ТАЙНА «ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ» В УГОЛОВНОМ ПРОЦЕССЕ РОССИИ, США, КИТАЯ И ГЕРМАНИИ

Черкасов В.С.
Владивостокский филиал Дальневосточного юридического института МВД России, г. Владивосток
email: viktor.kmsx@gmail.com

Аннотация. Современное оконечное оборудование (смартфоны, планшеты, ноутбуки и т.д.) содержат огромное количество информации, попадающей под различные режимы тайн. В статье рассмотрены юридические гарантии защиты тайн при производстве следственных действий в отношении изъятого электронного устройства в таких странах как США, Китай, Германия.

Ключевые слова: информационные технологии, уголовный процесс, следственные действия, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, зарубежные страны, телефон, социальные сети, электронные сообщения.

Человек доверяет информационным технологиям огромный массив личных данных: банковские транзакции, пароли, электронные сообщения, социальные сети, дистанционное управление домом и автомобилем, а также множество иной информации, попадающей под действия режима различных тайн. Современные информационные технологии значительно изменили повседневную жизнь человека.

Однако возникает вопрос, насколько защищены с юридической точки зрения личные данные человека, в особенности при уголовном преследовании?

Как указывает В.Ф. Васюков, в Российской Федерации действует следующее правило: «Правоотношения, регулируемые федеральными законами, касаются только принципов сохранения в тайне данных, которые были доверены гражданином только определенной организации или должностному лицу. Если информация выбыла из сферы ответственности организации (должностного лица) путем фиксации ее в памяти мобильного компьютерного устройства, она как таковая уже не подлежит защите с помощью судебного контроля» [1, с. 67].

Данное правило полностью согласуется с позицией Конституционного Суда РФ, который в Определении от 25 января 2018 г. № 189-О указал, что «проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения» [5].

В 2016 г. принят Федеральный закон № 375-ФЗ [7], которым в ст. 185 УПК РФ была введена ч. 7, согласно которой «при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных, передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка». Однако данное следственное действие, как подчеркивает В.Ф. Васюков» [1, с. 65], относится к получению электронных сообщений из учреждений связи, что фактически законодательно исключает судебный контроль над получением сведений с электронных носителей информации посредством следственного осмотра и производства экспертизы.

Исходя из изложенного, изъяв любое оконечное оборудование (телефон, ноутбук, планшет и т.д.), следователь получает неограниченный доступ ко всей информации, которая храниться не только в памяти устройства, но и электронно-информационном сервисе («ICloud», «Telegram», «Вконтакте», «Instagram» и т.д.).

При этом судебного разрешение на производство следственных действий в отношении оконечного оборудования получать не нужно [3, 7].

Как обстоит дело с юридическими гарантиями на неприкосновенность частной жизни, в условиях существования современных информационных технологий, при уголовном преследовании в зарубежных странах?

В ряде иностранных государств для исследования информации, содержащейся на электронном носителе, введен ведомственный и судебный контроль.

Уголовно-процессуальное законодательство Китайской Народной Республики не содержит специальных ограничений, связанных с исследованием со стороны правоохранительных органов оконечного оборудования. Несмотря на это существует ведомственный процессуальный контроль со стороны вышестоящего органа. Так, при необходимости производства процессуальных действий сотрудником полиции уровня провинции необходимо получить разрешения от органа уездного уровня. В своею очередь сотруднику полиции уровня уезда достаточно получить разрешение руководителя[1].

Необходимо обратить внимание на «Положение о процедуре осуществления осмотра места преступления, совершенного с применением средств информационно-цифровых технологий и проверки электронных доказательств», разработанное Министерством общественной безопасности Китая в 2005 году [9]. Согласно п. 18 данного положения, на месте происшествия допустимо производить онлай-анализ подразумевающий прямой анализ и сбор информационных данных, производимый в условиях использования электронных систем во включенном состоянии на месте совершения противоправных действий. Как правило, использование процедуры онлайн-анализа может осуществляться только в указанных ниже случаях:

1. экстренные случаи, при которых отказ от применения онлайн-анализа приведет к тяжелым последствиям;
2. особые случаи, при которых отключение электронного оборудования и его изъятие является невозможным.

Исходя из рассмотренных правил, исследования электронного носителя информации при осмотре места происшествия в Китае возможно только в особых случаях.

Согласно уголовно-процессуального кодекса Германии, электронные носители информации подлежат выемке и дальнейшему исследованию по судебному решению, если изъятие необходимо произвести в случаях, не терпящих отлагательств, то сотрудник правоохранительного органа обязан подтвердить производство выемки в суде в течение трех дней [2, с. 54-55].

Любопытно, что в уголовно-процессуальном кодексе Германии [6] режим свидетельского иммунитета распространяется на электронные сообщения, доступ к которым можно получить через электронный носитель информации. Как указывает П.В. Головненков: «Согласно § 97 (абз. 1 № 1) УПК ФРГ не подлежит выемке переписка между обвиняемым и лицами, которые имеют право отказаться от дачи показаний на основании §§ 52, 53 (абз. 1 предл. 1 № 1-3b), 53a УПК ФРГ (супруг/супруга, помолвленный/-ая, лица, состоящие с обвиняемым в родстве или свойстве, священнослужители, защитники, адвокаты, налоговые консультанты, врачи, сотрудники признанных государством консультаций и т.д., а также их профессиональные помощники). Запрет на выемку распространяется согласно § 97 (абз. 1 № 2) УПК ФРГ также на записи, которые лица, перечисленные в §§ 53 (абз. 1 предл.1 № 1-3b), 53a УПК ФРГ, сделали о сообщениях, доверенных им обвиняемым,

[1] На указанный порядок указал заместитель начальника факультета безопасности информации и сети милиции общественной безопасности Хэйлунцзянского института профессиональной подготовки офицеров МОБ КНР, Ли Вэньцзян в рамках проведенных 10-12 апреля 2018 в ДВЮИ МВД России лекционных занятий гостями из Хэйлунцзянского института МОБ КНР.

или о других обстоятельствах, на которые распространяется право на отказ от дачи показаний» [2, с. 54].

В США нарушение прав на неприкосновенность частной жизни устанавливается специальными стандартами, выработанными судебной практикой.

Как указывает Р.И. Оконенко: «В настоящее время компьютер приравнивается судьями к закрытому контейнеру, поэтому для его исследования необходимо получить судебную санкцию. При обыске обычного помещения действия ограничиваются предметом поиска, однако так как природа компьютерной информации неочевидна и относительна, а интересующие правоохранительные органы сведения могут находиться в любом месте и виде, суды стали признавать право полиции на открытие любого файла для осмотра его содержания [4, с. 78] … Указанный подход был применен в деле «United States vs Finely» (2007). Практически аналогичную позицию занял Верховный суд США» [11].

На основании изложенного допустимо сделать вывод, что исследование содержания компьютерной информации, находящейся на электронных носителях, в США происходит в режиме обыска и только по судебному разрешению. При этом, исходя из работы Р.И. Оконенко, орден на обыск в жилище, также распространяется и на электронную информацию [4, с. 68].

Важным аспектом, раскрытым в диссертации Р.И. Оконенко, является вопрос об исследовании электронных носителей информации, изъятых в ходе правомерного ареста, когда для производства личного обыска нет необходимости получать судебное разрешение.

Так, продолжительное время судебные органы США сравнивали электронный носитель информации с закрытым контейнером (к примеру, с пачкой сигарет), который допустимо исследовать при личном обыске без судебного разрешения, исходя из правомерного ареста [12]. Как указывает Р.И. Оконенко: «25 июня 2014 года Верховный суд США принял революционное решение для института обыска при аресте решение по делу «Riley versus California» [10] … Суд посчитал неправомерным обыск сотового телефона при аресте без получения дополнительного судебного ордена по правилам уголовного судопроизводства [4, с. 113].

Рассмотрим подробнее аргументы, которыми руководствовался Верховный суд США при принятии данного решения.

Судом был указано, что не всякий обыск может быть признан правомерным только потому, что проведен в рамках правомерного ареста, так как объект поиска может быть настолько большим и информативным, что его обследование выходит за рамки тех полномочий, которые предоставляются полиции в связи с арестом. Судом было отвергнута позиция представителя Соединенных Штатов, согласно которой поиск информации на мобильном телефоне фактически не различим с поиском физических объектов [4, с. 113].

Опровержение позиции суд мотивировал существенным отличием в свойствах электронных носителей информации и обычных физических объектов: во-первых, цифровые устройства несравнимы с физическими объектами по объему и видам информации, которые могут в них содержаться. Во-вторых, существенное отличие связано с термином «содержать в себе». Если относительно физического объекта всегда можно сказать, что в нем хранится, то с мобильными телефонами дело обстоит несколько сложнее. Рассуждая в этом ключе, суд привел технологии типа «ICloud», позволяющие отображать на экране телефона ту информации, которая не хранится у него в памяти [4, с. 113].

Следующим важным вопросом, который рассмотрел Верховный суд США, является возможность уничтожения или сокрытия доказательств. Суд указал, что, во-первых, отсутствие физического контроля владельца над мобильным телефоном

до получения соответствующего ордера вполне может предотвратить возможность уничтожения данных. Во-вторых, проблема удаленного доступа к мобильному телефону может быть решена с помощью простых и дешевых технологий (к примеру, «сумок Фарадея»), которые блокируют внешние сигналы, поступающие на телефон. В-третьих, уничтожение информации с помощью удаленного доступа производится третьими лицами, а не самим арестованным [4, с. 111-112].

Таким образом, уголовный процесс США значительно продвинулся в развитии правоотношений, регулирующих сбор доказательств, выраженных в электронной форме с учетом баланса между потребностями правоохранительных органов и прав и свобод человека и гражданина.

В целом, допустимо утверждать, что законодательство ряда государств уже учитывает особенности существования электронной информации, что объясняет появлением ведомственного и судебного контроля при собирании доказательств выраженных в электронной форме. Представляется верным вектор развития уголовно-процессуального права России, где будут созданы нормы, обеспечивающие юридические гарантии защиты конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений в форме судебного контроля при производстве следственных действий в отношении электронных носителей информации.

Библиографический список

1. Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. – 2016. – № 10. – С. 64-67.

2. Головненков П.В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия. Научно-практический комментарий и перевод текста закона. М., 2-е изд. 2014. - 314 с.

3. Кузнецова С.М. Реализация конституционного права на тайну переписки, телефонных переговоров и иных сообщений при осмотре сотового телефона в ходе производства по уголовному делу // Вестник Дальневосточного юридического института МВД России. – 2018. – № 2. – С. 39-43.

4. Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту таны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской федерации: дисс. … кан. юрид. наук. Москва. 2016. - 158 с.

5. Определение Конституционного суда РФ от 25 января 2018 г. № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс] // Доступ из СПС «Консультант плюс».

6. Уголовно-процессуальный кодекс Федеральной Республики Германии от 12.09.1950 года [Электронный ресурс] // Официальный сайт публикации документа режим доступа: http://www.gesetze-im-internet.de/englisch_stpo/index.html

7. Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // «Российская газета». – 2016. 11 июля.

8. Черкасов В.С. Проблемы регулирования режима компьютерной информации в уголовном досудебном производстве // Вестник Дальневосточного юридического института МВД России. – 2017. – № 2. – С. 40-46;

9. 计算机犯罪现场勘验与电子证据检查规则 (公信安[2005]161号 公安部) / «Положение о процедуре осуществления осмотра места преступления,

совершенного с применением средств информационно-цифровых технологий и проверки электронных доказательств» МОБ КНР 2005 [Электронный ресурс] // режим доступа: http: //www. 360doc.com /content/ 17/1121/23/ 44284862_706004600.shtml.

10. Riley v. California. 573 U.S. (2014).

11. United States v. Finely. 477 F.3d 250. 5 th Cir. (2007).

12. Ward K.B. The plain (or not so plain) view doctrine: applying the plain view doctrine to digital seizures // University of Cincinnati Law Review. – Vol. – 79. Iss. 3. – Art. 6. – 2011.

THE SECRET OF "ELECTRONIC COMMUNICATIONS" IN THE CRIMINAL PROCEEDIN LAW OF RUSSIA, THE UNITED STATES, CHINA AND GERMANY

Cherkasov V.S.
Vladivostok branch Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, Vladivostok
email: viktor.kmsx@gmail.com

Abstract. Modern terminal equipment (smartphones, tablets, laptops, etc.) contain a huge amount of information that falls under various mystery modes. The article deals with legal guarantees of protection of secrets in the course of investigative actions in relation to the seized electronic device in such countries as the United States, China, and Germany.

Keywords: information technologies, criminal procedure, investigative actions, secrecy of correspondence, telephone conversations, postal, Telegraph and other messages, foreign countries, telephone, social networks, electronic messages.