

УДК 343.9

Возможен ли свободный обмен информацией в современном мире?

Петроченков Сергей Дмитриевич

Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, кафедра оперативно-розыскной деятельности, Рязань, Россия
старший преподаватель, кандидат юридических наук, sedm-09-07@yandex.ru

Богданов Александр Андреевич

Отдел Министерства внутренних дел по Вeneвскому району Тульской области, следственный отдел, г. Вeneв, Тульская область, Россия, следователь, aabogdanov94@mail.ru

Аннотация. На основе анализа отечественного и зарубежного законодательства рассматривается возможность свободно обмениваться информацией, используя современные информационно-коммуникационные технологии, а также проблема соблюдения прав и свобод граждан в условиях необходимости контроля информационного обмена.

Ключевые слова: обмен информацией, информационно-коммуникационные технологии, соблюдение прав и свобод, контроль информации.

Is the free information possible in the modern world?

Sergey Petrochenkov

The Ryazan branch of Moscow university of Ministry of internal affairs of Russia named for V.Y. Kikot, department of Investigative Activities, Ryazan', Russia, senior lecturer, candidate of legal sciences, sedm-09-07@yandex.ru

Aleksandr Bogdanov

Department of Ministry of Internal Affairs in the Venevskiy district of the Tula Region, investigation department, Venev, Tula Region, Russia, investigator, aabogdanov94@mail.ru

The summary. The authors analyse domestic and foreign legislation, consider the possibilities of free information exchange by means of modern information and communication technologies, and study a problems of respecting civil rights and freedoms under the conditions of the required control over information traffic.

Keywords: information exchange, information and communication technologies, respect of civil rights and freedoms, information traffic control.

Согласно ст. 29 Конституции РФ каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современный мир характеризуется непрерывным обменом информацией с использованием информационно-коммуникационных технологий, которые не только обеспечивают коммуникацию, но и предоставляют возможность злоумышленникам совершать преступления, связанные с распространением информации, а также договариваться о совместном совершении преступлений. Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление новых форм общественно опасного поведения личности – компьютерной преступности (computer crime) [1, с. 74].

В связи с этим субъектами оперативно-розыскной деятельности осуществляется негласный контроль информации, передаваемой с использованием современных средств связи. В этом случае те же информационно-коммуникационные технологии выступают в качестве средства осуществления оперативно-розыскной деятельности и элемента технико-криминалистического обеспечения расследования преступлений [2, 3].

В соответствии со ст. 14 федерального закона от 07.07.2003 г. № 126-ФЗ «О связи» все предприятия связи, действующие на территории РФ, независимо от ведомственной принадлежности и форм собственности при разработке, создании и эксплуатации сетей связи обязаны оказывать содействие органам, осуществляющим ОРД, и предоставлять им возможность проведения ОРМ на

сетях связи, принимать меры к недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий [4]. В ст. 15 Закона о ФСБ закреплено, что физические и юридические лица, предоставляющие в Российской Федерации услуги почтовой связи, электросвязи всех видов, в том числе систем телекодовой, конфиденциальной, спутниковой связи, обязаны по требованию органов ФСБ включать в состав аппаратных средств дополнительное оборудование и программные средства, а также создавать другие условия, необходимые для проведения оперативно-технических мероприятий органами ФСБ [5]. Таким образом, ФСБ является главной службой, контролирующей коммуникацию физических и юридических лиц в нашей стране, и имеющей, благодаря этому, большие возможности для выявления готовящихся или совершенных преступлений.

Большой общественный резонанс вызвало принятие в июле 2016 года законодательных нововведений, направленных на борьбу с терроризмом, известных как «Пакет Яровой». «Пакет» состоит из двух федеральных документов, один из которых вносит изменения в уголовный и уголовно-процессуальный кодексы Российской Федерации, другой – в федеральный закон «О противодействии терроризму» [6], ст. 13 которого вносит изменения в федеральный закон от 07.07.2003 № 126-ФЗ «О связи» и обязывает операторов связи (при поступлении запроса от оперативно-розыскного органа) прекращать оказание услуг связи в случае неподтверждения соответствия персональных данных фактических пользователей сведениям, заявленным в абонентских договорах. Также в соответствии со ст. 64 федерального закона «О связи» операторы связи обязаны хранить на территории Российской Федерации:

- 1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – *в течение трех лет* с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – *до шести месяцев* с момента окончания их приема, передачи, доставки и (или) обработки.

Также операторы связи обязаны *предоставлять* уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию.

«Пакет Яровой» вызвал протесты правозащитников, обоснованно заявивших о создании условий для тотальной слежки государственных правоохранительных органов за гражданами и нарушении их конституционных прав на неприкосновенность тайны телефонных переговоров и иных сообщений. Вместе с тем, похожая ситуация, связанная с контролем коммуникаций, сложилась в большинстве развитых стран мира. Закон обязывает операторов телекоммуникационных компаний хранить сведения, касающиеся телефонных переговоров и сообщений абонентов, предоставлять их в распоряжение правоохранительных органов (как правило, на основании судебного решения). Например, в Великобритании действует закон под названием «Data Retention and Investigatory Powers Act» (англ. – «Акт о полномочиях следствия»). Он обязывает операторов связи хранить запись сообщений и телефонных переговоров в течение *12 месяцев*, и в указанных в законе случаях предоставить полиции, органам безопасности и разведки.

Акт о полномочиях следствия указывает, что сохранение коммуникационных данных и возможность доступа к ним являются важным средством обеспечения правовой защиты, расследования преступлений и обеспечения национальной безопасности. Подчеркнуто, что в ряде случаев коммуникационные данные – единственный путь к выявлению правонарушителей, особенно тогда, когда правонарушения совершаются в режиме реального времени. В качестве примера приводятся такие

преступления, как использование рабского труда и мошенничество [7].

Однако, даже в таких условиях технически отследить содержание каждого разговора довольно проблематично. Для этого в нашей стране и за рубежом используется программа проверки переписки по ключевым словам, известная, как DPI (Deep Packet Inspection). Её функция заключается в накоплении статистических данных, проверке и фильтрации сетевых пакетов в зависимости от их содержимого.

Основные сотовые операторы России внедрили DPI в 2009 (Мегафон, оборудование Huawei), 2010 (МТС, Cisco) и 2011 (Билайн, Procera) годах. Система умеет отслеживать любой незашифрованный трафик пользователей - от электронной переписки и звонков до изображений и личных сообщений в соцсетях. Это позволяет использовать ее не только в целях безопасности. В частности, российская компания «iMarker» бесплатно устанавливает систему анализа трафика, собирает данные о поведении пользователей и продает их рекламодателям [8]. Указанная система и ее аналоги позволяют контролировать информацию, которая не была зашифрована пользователями.

Вместе с тем информация может передаваться и в зашифрованном виде, может устанавливаться анонимное сетевое соединение. Физические лица для этого используют так называемые «анонимайзеры», систему «ТОР», передают информацию в чатах компьютерных игр. Популярные мессенджеры также ведут обмен информацией между абонентами в зашифрованном виде. Широкую известность получили факты использования террористами мессенджера Telegram, а также отказ генерального директора Павла Дурова предоставить органам ФСБ ключи для дешифрования информации, в связи с чем, 13 апреля 2018 года Таганский районный суд города Москвы удовлетворил требования Роскомнадзора РФ и постановил ограничить на территории России доступ к его сервису [9]. В свою очередь Павел Дуров заявил о невозможности технически выполнить предъявленные требования по причине дешифровки информации только на конечном устройстве

пользователя. Несмотря на все принятые меры мессенджер Telegram продолжает функционировать и сейчас.

Таким образом, одни законодательные запреты не могут обеспечить информационную безопасность. Для контроля информации требуется принятие комплексных мер, включающих как законодательные нововведения, так и меры по техническому противодействию незаконным действиям в информационно-коммуникационной сфере.

В современном мире складывается неоднозначная ситуация: коммуникационные технологии изменяют мир, делая его более открытым. Вместе с тем, этот же фактор дает принципиально новые возможности для контроля за гражданами со стороны правоохранительных органов, создает условия для нарушения гарантированного Конституцией Российской Федерации права на тайну переписки, телефонных переговоров и иных сообщений, неприкосновенность частной жизни, личной и семейной тайны.

Для того, чтобы не допустить нарушения указных конституционных прав, информация, затрагивающая неприкосновенность частной жизни, должна охраняться в режиме соответствующей профессиональной тайны [10]. Другой важной составляющей законности является соблюдение строгой процедуры получения сведений о переговорах и иных сообщениях граждан. Соблюдение этих условий является правовой гарантией, не допускающей необоснованной слежки под видом получения оперативно значимой информации.

Анализ правовой регламентации информационно-коммуникационной сферы позволяет утверждать, что отечественное законодательство в этой области идет по пути повышения открытости информационного пространства при одновременном усилении контроля за телекоммуникационными системами со стороны государственных структур. По этой причине незначительный неконтролируемый обмен информацией посредством информационно-коммуникационных технологий в настоящее время еще

возможен, однако он будет постепенно сокращаться. В современном мире это неизбежно.

Список литературы

1. Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. – 2017. – № 8.
2. Вязовец Р.Н. Использование информационных технологий в оперативно-розыскной деятельности органов внутренних дел: дис. ...канд. юрид. наук. Москва, 2010. - 205 с.
3. Кравец Е.Г. Информационно-коммуникационные технологии как элемент технико-криминалистического обеспечения расследования преступлений: автореф. дис. ...канд. юрид. наук. Волгоград, 2016. - 23 с.
4. О связи: федеральный закон от 07.07.2003 № 126-ФЗ // СЗ РФ. 2003. № 28. Ст. 2895 (с послед. изм. и доп.).
5. О федеральной службе безопасности: федеральный закон от 03.04.1995 № 40-ФЗ // СЗ РФ, 10.04.1995, № 15, ст. 1269 (с послед. изм. и доп.).
6. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 06.07.2016 № 374-ФЗ // СЗ РФ, 2016, № 28, ст. 4558 (с послед. изм. и доп.)
7. GOV.UK. Investigatory Powers Act. URL: <https://www.gov.uk/government/collections/investigatory-powers-bill> (дата обращения 15.06.2018).
8. Сайт газеты «Ведомости». Большой рекламный брат. URL: <https://www.vedomosti.ru/newspaper/articles/2013/08/28/bolshoj-reklamnyj-brat> (дата обращения 28.01.2019).
9. Сайт газеты «РБК». Суд постановил немедленно заблокировать Telegram в России. URL: https://www.rbc.ru/technology_and_media (дата обращения 09.06.2018).
10. Саванович Н.А. Личная информация граждан [Электронный ресурс] // Консультант Плюс. Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016.

References

1. Russkevich, E.A. (2017). Ugolovnoe pravo i informatizatsiya [Criminal law and information], *Zhurnal rossiyskogo prava*, (8).
2. Vyazovets, R.N. (2010). *Ispol'zovanie informatsionnykh tekhnologiy v operativno-rozysknoy deyatelnosti organov vnutrennikh del* [The use of information technology in operational investigative activities of internal Affairs], Moscow.
3. Kravets, E.G. (2016). *Informatsionno-kommunikatsionnye tekhnologii kak element tekhniko-kriminalisticheskogo obespecheniya rassledovaniya prestupleniy* [Information and communication technologies as an element of technical and forensic support of crime investigation] Volgograd.
4. O svyazi: federal'nyy zakon ot 07.07.2003 № 126-FZ [About the connection: the Federal law of 07.07.2003 № 126-FZ], (2003). *SZ RF*, (28), p. 2895
5. O federal'noy sluzhbe bezopasnosti: federal'nyy zakon ot 03.04.1995 № 40-FZ [About Federal security service: the Federal law of 03.04.1995 No. 40-FZ], *SZ RF*, (10.04.1995), (15), p. 1269.
6. O vnesenii izmeneniy v Federal'nyy zakon «O protivodeystvii terrorizmu» i otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeystviya terrorizmu i obespecheniya obshchestvennoy bezopasnosti: federal'nyy zakon ot 06.07.2016 № 374-FZ [About modification of the Federal law "On counteraction to terrorism" and separate legal acts of the Russian Federation regarding establishment of additional measures of counteraction to terrorism and ensuring public safety: the Federal law of 06.07.2016 No. 374-FZ] (2016). *SZ RF*, (28), p. 4558.
7. GOV.UK. Investigatory Powers Act. Retrieved from <https://www.gov.uk/government/collections/investigatory-powers-bill>.
8. *Vedomosti*. Bol'shoy reklamnyy brat [Big advertising brother] Retrieved from <https://www.vedomosti.ru/newspaper/articles/2013/08/28/bolshoj-reklamnyj-brat>.
9. *RBC*. Sud postanovil nemedlenno zablokirovat' Telegram v Rossii. [The court decided to block Telegram in Russia immediately]. Retrieved from https://www.rbc.ru/technology_and_media.
10. Savanovich, N.A. (2016). Lichnaya informatsiya grazhdan [Personal information of citizens] Konsul'tant Plyus. Belarus', Tekhnologiya 3000, OOO «YurSpektr», Nats. tsentr pravovoy inform. Resp. Belarus', Minsk.