следом была подписана резолюция, окончательно отменяющая правила конфиденциальности, принятые Бараком Обамой [70]. Если ранее провайдерам не позволялось использовать, делиться или продавать историю просмотра веб-страниц своих клиентов без получения от них явного разрешения, то новые правила закрепили за ними данное право. Предыдущие правила требовали от Интернет-провайдеров и принятия «разумных» мер для защиты персональных данных пользователей от неправомерного доступа злоумышленников, а также уведомления клиентов в случае нарушения их прав. Стоит отметить, что отмену

данного закона активно лоббировали наиболее крупные игроки рынка коммуникаций, которые утверждали, что компании, предоставляющие услуги доступа в сеть Интернет, регулировались государством более жестко, чем, непосредственно сами Интернет-сервисы. Тем не менее, новый закон по-прежнему сохраняет двойную систему регулирования рынка Интернет-услуг США. В частности, компании, предоставляющие доступ к сети Интернет, контролируются Федеральной комиссией по связи, а различного рода Интернет-сервисы, вроде социальных сетей или электронной почты, регулируются Федеральной торговой Комиссией. Между тем в США уже имели место случаи необоснованной слежки Интернет-провайдерами за своими пользователями. Так, в 2011 году было обнаружено, что крупнейшие Интернет-провайдеры США продавали смартфоны с предустановленным программным обеспечением для отслеживания, которое могло отслеживать всё, начиная от посещаемых сайтов до поисковых запросов. Целями же данной слежки, по словам провайдеров, являлся якобы поиск неисправностей, а не коммерческая заинтересованность. Позднее расследование Федеральной комиссии по связи выявило факт тайной слежки одного из крупных Интернет-провайдеров, связавшего телефоны пользователей со своими собственными файлами отслеживания. В итоге провайдерами были всё же закрыты данные программы слежки, однако, после утверждения новой политики в области персональных данных фактически ничто не мешает им возродить вышеуказанную практику. Тем не менее, и при предыдущем президенте Бараке Обаме политика США в области Интернет-приватности имела специфичные детали. Так, несмотря на поддержку ограничения распоряжения персональными данными пользователей Интернет-провайдерами, Бараком Обамой отмечалось, что американским компаниям не следует производить мобильные устройства, к данным владельцев которых у властей не будет доступа в случае серьезной необходимости [86]. Обладание же устройствами, устойчивыми ко взлому, экс-президент сравнил с тем, как если бы каждому был доступен

персональный швейцарский банк в кармане. По его мнению, это затруднило бы борьбу с незаконным уклонением от уплаты налогов или финансовыми махинациями, равно как и, например, с терроризмом в случае со смартфоном. Данная точка зрения была высказана на фоне набирающей обороты судебной тяжбы между компанией Apple и Федеральным бюро расследований (ФБР) США касательно смартфона лица, совершившего теракт в Сан-Бернандино в декабре 2015 года. Несмотря на требование властей предоставить им все необходимые технические средства для взлома смартфона iPhone, принадлежавшего террористу, со стороны компании последовал отказ. Глава компании Apple Тим Кук отметил, что инженеры компании уже предоставили властям все необходимые данные, важные с точки зрения расследования теракта, и не будут передавать спецслужбам программное обеспечение, позволяющее взламывать iPhone. Причину отказа глава компании объяснил тем, что выдача данных программных и аппаратных средств ставит под угрозу безопасность личной информации всех пользователей их устройств. Указанный случай вызвал бурный резонанс, в том числе и в Организации объединённых наций. В частности, верховный комиссар ООН по правам человека Зейд Раад аль-Хусейн выразил свою обеспокоенность и призвал власти США действовать в данном деле с требуемой осторожностью. Комментируя ситуацию, верховный комиссар отметил, что существует множество иных способов сбора доказательств помимо предоставления компаниями программного обеспечения, подрывающего защиту конфиденциальности добросовестных пользователей. Распространение же подобной практики принуждения, по его мнению, может потенциально стать инструментом давления авторитарных режимов, а также содействовать кибер-преступникам [88]. Вместе с этим, он отметил, что и ФБР заслуживает максимально возможной поддержки со стороны всех в расследовании преступления в Сан-Бернардино, однако необходима определённая красная линия, необходимая для защиты всех как от преступников, так и потенциальных репрессий.

Говоря о регулировании Интернет-приватности в США нельзя оставить без внимания и так называемый «Облачный закон» (англ. CLOUD Act), позволяющий правоохранительным органам США при наличии судебного ордера получать от американских IT-компаний имеющиеся у них данные граждан США, даже при хранении последних за рубежом [49]. В свою очередь иск компании Microsoft к правительству США, в котором компания отстаивала своё нежелание передавать ФБР хранящиеся на её заграничных серверах данные, был признан американским Верховным судом не имеющим основания. Интересным моментом может выступать противоречие данного закона законодательству других стран касательно порядка обработки персональных данных граждан, имеющих как официально, так и нет двойное гражданство. В частности, согласно ч.5 ст.18 федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных» при сборе персональных данных посредством сети Интернет, оператор обязан обеспечить хранение персональных данных российских граждан на территории Российской Федерации [9]. При этом складывается ситуация, когда «Облачный закон» фактически обязывает американские компании передавать данные граждан РФ, проживающих на территории России, но имеющих так же и гражданство США, американским правоохранительным органам. Возможными способами решения возникшей проблемы могут быть как заключение соглашения между властями РФ и США, касающегося хранения и передачи персональных данных в таких случаях, либо принятие закона, предписывающего зарубежным компаниям, работающим в РФ, уведомлять как самих граждан, чьи данные были запрошены властями иностранного государства, так и российские правоохранительные органы. За гражданами, в свою очередь, должно быть право обжаловать данный запрос через российский суд в статусе гражданина РФ.

Отдельного упоминания заслуживает практика организации законного перехвата коммуникаций, осуществляемая на территории ЕС и США. При этом,

стоит отметить, что чаще всего в мире подобные системы, как правило, строятся либо на основе стандарта CALEA (англ. Communications Assistance for Law Enforcement Act), – в США, Канаде и других странах Америки, либо ETSI (European Telecommunications Standards Institute) в случае Европейского Союза. В свою очередь, российская система СОРМ, упоминаемая ранее, как отмечает С.И. Семилетов, наиболее близка к Европейской ETSI, но обладает определёнными особенностями [32]. Так, в моделях ETSI и CALEA административную функцию по контролю правомочий должностного лица правоохранительного органа и техническую работу по инициализации перехвата и документированию получаемых данных перехвата ведет непосредственно оператор связи в соответствии с условиями и предписаниями, установленными судебным ордером или иным законным разрешением уполномоченного органа. При этом оператор связи обязан документировать все выполняемые им процедуры и операции. Важной особенностью выступает недопустимость установки собственных аппаратных средств правоохранительными органами, и их самостоятельное проведение перехвата коммуникаций. За правоохранительными органами лишь сохраняется право присутствовать и контролировать действия уполномоченных на то лиц оператора связи или поставщика коммуникационных услуг. Модели ETSI и CALEA предусматривают и неподконтрольное правоохранительным органам хранение оригинальных копий данных, перехваченных в процессе оперативного расследования, у третьей уполномоченной стороны в целях предотвращения возможных подлогов, фальсификаций и прочих злоупотреблений со стороны каких-либо участников дела. Присутствуют в обеих системах и свои уникальные элементы. Так, в американской модели оператор связи передаёт полученные данные на попечение суда, выдавшего судебный ордер на конкретный перехват. В европейской же модели ETSI перехваченные в законном порядке данные хранятся в течение установленного срока у оператора связи. Таким образом, в случае возникновения

сомнений участника судебного разбирательства в отношении подлинности предоставленных сведений, суд вправе в любой момент затребовать контрольную запись, хранящуюся у уполномоченной и незаинтересованной в исходе дела третьей стороны с целью сравнения и установления истины. Ещё одной интересной особенностью европейской и американской моделей, отличающей их от модели СОРМ, выступает обязательное письменное уведомление лица, право на тайну связи которого было нарушено, в случае установления фактов неправомерного применения перехвата связи или получения персональных данных, независимо от осуществляющего перехват субъекта, будь то оператор связи, прокурор или суд. Таким образом лицо, права которого были нарушены, вправе лично или через адвоката на законном основании ознакомиться со всеми полученными в отношении его сведениями и материалами, и подготовить обоснованную жалобу или иск с истребованием морального и материального ущерба и привлечения виновных лиц к ответственности. Для сравнения, в Российской Федерации операторам связи исполнение административной функции не поручается. При осуществлении негласных оперативно-розыскных мероприятий зачастую судебное решение ему вовсе может не предъявляться. Со стороны же оператора связи действия уполномоченного органа никак не контролируются, а возможные нарушения могут не фиксироваться, поскольку при работе уполномоченного органа с пункта управления он полностью отстранён. В моделях же ETSI и CALEA оператор может выступать равноправным партнером правоохранительных органов в борьбе с преступностью и терроризмом. Таким образом, модели ETSI и CALEA обладают рядом хороших отличительных особенностей, заимствование которых могло бы существенно повысить в глазах граждан прозрачность работы их отечественного аналога – СОРМ.

Особое отношение к регулированию Интернет-приватности имеется и в ряде других стран СНГ. Так, в частности, в Казахстане с 1 января 2016 года

исполнительным органам были поручены разработка и внедрение национального сертификата, фактически дающего властям полный контроль над зашифрованным SSL-трафиком пользователей страны [85]. Решение было принято в соответствии с Законом Республики Казахстан «О связи», обязывающего операторов связи осуществлять пропуск трафика с использованием поддерживающих шифрование протоколов с применением сертификата безопасности, кроме трафика, зашифрованного на территории Республики Казахстан. По словам ответственных чиновников, цель сертификата заключается в повышении безопасности казахстанских пользователей Интернета при пользовании зарубежными ресурсами, а также для борьбы с международным терроризмом, детской порнографией и транснациональной преступностью. Тем не менее, данное решение было подвергнуто критике со стороны многих экспертов, которые сочли его потенциальной возможностью прослушки всего внешнего трафика в стране, поскольку данная технология фактически осуществляет вторжение в зашифрованные коммуникации пользователей, играя роль «посредника». В частности, президентом Ассоциации казахстанского Интернет-бизнеса Константином Горожанкиным были высказаны опасения, что, внедрив указанную технологию, государство получит доступ ко всей информации, которую пользователи передают в зашифрованном виде, в том числе банковскую. Особую проблему, по его мнению, представляет низкое доверие к надежности отечественных сертификатов, а также способам их защиты и хранения, что представляет угрозу сохранности конфиденциальных данных. Вместе с этим, в правительстве Казахстана заверили, что пользователей социальных сетей, электронной коммерции и банковского сектора это никак не затронет. Однако, отдельной проблемой выступает и признание вышеуказанного национального сертификата иностранными сервисами и браузерами в качестве доверенного по причинам, изложенным президентом Ассоциации казахстанского Интернет-бизнеса.

Интересна так же и неоднозначная позиция казахстанских властей касательно анонимности Интернет-публикаций. Так, Мажилисом Парламента Республики Казахстан были одобрены поправки в законодательство по вопросам информации и коммуникаций, обязывающие владельцев электронных ресурсов заключать с пользователями соглашения в письменной или электронной форме, подтверждая личность последних на портале «электронного правительства» или посредством SMS-идентификации [59]. При этом, размещение информации пользователями по-прежнему осталось возможным как под своим именем, так и под псевдонимом. За владельцами электронных ресурсов была так же закреплена обязанность хранить всю информацию, используемую при заключении с ними соглашения, весь период его действия, а также в течение трех месяцев после его расторжения [59]. Некоторые особенности реализации указанной поправки разъяснил министр информации и коммуникаций Республики Казахстан Даурен Абаев [73]. В частности, министр отметил, что главной целью вышеуказанных мер является повышение эффективности расследования и пресечения разжигания межнациональной розни и призывов к антиконституционным действиям. Ранее, по его словам, нарушителей вычисляли только по IP-адресу, который можно было легко скрыть, что и сподвигло к принятию указанной новеллы. В ответ на суждения, что введение подобного рода бюрократических барьеров может искоренить комментирование как таковое, министр отметил, что это нормальная практика, когда каждый должен открыто заявлять те вещи, которые он хочет прокомментировать, и что целью нововведения не стоит преследование кого-либо за критику или советы. Что же касательно Интернет-ресурсов, находящихся вне Казахстана, Абаев отметил, что с ними сохранится работа в прежнем формате, когда в случае противоправных действий, Министерство информации и коммуникаций Казахстана направляет уведомление администраторам ресурса, чтобы те удалили противоправные сообщения. Вместе с этим, в казахстанском обществе присутствуют и альтернативные точки зрения. В

частности, отмечается, что фактически отследить любой комментарий по IP-адресу сегодня и так не составляет особого труда, и подобный радикальный подход излишен. Директор общественного фонда «Правовой медиацентр» Диана Окремова, принимавшая участие в обсуждении законопроекта, замечает, что подобные меры лишь существенно усложняют процедуру регистрации и повлекут ещё большие расходы для Интернет-ресурсов [68]. Осложняет ситуацию и слабое представление властей о реализации подобной инициативы. В качестве же основного прогноза развития и реализации данной нормы фондом ожидаются уход большей части комментаторов на иностранные ресурсы или социальные сети, и утрата местных СМИ значительной части аудитории.

В свою очередь в Республике Беларусь властями был выбран более радикальный метод. Так, в 2015 году Оперативно-аналитическим центром при президенте Республики Беларусь и Министерстве связи и информатизации РБ было принято постановление «Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещённым в глобальной компьютерной сети Интернет» [18]. Данным постановлением был введён «чёрный список» веб-ресурсов, доступ к которым блокируется на уровне Интернет-провайдера, а также запрет анонимайзеров, прокси-серверов и других инструментов, позволяющих получить доступ к заблокированным ресурсам. При этом, властями не было учтено, что использование средств анонимизации возможно не только для посещения заблокированных Интернет-ресурсов, но также и при других сценариях, которые были рассмотрены нами ранее.

Отдельного внимания заслуживает и практика в сфере Интернет-приватности в Китайской Народной Республике (далее КНР). Прежде всего, стоит отметить, что сама глобальная сеть Интернет на территории КНР фактически является не совсем глобальной. Так, с 2003 года в эксплуатацию была введена система «Золотой щит», имеющая так же неофициальное название «Великий китайский файервол», и

представляющая из себя комплекс мер и инструментов по фильтрации содержимого Интернета на всей территории КНР, за исключением Гонконга и Макао. Исследователями отмечается, что для удобного мониторинга сети Интернет, властями Китая предельно ограничивается круг доступных социальных сетей и площадок для дискуссий [76]. В частности, в стране находятся под запретом такие крупные иностранные ресурсы, как Facebook, Twitter, Google и YouTube.

Специфичной выступает и политика китайских властей в сфере Интернет-коммуникаций. Так, в опубликованном отчёте Гражданской лаборатории университета Торонто, подробно рассматриваются факты пренебрежения властями КНР тайны переписки. Несмотря на то, что статьёй 35 Конституции КНР [17] гражданам гарантируется свобода слова, а статьёй 40 – свобода и тайны переписки, исследователями были зафиксированы серьёзные нарушения. В частности, специалисты отмечают, что в последние годы крупнейший сервис Интернет-коммуникации Китая – WeChat сталкивается с повышенным давлением регулирующих органов, что сподвигло, в конечном итоге к введению системы фильтрации сообщений по ключевым словам, отмеченным государственными органами в качестве нежелательных. В случае, если сообщение содержит ключевое слово из реестра, то оно не будет доставлено адресату. В свою очередь вышеуказанные фразы охватывают широкий ряд категорий, включая текущие события, политику и социальные проблемы [50]. В частности, исследователями зафиксированы блокировки сочетаний слов «массовый арест», «защитник», «права человека в Китае» и т.д. Также специалистами исследовательской лаборатории были зафиксированы и случаи перехвата неугодных правительству изображений. Реализована же данная практика при помощи аналогичного программного алгоритма, анализирующего весь отправляемый контент и выделяющий потенциально опасные для властей файлы [56]. Подтверждают это и другие случаи. Так, издание The New York Times совместно с упоминаемой ранее Гражданской

лабораторией сообщают, что после смерти китайского правозащитника и нобелевского лауреата мира Лю Сяобо ими были зафиксированы случаи цензуры Интернет-сообщений, связанных с деятельностью и его кончиной [48]. При этом цензурирование велось как в отношении запретных ключевых слов, так и изображений, связанных с правозащитником и его деятельностью. Также специалистами отмечается, что сама фильтрация контента имела место как в личных переписках, так и групповых чатах [51]. Отдельный интерес исследователей вызвала неоднозначная «двухсистемность», применяемая при фильтрации и модерировании пользовательских переписок. В частности, фильтрация ключевых слов включена в WeChat для пользователей с аккаунтами, зарегистрированными на телефонные номера материкового Китая. Фильтрация также остаётся включенной, если в будущем пользователи связывают свою учетную запись с телефонным номером страны, не принадлежащей материковой части Китая, что означает невозможность ухода от цензуры пользователями с аккаунтами, зарегистрированными в Китае, даже после их возможного переезда или смены гражданства. Подобная дифференциация доступа к контенту на основе регистрации пользователя, по-видимому, создает модель цензуры «одно приложение, две системы» [50]. Стоит отметить, что схожий принцип администрирования имеет место и в других политических сферах жизни КНР, в частности, в отношениях с Гонконгом, который, будучи специальным административным районом Китайской Народной Республики, сохраняет суверенитет во внутренних делах, и на который, в частности, не распространяется, как отмечалось ранее, система «Золотой щит». В качестве правового обоснования подобных мер фильтрации можно выделить одну из норм статьи 40 Конституции КНР, дающую возможность ограничения права на тайну переписки в случае, когда в «интересах государственной безопасности или в целях расследования уголовного преступления органы общественной безопасности или органы прокуратуры в порядке, установленном законом, осуществляют проверку переписки» [17].

Содержание данной нормы можно назвать достаточно расплывчатым, особенно касаясь «интересов государственной безопасности». Для сравнения, аналогичная норма статьи 23 Конституции РФ предусматривает ограничение данного права исключительно на основании судебного решения [3]. При этом невозможность ведения фильтрации и модерации содержимого сообщений пользователей со стороны неподконтрольных сервисов, по всей видимости, воспринимается властями Китая потенциальной угрозой, результатом чего становятся блокировки. Так, накануне съезда Коммунистической партии Китая 18 октября 2017 года, проводящегося раз в пять лет, был заблокирован мессенджер Whatsapp, известный в том числе и благодаря использованию им шифрования пользовательских сообщений. В частности, сервисом обеспечивается так называемое сквозное шифрование, что фактически означает невозможность знать о содержании сообщений даже его владельцам и администраторам. Подобные технические нюансы, представляющие крайнюю сложность для регулирования, с высокой вероятностью могли выступить основной причиной для приостановки деятельности сервиса в стране. Стоит заметить, что не все зарубежные средства Интернет-коммуникации блокируются на территории КНР. Так, в Китае продолжает свою работу сервис голосовой и видеосвязи Skype, не предоставляющий сквозного шифрования, а, следовательно, дающий возможность контроля [38].

Также в преддверии последнего съезда Коммунистической партии Китая были утверждены новые правила пользования Интернетом, направленные на борьбу с анонимными сообщениями, которые пользователи оставляют на форумах и других площадках [61]. Так, с 1 октября 2017 г. вводилось распоряжение на удаление всех подобных сообщений. Выполнение нормы было поручено Администрации киберпространства Китая. Провайдеров Интернета и сервисов, в свою очередь, обязали запрашивать и верифицировать реальные имена пользователей в процессе их регистрации. Стоит отметить, что на данный момент сама по себе указанная

инициатива не так нова. Так, в Южной Корее с 2007 по 2012 год действовала система регистрации реальных имен пользователей для сайтов с аудиторией более 100 тыс. человек в день, однако, в конечном итоге данное положение было признано Конституционным судом противоречащим основному закону страны и отменено [69]. Похожая практика, как отмечалось ранее, была введена и в Республике Казахстан, однако на данный момент всё ещё сложно говорить о её реализации в жизнь. Была закреплена китайскими властями и обязанность компаний незамедлительного сообщения властям, в случае размещения пользователем какого-либо незаконного контента. Администрацией киберпространства Китая было так же определено какой контент считается в стране незаконным. Так, помимо контента, содержащего, к примеру, оскорбления и клевету, подстрекательство к преступлениям или национальной ненависти, либо этнической дискриминации, к числу запрещённых был отнесен и достаточно расплывчатый перечень контента. В частности, запрещённой оказалась информация, «подвергающая опасности национальную безопасность» или «наносящая ущерб национальной чести и интересам», а также «подрывающая национальное единство», «содержащая слухи», «нарушающая общественный порядок» и «разрушающая социальную стабильность».

Кроме того, отдельное место занимает и отношение китайских властей к средствам анонимизации и обхода блокировок. Так как VPN и всевозможные анонимайзеры позволяют обходить «Золотой щит» ожидаема была и крайне негативная реакция. Если до недавнего времени указанные средства, действительно, были своеобразной лазейкой для его обхода. Однако, в начале 2017 года властями было принято решение о лицензировании данной сферы [39]. На все VPN-сервисы, оказывающие услуги гражданам Китая, была возложенная обязанность в согласовании своей деятельности с государственными органами. Была анонсирована 14-месячная общенациональная кампания против «несанкционированных подключений к сети Интернет». Сервисы, не получившие надлежащего разрешения,

были лишены возможности оказывать услуги китайским гражданам. Пресечение несанкционированных Интернет-соединений стало составной частью политики властей в области усиления информационной безопасности в её киберпространстве. Тем не менее, стоит отметить, что подобная игра в «кошки-мышки» длится в стране уже не первый год, и по-прежнему многие Интернет-пользователи Поднебесной, в том числе и проживающие там иностранцы, полагаются на услуги функционирующих в стране VPN-сервисов для доступа к заблокированным сайтам и службам.

Данная политика властей КНР в сфере Интернет-регулирования неоднократно вызывала и продолжает вызывать международную критику, особенно в плане соблюдения конституционных прав и свобод её граждан, а также множественной цензуры. Вместе с этим, руководитель Китая Си Цзиньпин призвал страны мира с уважением относиться к кибер-независимости друг друга и принимать факт существования различных моделей управления Интернетом [77]. Глава КНР так же отметил, что каждая страна имеет право выбирать, как развивать и регулировать свое Интернет-пространство, а кроме того решать, что блокировать и подвергать цензуре, а что нет. Вместе с этим, он добавил, что страны должны сообща работать в области обеспечения кибербезопасности. Говоря о совместной работе стран мира над общей кибербезопасностью с главой КНР трудно не согласиться. Международное сотрудничество выступает одной из важнейших основ стабильного мирового порядка и безопасности. Должно уважаться и право суверенных стран определять свою внутреннюю политику. Вместе с этим стоит отметить, что данная политика не должна умалять права и свободы человека и гражданина, гарантируемые как международными соглашениями, так и внутренним законодательством. В частности, нормы статей 35 и 40 Конституции КНР провозглашают свободу слова и печати, а также свободу и тайну переписки, даже несмотря на некоторые имеющиеся расплывчатые формулировки. Также стоит

помнить, что статьёй 12 Всеобщей декларации прав человека 1948 года [1] не допускается произвольное вмешательство в тайну корреспонденции граждан, а, статья 19, в свою очередь, предусматривает свободу убеждений и право на их свободное выражение, что выражается в свободе искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ, за исключением случаев, если это направлено на уничтожение прав и свобод, изложенных в Декларации.

Отдельного внимания заслуживает внедряемая властями Китая Система социального рейтинга (SCS), существенно охватывающая личное Интернет-пространство жителей КНР, и выступающая в перспективе мощным инструментом контроля [40]. Инициатива о внедрении данной практики появилась ещё в июне 2014 года. Её же сущность заключается в оценке и определении социальной полезности каждого конкретного гражданина, на основании чего ему присваивается соответствующий рейтинг. При этом сам рейтинг будет открыт общественности. Параметров оценивания же достаточно много, но в целом оно определяется исходя из социального поведения гражданина, включая направленность его расходов, регулярность оплаты задолженностей, взаимодействие с другими людьми. От того же какой у гражданина рейтинг будет зависеть возможность его трудоустройства, одобрение или отказ в кредите, либо продаже транспортных билетов, и даже школа, в которой смогут обучаться его дети. Несмотря на планы по внедрению системы до 2020 года уже сейчас граждане могут встать на учёт самостоятельно. При этом правительство объявило о сотрудничестве с рядом крупных компаний, как Tencent и Alibaba, по отладке необходимых алгоритмов обработки столь масштабных данных. Tencent, в свою очередь, уже принялся за внедрение системы социального рейтинга в принадлежащий ему мессенджер QQ, в котором помимо самих баллов, рейтинг каждого пользователя будет состоять из пяти категорий: социальные связи, потребительское поведение, безопасность, материальное состояние и

законопослушность. Сторонники внедрения данной системы считают, что с её помощью возможно улучшение качества государственных услуг, а также побуждение граждан к более ответственному, в том числе финансовому поведению. В свою очередь критики отмечают, что данная система выходит далеко за рамки финансовой сферы, фактически определяя ценность каждого человека и вынуждая общество считаться с этим. Имеются существенные вопросы и в плане объективности данной рейтинговой системы, которая вполне может не учесть контекст тех или иных действий и создать ошибочный образ индивида. Так, тот, кто играет в видеоигры много часов в день, может быть записан системой в маргинальную группу, в то время как он просто работает разработчиком и тестирует эти самые игры. Аналогичные этические вопросы вызывает и влияние на рейтинг таких категорий, как наличие либо отсутствие у гражданина детей, особенности его интимной жизни, либо круга общения. Несмотря на кажущуюся утопичность, наличие подобного инструмента во властных руках фактически даёт возможность навязать обществу своё представление о социально приемлемом поведении, и вместе с этим иметь возможность контролировать все аспекты жизни граждан.

Тем не менее, в политике китайских властей относительно конфиденциальности граждан в сети Интернет за последнее время имеют место и положительные моменты. Так, 1 июня 2017 года в Китае вступил в силу закон «О кибербезопасности КНР», принятый в октябре 2016 года постоянным комитетом Всекитайского собрания народных представителей. Особый интерес вызывают нормы закона, возлагающие на операторов связи повышенную ответственность за безопасность и сохранность пользовательских данных. Отныне, китайские провайдеры должны обеспечивать наличие и функционирование внутренней системы управления безопасностью, а также принимать превентивные меры против компьютерных вирусов и сетевых атак, что может выражаться в более ответственном отношении к хранению и использованию персональных данных.

Шифрование и создание копий важной информации, без чего сложно представить какое-либо безопасное её хранение, так же дополнило и без того немалый список их обязанностей. Провайдерам сетевых продуктов и Интернет-услуг был предписан и логичный запрет устанавливать какие-либо вредоносные программы. Кроме того, теперь при обнаружении в сетевых продуктах и услугах потенциально опасных уязвимостей они должны незамедлительно принять все возможные меры по исправлению ситуации, а также своевременно уведомить пользователей и соответствующие уполномоченные органы. Указанные меры, действительно, могут быть достаточно обоснованными, поскольку провайдерам связи доступен широкий круг личных и персональных данных пользователей, включая платёжные. Пренебрежительное отношение к хранению и безопасности указанной информации недопустимо и способно причинить существенный вред в случае утраты или, что хуже, утечки.

В ряде восточных стран могут применять и особо-жёсткие меры контроля. Так, в июле 2016 года Президентом Объединенных Арабских Эмиратов (далее ОАЭ) были подписаны новые поправки в законодательство, направленные на борьбу с киберпреступлениями [41]. Фактически данные нововведения криминализировали использование средств анонимизации, такие как VPN, прокси или Tor. Нарушение закона отныне карается тюремным заключением, а также штрафом в размере до 2 млн дирхам, что составляет более 30 млн рублей (или 540 тысяч долларов США) на данный момент. Несмотря на то, что VPN и прокси могут применяться в абсолютно правовых целях, в том числе для защиты своих личных данных, с точки зрения властей ОАЭ фактически теперь любой, кто скрывает свою сетевую активность подозрителен и нарушает закон. Стоит отметить, что данное правило также распространяется и на туристов, посещающих страну. По своей сути данная мира выступает продолжением политики властей ОАЭ по ужесточению регулирования Интернета. Так, в ОАЭ уже давно находятся под запретом такие общеизвестные

сервисы, как WhatsApp, Viber, Facebook Messenger и SnapChat. Также ранее на территории страны был заблокирован не менее известный сервис Skype, хотя вскоре его запрет и был снят после критики лидеров отрасли, заключающейся в том, что подобные ограничения не делают страну привлекательной в глазах иностранных компаний, а также мешают их нормальной работе. Кроме того, главные провайдеры ОАЭ, в руках которых фактически сосредоточена монополия на Интернет, аудио- и видеозвонки, давно блокируют неугодные ресурсы, порносайты, а также основательно фильтруют Интернет.

Таким образом, мы видим, что в каждой из стран мира могут иметь место свои подходы к регулированию Интернет-приватности, а также хранению личных данных пользователей. Тем не менее, в общих чертах можно выделить «социальный» и «государственный» подходы к регулированию приватности в сети Интернет. «Социальный», к приверженцам которого в большей степени можно отнести страны Европейского Союза, представляет из себя комплекс принципов и норм, сочетающих прозрачность хранения личных данных и максимальную их доступность для владельцев. Последние, в свою очередь, обладают правом отказа от их хранения и распоряжения третьими лицами даже после их передачи. Касаясь «государственного», приверженцами которого можно назвать Китай и ближневосточные страны, то ему скорее присущи больший уровень вмешательства в отношения сервиса и клиента, меньшая степень прозрачности, а также принципиально превалирующие государственные интересы в отношении правового регулирования данной сферы. Таким образом, социальному подходу соответствуют принципы верховенства прав человека и гражданина, общественной прозрачности, демократичности. Государственному, в свою очередь, принципы верховенства государственных интересов (в том числе выдаваемых за общественные или коллективные) над правами личности, закрытости, недемократичности принятия решений. Можно также выделить и отдельную переходную категорию, к которой,

например, можно отнести как Российскую Федерацию, так и США. При этом отнесение к данной категории обуславливается сложностью выявления однозначного доминирования того или иного подхода, а также попытками законодателя урвать принципы управления из обеих систем. Однако, подобную категорию сложно выделить и в какую-то отдельную или уникальную, поскольку тот или иной использующийся принцип уже присущ конкретной стороне, которая под весом принятых решений рано или поздно перевесит в свою пользу. Это, в свою очередь, означает нелёгкий выбор в плане окончательного определения модели регулирования вышеуказанного вопроса. Что же до его последствий, то основным выгодополучателем в данном случае могут быть как общество, население с его правами и свободами при общественном подходе, так и государство с его органами в случае государственного. При выборе второго, в зависимости от конкретной страны и её политической обстановки, наличие в руках государства такого мощного инструмента может привести к различным последствиям, – как к обеспечению относительной безопасности за счёт властного давления, отсутствия прозрачности и росту бюрократизации, эффективность которой, впрочем, так же можно подвергнуть критике, так и полному подавлению инакомыслия под размытыми предлогами. Превалирование государственного подхода среди восточных стран, и стран, не прошедших ещё долгий путь становления демократии, подтверждает его слабое соотношение с современными демократическими ценностями. В то же время на примере США, прибегавшим ко многим принципам государственного подхода, и особенно в плане ныне раскрытой Эдвардом Сноуденом программы глобальной слежки, мы можем видеть, что даже в государствах со столь старым институтом демократии без надлежащего общественного контроля возможно обособление властных интересов от интересов граждан под различными уловками.

## Заключение

Таким образом, на основании приведённой информации можно сделать вывод, что приватность в сети Интернет, будучи составной частью конституционного права на неприкосновенность частной жизни и тайну сообщений, выступает важной, но ещё не до конца исследованной правоведами категорией. Являясь следствием бурного развития Интернет-технологий за последние десятки лет, указанная сфера обладает рядом особенностей, как технического, так и юридического характера. При этом те методы регулирования, работающие в отношении аналоговых средств коммуникации, как почтовая корреспонденция или телефонная связь, могут быть не эффективными или даже вредными при взаимодействии с Интернет-инструментами.

Обращаясь к теоретической составляющей права на приватность в сети Интернет, то стоит упомянуть о его элементах: тайне Интернет-сообщений, и Интернет-анонимности. Под тайной Интернет-сообщений следует понимать реализацию человеком права на конфиденциальность его общения и переписки через средства Интернет-коммуникации: как правило мессенджеры, сервисы аудио- и видеосвязи, а также личные сообщения в социальных сетях. Под Интернет-анонимностью же – стремление сохранить в тайне своё пребывание в сети Интернет путём использования средств анонимизации. Интересной особенностью указанных элементов выступает их способность как коррелировать друг другу, так и сосуществовать в раздельности. Так, в частности, не каждому может быть принципиально сокрытие своего Интернет-трафика, имея лишь заинтересованность в конфиденциальности своей Интернет-переписки. Иной же пользователь может ожидать как сохранности в тайне самой переписки, так и всего своего трафика. Цели же сокрытия подобного рода информации могут быть различны, но, должны предполагать законность и добросовестность (например, нежелание потенциальной слежки со стороны различных сервисов и Интернет-служб, или психологическая удовлетворенность своей приватностью). Стоит помнить, что, порой, данными

средствами пользуются и для противоправных целей, что, очевидно, не может подпадать под защиту законом. Однако, умаление прав неопределённого числа добросовестных пользователей путём автоматической слежки и прочего мониторинга является так же недопустимым, поскольку ограничение права на тайну переписки и иных сообщений допускается Конституцией только на основании судебного решения в отношении конкретного лица или определённой группы лиц, имеющих отношение к рассматриваемому делу.

Говоря о взаимодействии правоохранительных органов и организаторов распространения информации, прежде всего мы можем выделить необходимость выработки политики заинтересованности обеих сторон в эффективном противодействии реальной преступности, не нарушая при этом прав добросовестных пользователей. Тем не менее, возможны и случаи расхождения мнений, в том числе вследствие различной юрисдикции и иных причин. Однако, и в подобных случаях возможны компромиссы, выражающиеся, к примеру, в сохранении неприкосновенности личных переписок пользователей, но в блокировке публичных страниц, аккаунтов, групп или чатов, пропагандирующих терроризм и иную преступную деятельность. Возможно и достижение соглашений по выявлению создателей подобного рода страниц и чатов, их активных участников для дальнейших разбирательств, поскольку подобная деятельность так или иначе публична, и раскрытие связанных с ней данных не грозит приватности добросовестных пользователей. При этом по-прежнему сохраняется необходимость выработки на международном уровне адекватной, соответствующей времени и принципам прав человека политики взаимодействия организаторов распространения информации и государственных структур по противодействию международной преступности. При этом организаторы распространения информации, будучи профессионалами в указанной сфере, должны выступать полноправными участниками данного диалога.

Нами были рассмотрены и основные проблемы реализации права приватности в сети Интернет на примере элементов Интернет-приватности – тайны Интернет-сообщений и Интернет-анонимности. С одной стороны, отсутствие вовсе какого-либо контроля в данной сфере может стимулировать рост правонарушений, создавая иллюзию полной безнаказанности, с другой же – тотальный контроль и массовая слежка нарушают право на неприкосновенность частной жизни и тайну переписки добросовестных граждан, способствует их необоснованной самоцензуре даже в конфиденциальном общении. Любое вмешательство государства должно быть обоснованным и нести цель защиты прав и законных интересов его граждан. Одним из негативных примеров такого вмешательства можно назвать, в частности, историю бывшего сотрудника АНБ США Эдварда Сноудена, раскрывшего миру информацию о глобальной правительственной слежке. Однако, не только государственные структуры могут быть заинтересованы в слежке за пользователями сети Интернет. Таковыми могут быть и крупные Интернет-корпорации, собирающие «Большие данные» пользователей, как правило, в рекламных целях, но нередко с возможностью их дальнейшей перепродажи третьим лицам. В данном случае, даже передача обезличенной информации должна сопровождаться уведомлением пользователя о передаваемых им данных, и возможностью его отказа.

Нами были изучены и проблемы Интернет-приватности в российском законодательстве, а также международная практика по данному вопросу. Хотя до недавнего времени сфера Интернет-приватности в Российской Федерации не была столь ярко освещена вниманием, в последние годы вопросы её регулирования встают всё более остро. Началом же ему послужило введение в 1996 году Системы оперативно-розыскных мероприятий (СОРМ), обновляющейся и развивающейся до сих пор. И хотя первая версия была заточена лишь на прослушивание телефонных переговоров, последнее её поколение включает в себя внушительную систему сбора и хранения данных, включая информацию о перемещениях, телефонные переговоры,

сообщения и Интернет-трафик, а также достаточно широкие полномочия правоохранительных органов по обращению с данным комплексом. Хотя аналоги СОРМ присутствуют и в странах ЕС, а также США, российская версия имеет определённые проблемы. Наиболее острой из них выступает низкий уровень прозрачности как для граждан в целом, так и для операторов связи, что препятствует должному общественному контролю данной сферы, и создаёт почву для различных злоупотреблений и превышений полномочий со стороны правоохранительных органов. В свою очередь для общества работа над данными проблемами в сторону большей прозрачности функционирования СОРМ становится всё более актуальной при стремительном росте интернетизации и растущем охвате ею нашей жизни.

Также было определено, что в целях обеспечения права граждан на Интернет-приватность необходимо внести в действующее законодательство ряд изменений и дополнений. В частности, статьи 10.1 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также 46 федерального закона N 126-ФЗ «О связи» следует дополнить нормой, обязывающей организатора распространения информации в случае обнаружения утечки, а равно иной виновной компрометации личной информации пользователей, переписок и их содержания уведомить пострадавшую сторону немедленно (либо в кратчайшие сроки) после обнаружения указанной компрометации. Необходимо и включение в главу 13 КоАП РФ состава: «Сокрытие должностным (юридическим) лицом факта утечки (компрометации) личной информации». Также в федеральном законе № 144-ФЗ от 12.08.1995 «Об оперативно-розыскной деятельности» обоснованно включение «электронного наблюдения» в список оперативно-розыскных мероприятий, поскольку фактически данные отношения уже сложились, но ещё не закреплены нормативно. При этом в целях обеспечения прозрачности необходимо внесение в Уголовно-процессуальный кодекс Российской Федерации или федеральный закон «Об оперативно-розыскной деятельности» чёткой классификации тех преступлений,

при расследовании которых может применяться электронное наблюдение, либо же конкретных случаев, когда это оправдано или необходимо. Заслуживают законодательного закрепления и рамки проведения электронного наблюдения, где уведомление оператора связи становилось бы обязательным. Представляет также важность внесение поправок в норму статьи 13.6. КоАП РФ, уточняющих о запрете передачи через несертифицированные средства кодирования (шифрования) исключительно сообщений и сведений, составляющих государственную тайну, и отражение в новой формулировке статьи в виде примечания или отдельном правовом акте об отсутствии обязательной сертификация средств кодирования (шифрования) массово применяемых для защиты сведений, не составляющих государственную тайну. Кроме того, как минимум заслуживают пересмотра и нормы статьи 64 федерального закона «О связи», обязывающие операторов связи хранить Интернет-трафик абонентов, до разработки более прозрачного и безопасного механизма реализации, не вступающего в конфликт с конвенционным и конституционным правом на приватность. Заслуживает внимания и положение статьи 10.1 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» о передаче организаторами распространения информации ключей шифрования, которое заслуживает значительного пересмотра, либо полной отмены в связи с выявленными рисками и этическими проблемами, а также технической невозможностью реализации в определённых случаях. Так, передача ключей шифрования третьим лицам может быть потенциально небезопасна для всех пользователей сервиса, либо организатор распространения информации может вовсе не иметь доступа к сообщениям на устройстве из-за технических особенностей используемых им технологий. Отдельное внимание стоит обратить и на политику блокировки Интернет-ресурсов, не преследующих противоправных целей и готовых к сотрудничеству с правоохранительными органами в плане пресечения незаконного публичного контента. Предлагается практика по внесению

Интернет-ресурсов, не соответствующих в полней мере государственным стандартам, в публичный реестр «сомнительных» сервисов при сохранении к ним доступа, но наложения некоторых ограничений, вроде отказа от каких-либо налоговых послаблений или их государственной финансовой поддержки. В противовес этому Интернет-ресурсам, в полной мере соответствующим государственным стандартам, предлагается их одобрение в виде выдаваемых электронных сертификатов, а также возможности некоторых налоговых послаблений, либо финансовой господдержки, если Интернет-ресурс является отечественным. Таким образом, обеспечивается баланс между ограничением доступа к Интернет-ресурсам, действительно, преследующим противоправные цели, и сохранением за пользователем выбора в условиях справедливой конкуренции. Говоря о порядке функционирования такого инструмента как VPN, обоснованным стал бы пересмотр нормы о запрете доступа с иностранных VPN-серверов к ограниченным на территории РФ Интернет-ресурсам в связи с нахождением и функционированием указанных серверов в иностранной юрисдикции, а также сомнительной возможностью реализации данных норм из-за особенностей функционирования данной технологии. В свою очередь со стороны VPN-провайдеров, чьи серверы физически расположены на территории РФ и дают возможность выхода в сеть Интернет от российского IP-адреса, взаимной мерой стало бы соблюдение ими действующего российского законодательства. При использовании же зарубежных VPN-серверов достаточной мерой может выступить предупреждение пользователей о возможной доступности Интернет-сайтов с содержанием, признанным в их стране нахождения незаконным, и о возможной юридической ответственности за противоправные действия, совершаемые с помощью данных сервисов. В связи с достаточно частым применением положения статьи 138.1 УК РФ в отношении лиц, не имеющих умысла нарушать право приватности других, и мнением КС РФ, подчёркивающим руководящую роль

умысла в составе указанного преступления, должной мерой стал бы пересмотр положений данной нормы и легализация исключительно бытовых сценариев использования указанных инструментов. Говоря о киберпреступлениях, результатом которых стала незаконная эксплуатация чужих IP-адресов для совершения правонарушений, необходимой мерой может стать выделение из статей 272 (неправомерный доступ к компьютерной информации) и 273 (создание, использование и распространение вредоносных компьютерных программ) УК РФ отдельного состава правонарушения, предусматривающего юридическую ответственность за незаконное использование IP-адреса другого лица. Данная мера может быть полезна в связи с размытостью вышеуказанных составов, а также стремительным технологическим развитием, ушедшим значительно вперёд с момента введения данных составов. В целях гуманизации, допустимо разделение данного состава на административный и уголовный. Административный, наказываемый штрафом, возможно оставить на случаи, когда отсутствует конечный вред, либо же он незначителен. Уголовный состав, в свою очередь, должен иметь место в случае совершения от лица жертвы правонарушения, что опорочило её доброе имя, а также причинение этими действиями существенного вреда. «Незаконное использование» в данном случае должно предполагать использование IP-адреса без ведома и согласия лица путём применения вредоносного программного обеспечения, либо уязвимостей, а равно путём обмана или подбора пароля.

Обратившись к международной практике в отношении Интернет-приватности, мы увидим её существенное многообразие в зависимости от региона. Тем не менее, в общих чертах можно выделить «социальный» и «государственные» подходы к регулированию приватности в сети Интернет. «Социальный», к приверженцам которого в большей мере относятся страны Европейского Союза, представляет из себя комплекс принципов и норм, сочетающих прозрачность хранения личных данных и максимальную их доступность для владельцев, включающую право отказа

от хранения и распоряжения своих личных данных третьими лицами, в том числе и после передачи. В свою очередь «государственному» подходу, приверженцами которого можно назвать Китай и ближневосточные страны, присущ больший уровень вмешательства в отношения сервиса и клиента, меньшая степень прозрачности, а также руководящая роль государственных интересов в отношении правового регулирования данной сферы. Таким образом, социальному подходу соответствуют принципы верховенства прав человека и гражданина, общественной прозрачности, демократичности, а государственному, в свою очередь, – принципы верховенства государственных интересов (в том числе выдаваемых за общественные или коллективные) над правами личности, закрытости, недемократичности принятия решений. Можно также выделить и отдельную переходную категорию, к которой, например, можно отнести как Российскую Федерацию, так и США. Главным образом отнесение к данной категории обуславливается сложностью определения превалирования того или иного подхода, а также попытками властей урвать те или иные принципы управления из обеих систем. Однако, подобную категорию сложно выделить и в какую-то отдельную или уникальную, поскольку тот или иной использующийся принцип уже присущ конкретной стороне, которая под весом принятых решений рано или поздно начнёт доминировать. В случае же ориентирования на ту или иную модель, основными выгодополучателями могут выступать как общество в целом, а также население с его правами и свободами при общественном подходе, либо же государство и его органы в случае государственного. При выборе второго, в зависимости от конкретной страны и её политической обстановки, наличие в руках государства столь мощного инструмента может привести к различным последствиям, – как к обеспечению безопасности за счёт давления, отсутствия прозрачности и росту бюрократизации, эффективность которой, впрочем, так же можно подвергнуть критике, так и подавлению инакомыслия под размытыми предлогами. Говоря о Российской Федерации, можно

сделать вывод, что с учётом таких ошибок советского периода, как наличие репрессивных механизмов и нередких должностных злоупотреблений, очередной разворот к превалированию государства над личностью и обществом нельзя назвать необходимым, обоснованным и соответствующим действующим конституционным принципам, провозглашающим человека, его права и свободы высшей ценностью.

## Список используемой литературы

**Нормативно правовые акты:**


1. Всеобщая декларация прав человека (Принята Генеральной Ассамблеей ООН 10.12.1948) // Официальный сайт Организации объединённых наций. URL: http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml/ (Дата обращения: 22.02.2018).
2. Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс (Дата обращения: 22.02.2018).
3. Конституция Российской Федерации: закон от 12.12.1993 / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения: 22.02.2018).
4. Кодекс Российской Федерации об административных правонарушениях: федеральный закон от 30.12.2001 N 195-ФЗ / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс». (Дата обращения: 22.02.2018).
5. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 N 63-ФЗ / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения: 22.02.2018).
6. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс». (Дата обращения: 22.02.2018).
7. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»: / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения 22.02.2018).

8. Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения: 22.02.2018).
9. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения: 15.04.2018).
10. Федеральный закон от 06.07.2016 N 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания Консультант Плюс (Дата обращения: 22.02.2018).
11. Федеральный закон «О Федеральной службе безопасности» от 03.04.1995 N 40-ФЗ / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения: 22.02.2018).
12. Постановление Правительства РФ от 25.06.2009 N 532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации» / Справочно-правовая система «Консультант Плюс» [Электронный ресурс] // Компания «Консультант Плюс» (Дата обращения: 22.02.2018).
13. Постановление Правительства Российской Федерации от 18.01.2018 № 21 «О внесении изменений в Правила взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети „Интернет “ с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201801220009?index=0&rangeSize=1/ (Дата обращения: 22.02.2018).

14. Постановление Правительства Российской Федерации от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» [Электронный ресурс] // Официальный Интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201804190032?index=0&rangeSize=1 (Дата обращения: 19.04.2018).
15. Приказ Министерства информационных технологий и связи Российской Федерации от 16.01.2008 № 6 «Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий» / Справочно-правовая система «Гарант» // Компания «Гарант» (Дата обращения: 22.02.2018).
16. Извещение по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети «Интернет» от 18.07.2016 // Официальный сайт ФСБ. URL: http://www.fsb.ru/fsb/science/single.htm%21_print%3Dtrue%26id%3D10437738%40fsbResearchart.html/ (Дата обращения: 22.02.2018).
17. Конституция КНР 1982 г. (с изм. 1988, 1993, 1999, 2004 гг.) // ChinaInfo. URL: http://chinalawinfo.ru/constitutional_law/constitution/ (Дата обращения: 22.02.2018).
18. Постановление Оперативно-аналитического центра при президенте Республики Беларусь и Министерстве связи и информатизации РБ от 19.02.2015 № 6/8 «Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещённым в глобальной компьютерной сети Интернет» // Национальный правовой Интернет-портал Республики

Беларусь. URL: http://pravo.by/document/?guid=12551&p0=T21503059&p1=1/ (Дата обращения: 22.01.2018).

**Специальная литература:**

19. Friedman, M. Edward Snowden: hero or traitor? Considering the implications for Canadian national security and whistleblower law [Text] / M. Friedman // Dalhousie Journal of Legal Studies Vol. 24. – University of Ottawa, 2015. – PP. 1-23.

20. Hays, D. The Ethics of Government Surveillance: Is Edward J. Snowden a Hero or a Villain? [Text] / D. Hays // Mercatus Center. – The University of Liechtenstein, 2015. – PP. 1-12.

21. Warren S., Brandeis L. The Right to Privacy [Электронный ресурс] / S. Warren, L. Brandeis // Harvard Law Review, 1890. – PP. 193-220. / URL: http://www.jstor.org/stable/1321160// (Дата обращения: 22.02.2018).

22. Аберхаев Э.Р. Право на неприкосновенность частной жизни: юридическая характеристика и проблемы реализации [Текст] / Э.Р. Аберхаев // Актуальные проблемы экономики и права. – 2008. - №1. С. 90-94.

23. Баглай М.В. Конституционное право Российской Федерации [Текст]: учеб. для вузов / М.В. Баглай. – 6-е изд., изм. и доп. – М.: Норма, 2007. – 784 с. ISBN: 978-5-468-00078-6.

24. Дарбинян С., Климарёв М., Говядинов С. Рейтинг открытости мобильных операторов [Текст] / С. Дарбинян, М. Климарёв, С. Говядинов // Роскомсвобода, Общество защиты Интернета – 2018. – 58 с. URL: https://roskomsvoboda.org/media/2018/03/RDR-report.pdf (Дата обращения: 29.03.2018).

25. Куликова С.А. Конституционно-правовые аспекты содержания понятия «тайна» [Текст] / С.А. Куликова // Ленинградский юридический журнал. – 2012. - №4. С. 221-229.

26. Майоров А.В., Поперина Е.Н. Формирование и развитие права на неприкосновенность частной жизни [Текст] / А.В. Майоров, Е.Н. Поперина // Юридическая наука и правоохранительная практика. – 2012. - №3(21). С. 34-38.
27. Митин Е.В. Право на тайну сообщений, передаваемых по электронным почтовым ящикам: проблемы реализации [Текст] / Е.В. Митин // Теория и практика общественного развития. – 2012. - №9. С. 271-273.
28. Назаров С.А. IP адрес как идентификатор при расследовании правонарушений [Текст] / С.А. Назаров // Сборник статей Международной научно-практической конференции «Актуальные проблемы правотворчества и правоприменительной деятельности в Российской Федерации» (Том 2) (Самара, 11.01.2017 г.). – Уфа: Аэтерна, 2017. – С. 40-44.
29. Назаров С.А. Концепция Интернет-приватности // Сборник статей Международной научно-практической конференции «Актуальные вопросы современного права. Пути теоретического и практического решения проблем» (Уфа, 01.03.2018 г.). – Уфа: Аэтерна, 2018. – С. 130-133.
30. Назаров С.А. Правовая охрана тайны сообщений в Российской Федерации [Текст] / С.А. Назаров // Сборник тезисов работ участников XI Всероссийского конкурса молодёжи образовательных и научных организаций на лучшую работу «Моя законотворческая инициатива» (II том). – М.: Государственная Дума ФС РФ, НС «ИНТЕГРАЦИЯ», 2016. – С.119-120.
31. Поперина Е.Н. Пределы допустимого вмешательства государства в сферу частной жизни [Текст] // Правопорядок: история, теория, практика. – 2014. - № 1 (2). С. 41-46.
32. Семилетов С.И. Модель правовой организации оперативно-розыскных мероприятий на сетях связи в Российской Федерации [Текст] // Труды Института государства и права РАН, № 5, 2012. С. 191-205.

33. Стешенко Л.А., Шамба Т.М. История государства и права России [Текст]: Академический курс. Т. 1. М.: Норма, 2003. – 480 с. ISBN: 5-89123-667-2.

34. Стороженко О.Ю. Система технических средств для обеспечения функций оперативно-розыскных мероприятий: вчера, сегодня, завтра [Текст] // Вестник Краснодарского университета МВД России, № 3 (25), 2014. С. 69-72.

35. Фролова О.С. Частная жизнь в свете Конвенции о защите прав человека и основных свобод [Текст] / О.С. Фролова // Журнал российского права. – 2008. - №10(142). С. 118-123.

36. Шкудунова Ю.В. Концептуальная основа «публичности» и «приватности» / Ю.В. Шкудунова // Вестник Омского университета. – 2007. - №4. С. 64-68.

**Интернет-ресурсы:**

37. A View of ISIS's Evolution in New Details of Paris Attacks [Electronic resource] // The New York Times, 2016. URL: https://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html/ (Дата обращения: 22.02.2018).

38. China Blocks WhatsApp, Broadening Online Censorship [Electronic resource] // The New York Times, 2017. URL: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html/ (Дата обращения: 22.02.2018).

39. China tightens Great Firewall by declaring unauthorised VPN services illegal [Electronic resource] // South China Morning Post, 2017. URL: http://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall/ (Дата обращения: 22.02.2018).

40. China's "Social Credit System" Will Rate How Valuable You Are as a Human [Electronic resource] // Futurism, 2017. URL: https://futurism.com/china-social-credit-system-rate-human-value/ (Дата обращения: 22.02.2018).

41. Dh 500,000 fine if you use fraud IP in UAE: President issues several federal laws [Electronic resource] // Emirates 24/7 News, 2016. URL:

https://www.emirates247.com/news/emirates/dh500-000-fine-if-you-use-fraud-ip-in-uae-2016-07-22-1.636441/ (Дата обращения: 22.02.2018).

42. Facebook годами собирал информацию о звонках и СМС пользователей так, что они об этом не догадывались. В соцсети говорят, что все законно [Электронный ресурс] // Meduza, 2018. URL: https://meduza.io/feature/2018/03/27/facebook-godami-sobiral-informatsiyu-o-zvonkah-i-sms-polzovateley-tak-chto-oni-ob-etom-ne-dogadyvalis-v-sotsseti-govoryat-chto-vse-zakonno (Дата обращения: 29.03.2018).
43. Facebook рассказал о сканировании личных сообщений пользователей [Электронный ресурс] // РБК, 2018. URL: https://www.rbc.ru/technology_and_media/04/04/2018/5ac4fd779a7947420af1b3bb (Дата обращения: 11.04.2018).
44. FBI blasts Apple, Google for locking police out of phones [Electronic resource] // The Washington Post, 2014. URL: https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html/ (Дата обращения: 22.02.2018).
45. Google начнет показывать имя и фото пользователей в рекламе [Электронный ресурс] // Вести, 2013. URL: https://hitech.vesti.ru/article/620611/ (Дата обращения: 22.02.2018).
46. Google ушел из Китая [Электронный ресурс] // Forbes, 2010. URL: http://www.forbes.ru/tehno/internet-i-telekommunikatsii/46869-google-ushel-iz-kitaya/ (Дата обращения: 22.02.2018).
47. Let's Encrypt Stats [Электронный ресурс] // Let’s Encrypt. URL: https://letsencrypt.org/stats/ (Дата обращения: 22.02.2018).
48. Liu Xiaobo’s Death Pushes China’s Censors Into Overdrive [Electronic resource] // The New York Times, 2017. URL: https://www.nytimes.com/2017/07/17/world/asia/liu-xiaobo-censor.html/ (Дата обращения: 22.02.2018).

49. Microsoft, Apple и Google обязали выдавать властям США переписку пользователей с серверов по всему миру [Электронный ресурс] // CNEWS, 2018. URL: http://www.cnews.ru/news/top/2018-04-06_microsoft_okonchila_tyazhbu_s_vlastyamikotoraya_izmenila (Дата обращения: 15.04.2018).
50. One App, Two Systems. How WeChat uses one censorship policy in China and another internationally [Electronic resource] // Citizenlab, 2016. URL: https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/ (Дата обращения: 22.03.2018).
51. Remembering Liu Xiaobo. Analyzing censorship of the death of Liu Xiaobo on WeChat and Weibo [Electronic resource] // Citizenlab, 2017. URL: https://citizenlab.ca/2017/07/analyzing-censorship-of-the-death-of-liu-xiaobo-on-wechat-and-weibo/ (Дата обращения: 22.02.2018).
52. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression [Electronic resource] // SCRIBD. URL: https://ru.scribd.com/doc/266938105/A-HRC-29-32-AEV/ (Дата обращения: 22.02.2018).
53. Report: Some Android phones are given credit for security patch updates they never received [Electronic resource] // phoneArena, 2018. URL: https://www.phonearena.com/news/Some-Android-handset-manufacturers-skip-security-updates-while-making-it-look-like-it-was-installed_id104036 (Дата обращения 15.04.2018).
54. Telegram в октябре заблокировал более 8500 каналов за связь с терроризмом [Электронный ресурс] // Ведомости, 2017. URL: https://www.vedomosti.ru/technology/news/2017/10/29/739749-telegram-v-oktyabre-zablokiroval/ (Дата обращения: 22.02.2018).

55. Warrant Canary Frequently Asked Questions [Electronic resource] // Electronic Frontier Foundation, 2014. URL: https://www.eff.org/deeplinks/2014/04/warrant-canary-faq/ (Дата обращения: 22.02.2018).
56. We (Can't) Chat "709 Crackdown" Discussions Blocked on Weibo and WeChat [Electronic resource] // Citizenlab, 2017. URL: https://citizenlab.ca/2017/04/we-cant-chat-709-crackdown-discussions-blocked-on-weibo-and-wechat/ (Дата обращения: 22.02.2018).
57. А за коровой следить можно. За использование «шпионских» гаджетов в быту не накажут [Электронный ресурс] // Российская Газета, 2017. URL: https://rg.ru/2017/12/25/v-rossii-zapretiat-nakazyvat-za-ispolzovanie-shpionskih-gadzhetov-v-bytu.html (Дата обращения: 18.04.2018).
58. Автор экстремистских постов с IP-адреса Богатова назвался гражданином США [Электронный ресурс] // РБК, 2018. URL: https://www.rbc.ru/rbcfreenews/58f8d23d9a79472ad5332a7b/ (Дата обращения: 22.02.2018).
59. Анонимные комментарии в Интернете запретят: Мажилис одобрил поправки [Электронный ресурс] // Tengri News, 2017 / URL: https://tengrinews.kz/kazakhstan_news/anonimnyie-kommentarii-internete-zapretyat-majilis-odobril-331676/ (Дата обращения: 22.02.2018).
60. База ФСКН с тысячами ВИЧ-инфицированных, наркозависимых, склонных к суициду и пациентов психбольниц утекла на чёрный рынок [Электронный ресурс] // Роскомсвобода, 2016. URL: https://roskomsvoboda.org/21087/ (Дата обращения: 24.03.2018).
61. В Китае полностью запретили анонимность в Интернете [Электронный ресурс] // Cnews, 2017. URL: http://safe.cnews.ru/news/top/2017-08-28_v_kitae_zapretili_pisat_anonimnye_posty_v_internete/ (Дата обращения: 22.02.2018).

62. В США отменили закон, запрещавший провайдерам торговать пользовательскими данными [Электронный ресурс] // Роскомсвобода, 2017. URL: https://roskomsvoboda.org/27157/ (Дата обращения: 22.02.2018).
63. Ваш «умный» квартирный водосчетчик оборудован подслушивающим устройством [Электронный ресурс] // Интернет-сайт академика Теплышева Вячеслава Юрьевича, 2010. URL: https://teplyshev.wordpress.com/2-2/ (Дата обращения: 19.04.2018).
64. Ваш разговор подписывается, и ставится печать [Электронный ресурс] // Коммерсант, 2018. URL: https://www.kommersant.ru/doc/3606298 (Дата обращения: 19.04.2018).
65. Взломанные измены обратились самоубийствами [Электронный ресурс] // Коммерсант, 2015. URL: https://www.kommersant.ru/doc/2796076/ (Дата обращения: 22.02.2018).
66. Вне прослушки: почему Роскомнадзор и ФСБ судятся с операторами связи [Электронный ресурс] // РБК, 2017. URL: https://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53/ (Дата обращения: 22.02.2018).
67. Вступил в силу закон о запрете обхода блокировок через VPN и анонимайзеры [Электронный ресурс] // Ведомости, 2017. URL: https://www.vedomosti.ru/technology/news/2017/11/01/740155-vpn-anonimaizeri (Дата обращения: 15.04.2018).
68. Государство собирается запретить анонимные комментарии в СМИ. Зачем это делается? [Электронный ресурс] // Информбюро, 2017. URL: https://informburo.kz/stati/gosudarstvo-sobiraetsya-zapretit-anonimnye-kommentarii-v-smi-zachem-eto-delaetsya.html/ (Дата обращения: 22.02.2018).
69. Гражданам Южной Кореи вернули анонимность комментариев в сети [Электронный ресурс] // Росбалт, 2012. URL:

http://www.rosbalt.ru/main/2012/08/24/1025998.html/ (Дата обращения: 22.02.2018).

70. Дональд Трамп окончательно лишил американцев конфиденциальности [Электронный ресурс] // Роскомсвобода, 2017. URL: https://roskomsvoboda.org/27288/ (Дата обращения: 22.02.2018).
71. Замминистра связи не видит проблем в блокировке Telegram [Электронный ресурс] // Ведомости, 2018. URL: https://www.vedomosti.ru/technology/news/2018/04/13/766627-minkomsvyazi-zayavilo (Дата обращения: 15.04.2018).
72. Защита персональных данных европейцев дорого обойдется российскому бизнесу [Электронный ресурс] // ТАСС, 2017. URL: http://tass.ru/ekonomika/4655909/ (Дата обращения: 22.02.2018).
73. Как будут находить «плохих» комментаторов в Казнете [Электронный ресурс] // Tengri News, 2017. URL: https://tengrinews.kz/kazakhstan_news/kak-budut-nahodit-plohih-kommentatorov-v-kaznete-332022/ (Дата обращения: 22.02.2018).
74. Как шпионят за миром [Электронный ресурс] // Российская Газета, 2014. URL: https://rg.ru/2014/01/28/snouden.html/ (Дата обращения: 22.02.2018).
75. Какой гражданин России имеет право на уважение частной жизни [Электронный ресурс] // Ведомости, 2018. URL: https://www.vedomosti.ru/politics/articles/2018/02/26/751940-za-utechku-ne-otvechaem (Дата обращения: 24.03.2018).
76. Китай истребляет пятую колонну [Электронный ресурс] // Газета.Ру, 2014. URL: https://www.gazeta.ru/science/2014/08/22_a_6185281.shtml/ (Дата обращения: 22.02.2018).
77. Китай настаивает на праве цензуры в интернете [Электронный ресурс] // Русская служба BBC, 2015. URL:

http://www.bbc.com/russian/international/2015/12/151216_china_internet_conference/ (Дата обращения: 22.02.2018).

78. Конституционный совет Франции одобрил новый закон о слежке [Электронный ресурс] // РИА Новости, 2015. URL: https://ria.ru/world/20150724/1145904208.html/ (Дата обращения: 22.02.2018).
79. Крупная утечка: Оператор Wi-Fi в метро Москвы выкладывает данные о пользователях в общий доступ [Электронный ресурс] // The Village, 2018. URL: http://www.the-village.ru/village/city/situation/308363-krupnaya-utechka-operator-wi-fi-v-metro-moskvy-vykladyvaet-dannye-o-polzovatelyah-v-obschiy-dostup (Дата обращения: 15.04.2018).
80. Математик Богатов вышел из СИЗО [Электронный ресурс] // Газета.Ru, 2017. URL: https://www.gazeta.ru/social/2017/07/24/10802642.shtml/ (Дата обращения: 22.02.2018).
81. Мессенджер выпускника мехмата МГУ стал инструментом протеста в Гонконге [Электронный ресурс] // РБК, 2014. URL: https://www.rbc.ru/technology_and_media/30/09/2014/542a70d8cbb20f3bd7068c7a/ (Дата обращения: 22.02.2018).
82. Минкомсвязи предложило снизить объём хранения данных по «закону Яровой» в 10 раз [Электронный ресурс] // Интерфакс, 2017. URL: http://www.interfax.ru/russia/546085/ (Дата обращения: 22.02.2018).
83. Мы не скрываем от вас, какую информацию собираем и как ее используем [Электронный ресурс] // Google. URL: https://privacy.google.com/intl/ru/your-data.html/ (Дата обращения: 22.02.2018).
84. Найти любовь станет проще: названы лучшие приложения для онлайн-знакомств [Электронный ресурс] // Роскачество, 2018. URL: https://roskachestvo.gov.ru/news/nayti-lyubov-stanet-proshche-nazvany-luchshie-prilozheniya-dlya-onlayn-znakomstv/ (Дата обращения: 22.02.2018).

85. Национальный сертификат безопасности Казахстана: Защита пользователей или государства? [Электронный ресурс] // Zakon.KZ, 2016. URL: https://www.zakon.kz/4772058-nacionalnyjj-sertifikat-bezopasnosti.html/ (Дата обращения: 22.02.2018).
86. Обама выступил против смартфонов, к которым нельзя получить доступ [Электронный ресурс] // ТАСС, 2016. URL: http://tass.ru/mezhdunarodnaya-panorama/2733318/ (Дата обращения: 22.02.2018).
87. Объем утечек конфиденциальной информации в мире в 2017 году вырос в 8 раз [Электронный ресурс] // РБК, 2017. URL: www.rbc.ru/technology_and_media/10/10/2017/59db57549a7947f8d8839ac3/ (Дата обращения: 22.02.2018).
88. ООН: судебная тяжба ФБР и Apple может иметь последствия для сферы прав человека в мире [Электронный ресурс] // ТАСС, 2016. URL: http://tass.ru/mezhdunarodnaya-panorama/2717275/ (Дата обращения: 22.02.2018).
89. Операторам выставили счет [Электронный ресурс] // Коммерсант, 2016. URL: https://www.kommersant.ru/doc/3181666/ (Дата обращения: 22.02.2018).
90. Очередной скандал с утечкой персональных данных сильно ударил по Facebook [Электронный ресурс] // Роскомсвобода, 2018. URL: https://roskomsvoboda.org/37210/ (Дата обращения: 29.03.2018).
91. Политика конфиденциальности [Электронный ресурс] // Компания Яндекс. URL: https://yandex.ru/legal/confidential/ (Дата обращения: 22.02.2018).
92. Постановление Конституционного Суда Российской Федерации от 31 марта 2011 г. N 3-П город Санкт-Петербург «по делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С.В. Капорина, И.В. Коршуна и других» [Электронный ресурс] // Российская газета, 2011. URL: https://rg.ru/2011/04/13/ks-grazhdane-dok.html (Дата обращения: 25.04.2018).

93. Приговор Новотроицкого городского суда Оренбургской области от 9 августа 2011 г. По делу № 1-304/11 [Электронный ресурс] // РосПравосудие, 2011. URL: https://rospravosudie.com/court-novotroickij-gorodskoj-sud-orenburgskaya-oblast-s/act-422970056/ (Дата обращения: 22.02.2018).
94. Приложением GetContact заинтересовался Роскомнадзор [Электронный ресурс] // Роскомсвобода, 2018. URL: https://roskomsvoboda.org/36763/ (Дата обращения: 29.03.2018).
95. Публичный Wi-Fi в Москве: безопасный или не очень? [Электронный ресурс] // Блог лаборатории Касперского, 2016. URL: https://www.kaspersky.ru/blog/moscow-wifi-insecure/12975/ (Дата обращения: 22.02.2018).
96. Референдум о расширении полномочий спецслужб поделил Нидерланды на два почти равных лагеря [Электронный ресурс] // Роскомсвобола, 2018. URL: https://roskomsvoboda.org/37292/ (Дата обращения: 24.03.2018).
97. Россия выступила за создание конвенции в сфере регулирования интернета под эгидой ООН [Электронный ресурс] // Роскомсвобода, 2018. URL: https://roskomsvoboda.org/37273/ (Дата обращения: 24.03.2018).
98. Россия стала второй после США по числу утечек конфиденциальных данных [Электронный ресурс] // РБК, 2017. URL: https://www.rbc.ru/technology_and_media/23/03/2017/58d2bbb39a794721422e1588/ (Дата обращения: 22.02.2018).
99. С миру по Wi-Fi-точке, или как преступники воруют данные прямо по воздуху [Электронный ресурс] // Блог лаборатории Касперского, 2016. URL: https://www.kaspersky.ru/blog/kaspersky-secure-connection/13119/ (Дата обращения: 22.02.2018).

100. Соглашение об использовании служб Microsoft [Электронный ресурс] // Компания Microsoft, 2018. URL: https://www.microsoft.com/ru-ru/servicesagreement/upcoming.aspx (Дата обращения 11.04.2018).
101. Статистика: активность в Telegram в России выросла после блокировки [Электронный ресурс] // vc.ru, 2018. URL: https://vc.ru/36598-statistika-aktivnost-v-telegram-v-rossii-vyrosla-posle-blokirovki/ (Дата обращения: 21.04.2018).
102. Суд ЕС счел незаконным хранение Интернет-провайдерами личных данных пользователей [Электронный ресурс] // ТАСС, 2016. URL: http://tass.ru/obschestvo/3893814/ (Дата обращения: 22.02.2018).
103. Суд разрешил Роскомнадзору заблокировать Telegram [Электронный ресурс] // vc.ru, 2018. URL: https://vc.ru/36280-sud-razreshil-roskomnadzoru-zablokirovat-telegram (Дата обращения: 15.04.2018).
104. Угон Телеграм на волнах паники [Электронный ресурс] // Хабрахабр, 2018. URL: https://habrahabr.ru/post/353948/ (Дата обращения: 21.04.2018).
105. ФСБ подсчитала «пакет Яровой» [Электронный ресурс] // РБК, 2017. URL: https://www.rbc.ru/newspaper/2017/04/14/58ef849a9a7947134a887f98/ (Дата обращения: 22.02.2018).
106. Что ждет биткоин. Япония призвала ужесточить регулирование криптовалют [Электронный ресурс] // РБК, 2018. URL: https://www.rbc.ru/crypto/news/5aa77c359a7947eb72c0f56c/ (Дата обращения: 30.04.2018).
107. Япония легализовала криптовалюты [Электронный ресурс] // N+1, 2017. URL: https://nplus1.ru/news/2017/05/13/legalize/ (Дата обращения: 30.04.2018).