УДК 342.738

ПРАВОВЫЕ АСПЕКТЫ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ХРАНЕНИЯ КЛЮЧЕЙ ШИФРОВАНИЯ НА СТОРОНЕ КЛИЕНТА

Хмель И.В.

к.филос.наук, доцент

ЧОУ ВО «Южный университет (ИУБИП)»

willhunter@yandex.ru

Аннотация: Статья посвящена проблеме регулирования хранений ключей шифрования на стороне клиента и защите конституционного права на тайну переписки.
Ключевые слова: кодирование сообщений, тайна переписки, организатор распространения информации в интернет

LEGAL ASPECTS OF GOVERNMENTAL REGULATION OF KEEPING THE ENCRYPTION KEYS ON THE CLIENT'S SIDE

Khmel' I.V.

Abstract: The article discusses the problem with control over the encryption keys on client's side and protection of constitutional rights for correspondence privacy
Keywords: end-to-end encryption, correspondence privacy, provider of the informational expansion in the internet

Актуальность темы обусловлена сложными процессами, происходящими в российском правовом пространстве, и привлекающим большое внимание как общественности, так и международных организаций, в том числе ООН.

В августе 2014 года в силу вступили поправки в закон от 27 июня 2006 г.№149 ФЗ «Об информации, информационных технологиях и о защите информации». В соответствии с этими поправками любой организатор распространения информации в интернет (ОРИ) должен предоставлять Роскомнадзору ряд сведений, которые будут включены в специальный реестр. По состоянию на 10 февраля 2019 года в реестре организаторов распространения информации в интернете значится 168 сервисов, в том числе и мессенджер Телеграм. [1]

Также мессенджеры обязаны идентифицировать своих пользователей и передавать в федеральные органы исполнительной власти информацию о применяемых методах кодирования сообщений, если их потребуется расшифровать (ключи шифрования). За неисполнения закона предусмотрены штрафы до 1 миллиона рублей. По тому же закону мессенджеры обязаны предоставлять услуги только тем пользователям, которые идентифицированы на основании абонентского номера и соответствующего договора.

При этом в заключении от 19.12.2017 №36553-СШ\Д26и «Об оценке регулирующего воздействия на проект постановления Правительства Российской Федерации «Об утверждении порядка идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями», которое было сделано Минэкономразвития России отмечено, что идентификации пользователей сети по номеру мобильного телефона не обеспечит в полном объеме достижение цели регулирования, так как, во первых, разовое подтверждение использования абонентского номера пользователем не позволит обеспечить контроль передачи сим-карты и\или мобильного устройства, на котором установлен СОМС, другому лицу. Во-вторых, существует целый ряд СОМС, которые не требует наличия абонентского номера от оператора связи (Googlt Talk, Skype, Confide, Ansa и др.). Некоторые виды СОМС могут быть установлены на переносном носителе (например, Miranda IM) и могут использоваться без привязки к сим-карте. Таким образом, заявленные требования лишь усложняют условия работы для СОМС и требуют дополнительных финансовых затрат, потому что теперь им придется заключать договор с сотовыми операторами. [2]

С 26.12.2017 вступило в силу постановление правительства РФ, которое требует хранить на территории РФ в течение года информацию о фактах приема, передачи, доставки, обработки сообщений (в том числе видео и звука) а так же о данных пользователей, участвующих в переписке. С 1 июля 2018 года, согласно №374-ФЗ и №375-ФЗ (так называемый «Пакет

Яровой») организаторы распространения информации должны будут хранить на территории России все передаваемые пользователями данные и предоставлять информацию по запросу спецслужб. С точки зрения авторов закона, он поможет в борьбе с экстремизмом [3].

В декабре 2017 года Telegram Messenger LLP подали иск в Верховный суд России о признании недействующим приказа службы от 19.082016 №432 об утверждении порядка представления организаторами распространения информации в интернете данных, необходимых для декодирования электронных сообщений пользователей сети, как противоречащий требованию закона о необходимости судебного решения для доступа к переписке граждан. С точки зрения юристов истца документ, описывающий порядок передачи ключей ФСБ, был издан на основании не действующего на тот момент «закона Яровой». К тому же, выполнение требований о дешифровке нарушит право на тайну переписки, охраняемое Конституцией. Тем не менее, ФСБ выиграло дело, заявив, что информация, необходимая для декодирования, не является охраняемой Конституцией. [4]

Можно предположить, что решение Верховного суда в споре с Телеграм и ФСБ распространяется на все интернет сервисы, которые попадают в сложную ситуацию, потому что предоставление данных пользователей ФСБ может нанести значительный репутационный ущерб (скандал с касперским). Мессенджер, не смотря не решение суда, отказался передавать ключи шифрования, что и привело к блокировке сервиса на территории Российской Федерации. При этом в Роскомнадзоре признают, что ключи от секретных чатов передать невозможно, но претензии вызывает сам отказ Телеграм идти на диалог с властью [5]. Сложность ситуации заключается в том, что даже в случае передачи ключей степень контроля мессенджера не вырастет, так как end to end шифрования (оконечное\сквозное) все равно останется, и ключи от него предать невозможно, так как шифрование происходит непосредственно на устройстве пользователя.

Переписка в обычных чатах хранится на серверах компании, но эти сервера расположены в разных юрисдикциях, и если сама компания не хочет отдать ключи, то даже по решению суда РФ получить эти данные будет невозможно. Это одна из причин, по которым Телеграмм считается одним из самых надежных мессенджеров, защищающих конституционные права пользователей.

После решения о блокировке РКН начал блокировать айпи адреса, но это не привело к ожидаемому эффекту, так как мессенджер просто стал менять эти адреса. Помимо того, что сам Телеграм начал использовать средства защиты от блокировок, к процессу активно подключились пользователи, которые начали массово устанавливать прокси и анонимайзеры.

Таким образом, на сегодняшний день, эффект от блокировок, оказался не совсем тем, на который рассчитывал Роскомнадзор.

- во-первых, подавляющая часть пользователей начала интенсивно использовать средства обхода блокировок.

- во-вторых, все пользователи приложения теперь вообще недостижимы для российских служб контроля, то есть ушли в тень.

- в-третьих, массовые блокировки адресов привели к некорректной работе ряда сайтов, в том числе и Сбербанка

- в-четвертых, так как никакой ответственности пользователей не предусмотрено, количество пользователей телеграмм не уменьшилось. Более того, продолжают работать каналы ряда официальных лиц, например Марии Захаровой.

- в-пятых, неудачные попытки перекрыть доступ к приложению работают против Роскомнадзора, потому что у России нет таких технических возможностей. Единственный вариант – строить Файервол по примеру Китая, в котором активная часть населения все равно пользуется средствами обхода блокировок.

- в шестых, это приводит к значительным репутационным издержкам для власти. Превращение нескольких миллионов россиян в бунтовщиков анонимов, которые гордятся тем, что помогают мессенджеру не выполнять требования закона – это серьезный удар по уважению к законам и власти на территории Российской Федерации [6].

Таким образом, на данный момент ключевой задачей представляется направление усилий не на попытки заблокировать Телеграм, а на улучшение репутации РКН и поиск приемлемого способа выйти из ситуации. По сути, мы наблюдаем столкновение формального закона – того, что древние римляне называли lex и божественного права, ius. На данный момент происходящее лишь усиливает правовой нигилизм, что очень негативно сказывается на развитии правосознания в России.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Реестр организаторов распространения информации в сети «Интернет» (Электронный ресурс). URL: http://rkn.gov.ru/opendata/7705846236-InformationDistributor/ (дата обращения 10.02.2109)
2. ЗОРВ на проект постановления Правительства Российской Федерации «Об утверждении порядка идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями» (Электронный ресурс). URL: http://orv.gov.ru/Content/Item?n=27608 (дата обращения 10.02.2109)
3. Гаспарян Г.А. Экстремистские проявления как угроза национальной безопасности Российской Федерации // Интеллектуальные ресурсы – региональному развитию. – 2015. – №5. – С. 69-72.
4. Верховный суд РФ признал законным приказ ФСБ о расшифровке сообщений в Telegram (Электронный ресурс) URL: https://tass.ru/obschestvo/5047772 (дата обращения 10.02.2109)
5. Telegram согласился передавать спецслужбам данные пользователей (Электронный ресурс) URL:

https://www.rbc.ru/technology_and_media/28/08/2018/5b8527749a7947318f857b0f (дата обращения 10.02.2109)

6. Асланян Р.Н. Влияние Интернета на становление гражданского общества // Интеллектуальные ресурсы – региональному развитию. – 2018. – №1. – С. 538-542.