УДК 343.1 Вестник СПбГУ. Право. 2021. Т. 12. Вып. 1

Получение электронной информации по уголовным делам в рамках международного сотрудничества

К. К. Клевцов[1], *В. Ф. Васюков*[1,2]

[1] Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Российская Федерация, 119454, Москва, пр. Вернадского, 76

[2] Орловский юридический институт им. В. В. Лукьянова Министерства внутренних дел Российской Федерации, Российская Федерация, 302025, Орел, ул. Игнатова, 2

Для цитирования: Клевцов, Кирилл К., Виталий Ф. Васюков. 2021. «Получение электронной информации по уголовным делам в рамках международного сотрудничества». *Вестник Санкт-Петербургского университета. Право* 1: 36–51. https://doi.org/10.21638/spbu14.2021.103

Взрывной рост информационно-коммуникационных технологий, затронувший институты социальной коммуникации человека, стал соизмерим с повышением потенциальных рисков для безопасности и прав граждан. В статье анализируются вопросы международного сотрудничества правоохранительных органов Российской Федерации и других стран в рамках получения электронной информации, имеющей значение для доказывания по уголовным делам. Освещаются процедуры по обеспечению сбора и использования электронных данных при противодействии преступности в условиях тонкой грани конфиденциальности личной информации и безопасности государства. Несмотря на соглашения, подписанные многими странами, практическая реализация нормативных актов, обеспечивающих предоставление электронной информации в рамках международного сотрудничества, в настоящее время сопровождается определенными проблемами. Между тем в условиях противодействия таким опасным для мирового сообщества явлениям, как терроризм, экстремизм, торговля наркотиками, оружием, людьми, до сих пор не выработано единого механизма обмена информацией, сохраняемой в гигантских масштабах на серверах операторов связи и провайдеров. Фактический поиск данных, хранящихся на мобильных устройствах, обычно требует ордера в странах общего права. В ситуации, когда существует значительный риск потери доказательств (например, когда активно используется детекция данных и другие инструменты компьютерной экспертизы), некоторые юрисдикции позволяют правоохранительным органам осуществлять ограниченный поиск устройств без ордера из-за предполагаемой уязвимости данных. Еще одна проблема связана с сохранением хранимых данных, поскольку в разных странах применяются разные практики. Поэтому крайне важно, чтобы следователи и прокуроры были хорошо информированы о геоспецифических вопросах картографирования данных, включая эмбарго или запреты на обмен компьютерной информацией.

Ключевые слова: международное сотрудничество, международный договор, процессуальные действия, следственные действия, компьютерная информация, правовая помощь, электронные доказательства, уголовное судопроизводство, электронные сообщения, абонентская информация, компетентные органы.

1. Введение

В XXI в., особенно в последнее время, наметилась тенденция перманентного проникновения информационных технологий в сферу социальной жизни, а также переход в так называемую цифровую реальность (Шестак, Волеводз 2019), что имеет положительный характер. Однако результаты научно-технической революции используются не только в благих, но и в преступных целях. Зачастую преступления совершаются в киберпространстве (Broadhurst et al. 2014; Collin 1997) и при апробации достижений электронной промышленности, например при использовании криптовалюты (Cox 2016; Foley, Karlsen, Putnins 2018), различных мессенджеров (WhatsApp, Telegram, Wickr Me и т. д.), электронных платежных сервисов (Qiwi, WebMoney, Payoneer и др.) (Leukfeldt 2015).

Очевидно, что все это требует от правоохранительных органов разработки соответствующих концептуальных методов борьбы с такой преступностью и алгоритмизации действий по сбору необходимой информации в целях предупреждения, пресечения, раскрытия и расследования подобных общественно опасных деяний.

Не менее важно, что при совершении указанных выше преступлений злоумышленники в большинстве случаев используют удаленные серверы, как правило расположенные за рубежом, вследствие чего властям России крайне трудно получить сведения о переписке уголовно преследуемых лиц в информационно-коммуникационной сети Интернет (Lievens 2014) и об их безналичных, электронных переводах, особенно с использованием криптовалюты (Волеводз 2018), не прибегнув к помощи государства, где располагается провайдер либо оператор связи. В этом случае главенствующую роль занимает такое сложное, многоступенчатое и многообразное правовое явление, как международное сотрудничество государств в сфере борьбы с преступностью. Как известно, взаимодействие государств может осуществляться и в рамках международных договоров, и при отсутствии таковых — на основании принципа взаимности (международной вежливости) (Щерба 2016).

Впрочем, в зависимости от конкретных целей и обстоятельств сношения компетентных органов иностранных государств следует различать *сотрудничество в сфере уголовной юстиции* (criminal justice cooperation), как правило используемое в целях формирования доказательств в уголовном процессе посредством межгосударственных договоров об оказании правовой помощи или предназначенных для борьбы с конкретными видами преступлений[1], и *международное полицейское сотрудничество* (law enforcement, police-to police cooperation (enquiries)), которое задействуется в целях получения оперативной информации и в рамках межправительственных и межведомственных договоров (Литвишко 2015).

В рассматриваемом контексте уместно упомянуть Конвенцию о киберпреступности, подписанную 23.11.2001 в г. Будапеште[2]. Однако для Российской Федерации данный международный документ не имеет юридической силы, поскольку Россия

[1] Например, Конвенция ООН против коррупции от 31.10.2003 (United Nations Convention against corruption 31.10.2003). Дата обращения 1 января, 2020. https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.

[2] Convention on Cybercrime 23.11.2001. Дата обращения 1 января, 2020. https://rm.coe.int/1680081561.

отказалась предоставлять трансграничный доступ к компьютерным данным на своей территории[3]. При этом стоит учитывать интересные определения понятий, связанных с компьютерными преступлениями, в пояснительном докладе к Конвенции[4]. В частности, аналогичными соображениями законодатель руководствовался при принятии Федерального закона от 06.06.2019 № 120-ФЗ «О ратификации Второго дополнительного протокола к Европейской конвенции о взаимной правовой помощи по уголовным делам», оставив за Россией право не принимать положения ст. 16, 17 и 19 данного протокола.

Однако это не означает, что наша страна не имеет международно-правовой платформы для борьбы с транснациональными организованными преступлениями, совершаемыми с использованием компьютеров, телекоммуникационных сетей и других современных технологий. Упомянем также Конвенцию ООН против транснациональной организованной преступности от 12.12.2006[5], предусматривающую большой объем правовой помощи в данной сфере, а также другие договоры об оказании правовой помощи при расследовании уголовных дел о преступлениях, которые охватываются указанной выше Конвенцией о киберпреступности. В подобных договорах отсутствуют прямые формулировки, касающиеся возможности получения электронных доказательств. Поэтому если иностранным партнерам необходимо получить информацию, имеющуюся в распоряжении российских поставщиков услуг связи по находящемуся у них в производстве уголовному делу, то им необходимо либо направить компетентным органам Российской Федерации соответствующий запрос о правовой помощи в рамках межгосударственного договора об оказании правовой помощи по уголовным делам или на основании принципа взаимности, либо подготовить запрос о содействии, адресованный напрямую органам, правомочным осуществлять оперативно-разыскную деятельность на основании межправительственных или межведомственных договоров, либо воспользоваться так называемым связующим звеном — Интерполом.

Напомним, что у российских правоохранительных органов возникают серьезные трудности при получении необходимых сведений от иностранных коллег в силу отсутствия внутригосударственного регулирования данного вопроса и существенного различия законодательства России и зарубежных суверенов в указанной сфере, что, в свою очередь, приводит к путанице в правоприменительной практике при определении конкретного алгоритма действий в целях получения электронных доказательств. Все это негативно сказывается на результате и наносит процессуальный ущерб раскрытию и расследованию конкретных преступлений.

Итак, рассмотрим получение электронной информации в рамках международного сотрудничества на примере конкретных государств, с тем чтобы попытаться оптимизировать данный проблемный правовой участок.

---

[3] Распоряжение Президента РФ от 22.03.2008 № 144-рп «О признании утратившим силу распоряжения Президента РФ от 15.11.2005 № 557-рп "О подписании Конвенции о киберпреступности"». Здесь и далее все ссылки на российские нормативно-правовые акты приводятся по СПС «КонсультантПлюс». Дата обращения 1 января, 2020. http://www.consultant.ru.

[4] Explantory Report to the Convention on Cybercrime. Дата обращения 1 января, 2020. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.

[5] United Nations Convention against Transnational Organized Crime. 12.12.2006. Дата обращения 1 января, 2020. https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

2. Основное исследование

Главный правовой инструмент обмена электронными доказательствами в международном измерении — Конвенция о киберпреступности[6]. Настоящий документ является результатом усилий, направленных на решение проблемы киберпреступности членами Совета Европы (СЕ), Интерпола, Европола, Организации экономического сотрудничества и развития, Содружества и Организации Объединенных Наций (ООН).

Конвенция о киберпреступности вступила в силу в июле 2004 г. Документ ратифицировали 43 из 47 членов (до августа 2018 г.) Совета Европы (Сан-Марино, Ирландия, Россия и Швеция еще не ратифицировали его) и Аргентина, Австралия, Кабо-Верде, Канада, Чили, Коста-Рика, Доминиканская Республика, Израиль, Япония, Маврикий, Марокко, Панама, Парагвай, Филиппины, Сенегал, Шри-Ланка, Тонго и Соединенные Штаты Америки. Помимо вопросов киберпреступности, указанная Конвенция рассматривает процедуры, касающиеся сбора доказательств в электронной форме (the collection of evidence in electronic form) по любой категории преступлений, когда такие электронные доказательства могут иметь значение для уголовного дела.

Таким образом, Конвенция о киберпреступности представляет собой первый и наиболее важный многосторонний императивный документ, провозглашающий международные стандарты получения и передачи компьютерной информации. Реализация Конвенции основана на существовании соглашения о взаимной правовой помощи между подписавшими сторонами, которая зависит от такой более детальной спецификации инструментов, предоставляемых в рамках Конвенции, которая известна как «направление запроса».

Для решения этой проблемы Комитет по Конвенции о киберпреступности (Cybercrime Convention Committee) опубликовал в марте 2017 г. документ под названием «Руководство применения ст. 18 Конвенции о порядке направления запроса для получения абонентской информации»[7] (далее — Руководство).

Вскоре после принятия Руководства при правоприменении возникли проблемы толкования ст. (18) (1) (b) Конвенции. Основная проблема касалась ст. 1 (3) Конвенции, где оператор связи (поставщик услуг) определяется как (i) любое государственное или частное лицо, которое предоставляет пользователям своих услуг возможность общаться с использованием компьютерной системы, и (ii) любое другое лицо, которое обрабатывает или хранит компьютерные данные от имени такой службы связи или пользователей такой службы.

Статья 18 (1) Конвенции определяет порядок направления запроса в целях получения электронной информации правоохранительными органами у иностранных операторов связи. Однако в положениях Конвенции отсутствует указание на то, хранится ли требуемая информация об абоненте на территории или за преде-

[6] European Parliament and Council of the European Union, Directive 2014/41/EU of European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. 2014. Дата обращения 1 января, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041.

[7] Cybercrime Convention Committee (T-CY), T-CY Guidance Note No. 10 Production orders for subscriber information (Article 18 Budapest Convention), revised version as adopted by the T-CY following 16 Plenary by written procedure. 2017. Дата обращения 1 января, 2020. https://rm.coe.int/16806f943e.

лами территории запрашивающего государства. Кроме того, не приводятся виды электронной информации, подлежащей поиску, ее потенциальное местоположение. Это усугубляется еще и тем, что Руководство не дает необходимого толкования процедуры получения данной информации, поскольку взаимное согласие сотрудничающих государств относительно оформляемых документов не позволяет классифицировать его как согласие на экстерриториальное исполнение внутренних производственных запросов для сбора электронных доказательств.

Запрос правомерен только в тех случаях, когда направляется к иностранным операторам связи, хранящим данные на территории иностранного государства. Кроме того, эта процедура не может осуществляться уполномоченными органами на территории другого суверена.

Расширение сферы применения ст. 18 Конвенции, предлагаемое в Руководстве, существенным образом нарушает принципы территориальности и суверенитета, связанные с защитой основных прав и верховенством права. В документе не уточняется, какие сведения являются абонентской информацией, несмотря на то что перечень таких сведений имеет огромное значение для оценки влияния конфиденциальности данных при формировании запросов, направленных в соответствии со ст. 18 (1) (b) Конвенции.

К тому же одним из пробелов Руководства является отсутствие разъяснения термина «динамический IP-адрес», а также разъяснений того, могут ли эти данные рассматриваться в качестве запрашиваемой абонентской информации, или же они подпадают под категорию «данные о трафике» и, следовательно, выходят за рамки ст. 18 Конвенции.

Отсутствие последовательных определений различных типов данных в Руководстве может также привести к коллизии правовых норм в отношении сферы охвата предусмотренных мер, к недоразумениям между запрашивающим органом и органом-исполнителем или оператором связи, к которому обратились правоохранительные органы с запросом.

Во многих государствах имеется национальное законодательство, направленное на защиту конфиденциальной информации, в частности о семейной и частной жизни лица.

Как отмечается в юридической литературе, в США выделяют три вида хранимой и доступной информации:

— базовая информация абонента (Basic Subscriber Information) — сведения, которые описывают, кем является абонент (имя и адрес), и включают в себя простую информацию об использовании пользователем онлайн-службы в конкретную дату и время (время входа в учетную запись и количество времени, в которое абонент пользовался этим сервисом); в этом случае необходимо лишь связать имя пользователя с преступлением; при направлении запроса указываются адрес (например, электронной почты или IP-адрес либо URL веб-страницы), имя пользователя, если имеется такая возможность, дата и время;
— информация о транзакциях (Transactional Information), которые представляют собой записи, идентифицирующие, с кем был связан пользователь, какие сайты он посетил, и онлайн-активность; чтобы получить такую информацию, необходимо представить суду справку о расследовании и обос-

новать необходимость получения сведений; такое требование вытекает из положения разд. 2703 (d) Закона США от 1986 г. «О защите информации, передаваемой при помощи электронных систем связи»[8];

— содержание (Content), подразумевающее под собой сведения, отправленные по электронной почте отправителем получателю, которые могут включать сообщения, фото и аудиозапись, прикрепленные к переписке; сюда следует отнести информацию и файлы, передаваемые посредством электронной почты (G-mail, Yahoo), социальных сетей (Facebook, Twitter) или мессенджеров (Snapchat, WhatsApp, Telegram); однако стоит иметь в виду, что такие операторы, как Snapchat и WhatsApp, не сохраняют содержание сообщений, поэтому получить необходимую переписку можно только при изъятии самого устройства, на котором установлена соответствующая программа (Малов 2018).

Для того чтобы направить подобный запрос, российские правоохранительные органы должны через круглосуточную сеть оповестить интернет-провайдеров о необходимости сохранить сообщения, передаваемые посредством электронной связи. В США провайдеры по общему правилу сохраняют такие данные до 90 дней, однако при необходимости указанное время может быть продлено.

При направлении запроса об оказании правовой помощи, адресованного компетентным органам США (Министерству юстиции), необходимо указать, что (1) запрос является официальным документом о предоставлении электронных доказательств от интернет-провайдера (или других компаний, таких как хостинговая) в США, включая соответствующий адрес; (2) правоохранительные органы России предприняли необходимые шаги для сохранения данных; также указываются дата подачи запроса о сохранении и имеющиеся номера ссылок, которые могли быть переданы в процессе сохранения; (3) запрос проверен Центральным компетентным органом России на предмет удовлетворения требований договора об оказании правовой помощи по уголовным делам и норм национального законодательства США; кроме того, требуется (4) сформулировать достаточность фактической информации для установления оснований считать, что в России присутствует преступная деятельность, и установить причинно-следственную связь между противоправными действиями и электронным данными, находящимися под юрисдикцией США. Если же нужно само содержание электронного сообщения, то судебный ордер может быть получен только при наличии вероятных оснований — высшей нормы доказательства, демонстрируемой более конкретными фактическими деталями и необходимой мотивировкой таких деталей. В противном случае запрос будет возвращен для предоставления дополнительной информации, что негативно отразится на сроках раскрытия и расследования преступлений.

Также упомянем Краткое руководство по получению взаимной правовой помощи от США, подготовленное отделом по международным делам Управления по уголовным делам Министерства юстиции США[9], которое более подробно описывает порядок действий при определении конкретного вида запрашиваемой помощи

[8] Electronic Communications Privacy Act of 1986 — ECPA. Дата обращения 1 января, 2020. https://www.justice.gov/jmd/electronic-communications-privacy-act-1986-pl-99-508.

[9] Brief Guide to Obtaining Mutual Legal Assistance from the United States. Office of Internat. Affairs, Criminal Div., U.S. Dept. of Justice, 3/8/2011. Дата обращения 1 января, 2020. https://www.justice.gov.

в рассматриваемой нами сфере. Так, по указанному документу можно: 1) запросить сохранение хранимых данных; 2) получить журналы подключений, информации об абоненте и содержания более старых хранимых сообщений электронной почты от поставщиков услуг Интернета; 3) исполнить ордер на получение содержания новых хранимых сообщений электронной почты от поставщиков услуг Интернета; 4) перехватить телекоммуникации или компьютерные данные в реальном времени. Рассмотрим подробнее каждый из видов запрашиваемых действий.

1. Сохранение хранимых данных. Напомним, что, если правоохранительные органы России собираются направить в США запрос о разглашении хранимых компьютерных данных, во многих случаях рекомендуется прежде всего истребовать, чтобы данные сохранялись до исполнения запроса об их разглашении. Это обусловлено тем, что, в отличие от российского законодательства, поставщики интернет-услуг в США по общему правилу не обязаны хранить данные для последующего использования правоохранительными органами, вследствие чего они часто удаляют журналы операций или даже содержание электронных почтовых сообщений (например, бесплатные счета электронной почты компании Yahoo! удаляются, если счетом не пользовались в течение четырех месяцев).

Кроме того, интернет-провайдеры в США имеют филиалы в ряде иностранных государств. В некоторых случаях российские правоохранительные органы могут, как мы подчеркивали выше, напрямую связываться с такими организациями по вопросу сохранения данных. Так, в Республике Ирландия имеются филиалы поставщиков услуг США (например, Yahoo!). Поэтому существует два варианта направления запроса, подготовленного согласно Руководству о международно-правовой помощи центрального органа Республики Ирландии: напрямую в филиал поставщику услуг; в компетентный орган Республики Ирландия[10].

Кроме того, в качестве альтернативы правоохранительный орган США, ведущий расследование по делу, может получить данные в силу имеющейся у него отечественной юрисдикции, а затем уже поделиться ими с правоохранительными органами Российской Федерации.

2. Получение журналов подключений и информации об абоненте от поставщика услуг Интернета или хостинговой компании. Законы, касающиеся электронных доказательств, находятся в США в стадии развития. Поэтому получение от поставщиков услуг Интернета разглашенных данных в виде журналов подключений, информации об абоненте и подобной информации от хостинговых компаний, обслуживающих веб-сайты, можно обеспечить путем направления официального запроса об оказании правовой помощи, содержащего точное описание данных, разглашение которых запрашивается, а также детальное объяснение того, какую пользу принесет расследованию разглашение этих данных. В таком случае необходимо получить судебный ордер.

Например, ст. 2703 (d) разд. 18 Свода законов США[11] гласит: «Судебный приказ о разглашении… должен выдаваться тогда, когда государственные органы…

[10] A Guide to Irish Law and Procedures of Mutual Legal Assistance in Criminal Matters. 2008. Дата обращения 1 января, 2020. http://www.justice.ie/en/JELR/Guide_to_Irish_Law_and_Procedures_-_Mutual_legal_Assistance_in_Criminal_Matters.pdf/Files/Guide_to_Irish_Law_and_Procedures_-_Mutual_legal_Assistance_in_Criminal_Matters.pdf.

[11] 18 U.S.C. Title 18 — Crimes and Criminal Procedure. 1948. Дата обращения 1 января, 2020. https://www.govinfo.gov/content/pkg/USCODE-2018-title18/pdf/USCODE-2018-title18.pdf.

предоставляют конкретные, словесно выражаемые факты, показывающие, что имеются достаточные основания полагать, что содержание… или учетные записи, или другая искомая информация имеют отношение к проводимому расследованию и существенны для него». Если запрос удовлетворяется, поставщик услуг Интернета или хостинговая компания делает копию запрашиваемых сведений и предоставляет их в электронном и/или бумажном формате официальному представителю правоохранительного органа США, исполняющего запрос иностранного государства.

Впрочем, поставщик услуг Интернета или его иностранный филиал имеет возможность предоставлять иностранным правоохранительным органам в той или иной форме помощь напрямую, без необходимости направления официального запроса в США, поскольку поставщик услуг Интернета работает в рамках других организационных, правовых и политических структур.

3. Исполнение ордера на получение информации о содержании хранимых электронных сообщений от поставщика услуг Интернета или хостинговой компании. Чтобы получить информацию об электронных сообщениях, хранящихся у поставщика услуг Интернета, или подобную информацию о содержании сообщений, хранящихся в хостинговой компании, потребуется приказ, известный как «ордер на обыск». В настоящее время крупные поставщики услуг Интернета и хостинговые компании не разглашают содержание каких-либо сообщений без ордера на обыск, выданного судом США. Для того чтобы получить такой ордер, необходима бóльшая степень детализации запрашиваемой информации.

Прежде всего нужно показать, что информация заслуживает доверия. Информация считается заслуживающей доверия, если ее источник — обычный гражданин, сотрудник правоохранительного органа или другое государственное должностное лицо. Если есть подозрения, что источник информации является нарушителем закона или анонимным лицом, следует предоставить дополнительные сведения, которые продемонстрировали бы надежность информации.

Подобная судебная процедура необходима для получения доказательств как по уголовному делу в США, так и по делу, находящемуся в производстве другого государства. Подчеркнем, что в США провайдер не обязан предоставлять информацию или данные правоохранительным органам без соответствующего ордера, за исключением отдельных обстоятельств.

Так, достаточную известность получило дело United States v. Meregildo[12]. Правоохранительные органы получили информацию с аккаунта Facebook фигуранта с помощью свидетеля, который был подписан на этот аккаунт в качестве друга. Соответственно, являясь виртуальным другом фигуранта, свидетель мог просматривать на странице информацию, имеющую значение для уголовного дела. В ходе судебного заседания действия представителей правоохранительных органов были обжалованы, так как, по мнению подсудимого, они нарушали положения Четвертой поправки Конституции США[13]. Изучив все обстоятельства, суд пришел к выводу, что в случае, если настройки конфиденциальности Facebook позволяют

[12] United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2, S. D. N. Y. Aug. 10, 2012. Дата обращения 1 января, 2020. https://casetext.com/pdf-email?slug=united-states-v-meregildo.

[13] Fourth Amendment to the U. S. Constitution. 1792. Дата обращения 1 января, 2020. https://www.govinfo.gov/content/pkg/GPO-CONAN-2017/pdf/GPO-CONAN-2017-10-5.pdf.

просматривать публикации друзей, правоохранительные органы могут получить к ним доступ через сотрудничающего с ними свидетеля, который является другом, без нарушения Четвертой поправки. Обосновывая решение, суд привел следующий довод: если пользователь страницы открывает доступ к ней своим друзьям, то эти друзья могут свободно использовать открытые для них данные, в том числе при сотрудничестве с правоохранительными органами.

Также в США действует так называемое право на удаление: если по уголовному делу были изъяты электронные носители информации, а сведения, полученные из них, были использованы против обвиняемого, то после вступления приговора в силу информация на этих электронных носителях, не имеющая отношения к делу, должна уничтожаться. Данного правила придерживаются все правоохранительные органы после судебного процесса United States v. Ganias[14], в результате которого под действие ордера на изъятие не попадают электронные сведения, хранящиеся более двух с половиной лет.

4. Перехват телекоммуникаций или компьютерных данных в реальном времени. В настоящее время законы США напрямую не разрешают перехват содержания телекоммуникаций или компьютерных сообщений в реальном времени по запросу об оказании правовой помощи по уголовным делам, затрагивающим интересы только иностранного государства. Эта мера возможна только в том случае, если в США проводится расследование и дело, в связи с которым оно проводится, является конкретным преступлением в США. В такой ситуации необходимо получить ордер на электронное прослушивание (часто называемое «перехват телефонных разговоров») с целью оказания помощи расследованию. В дальнейшем компетентные органы США могут поделиться перехваченными данными с иностранными партнерами на добровольной основе. В определенных обстоятельствах следует получить данные, перехваченные в реальном времени, не являющиеся содержанием, такие как номера телефонов, по которым звонило интересующее российских правоохранительных органов лицо, или информацию о подключениях, раскрывающих адреса интернет-протоколов (IP-адреса), с которых и на которые отсылаются электронные сообщения.

Таким образом, сегодня при направлении в США запроса о получении необходимой электронной информации стоит учитывать упомянутую выше классификацию информации, поскольку при запрашивании базовой информации и сведений о транзакциях российские правоохранительные органы могут напрямую на официальном бланке своего ведомства в рамках межведомственного сотрудничества направить запрос соответствующему поставщику услуг, приложив согласно законодательству РФ решение отечественного суда, а для того, чтобы получить содержание самой «переписки», требуется также наличие судебного ордера запрашиваемого государства (Малов 2018).

Европейский подход к получению электронной информации определяется Директивой о Европейском порядке расследования уголовных дел[15], принятой Парламентом и Советом Европейского союза (далее — ЕС) 03.04.2014 (далее — Ди-

[14] United States v. Ganias 755 F. 3d 125, 2d Cir, 2014. Дата обращения 1 января, 2020. https://www.epic.org/amicus/ganias/CCR-Ganias-En-Banc.pdf.

[15] Directive regarding the European Investigation Order in criminal matters / Directive 2014/41/EU. Дата обращения 1 января, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041.

ректива). С 22.05.2017 Директива заменила соответствующие положения конвенций, применимых между государствами-членами, связанными данной Директивой (ст. 2), в числе которых: 1) Европейская конвенция о взаимной помощи по уголовным делам Совета Европы от апреля 1959 г.[16], а также два дополнительных протокола и двусторонние соглашения, подписанные в соответствии со ст. 26; 2) Конвенция об осуществлении о применении Шенгенского соглашения от 14.06.1985 между правительствами государств экономического союза Бенилюкс, Федеративной Республики Германии и Французской Республики о постепенной отмене проверок на общих границах от 19.06.1990[17]; 3) Конвенция о взаимной помощи по уголовным делам между государствами — членами ЕС 29.05.2000 (вместе с протоколом)[18].

Кроме того, Директива заменяет Рамочное решение 2008/978/JHA[19] Совета о европейском ордере на получение доказательств в целях получения предметов, документов и данных, которые будут использоваться в производстве по уголовным делам, а также заменяет положения Рамочного решения 2003/577/JHA от 22.07.2003[20], касающиеся замораживания доказательств (п. 25 и 26 Директивы).

Европейский ордер на расследование — это судебное решение, которое было вынесено или подтверждено судебным органом государства-члена (государства выдачи) для проведения одной или нескольких конкретных следственных мер в другом государстве-члене (государстве исполнения) для получения доказательств в соответствии с Директивой. Что касается органов, способных выдавать и подтверждать европейский ордер на расследование (ст. 2 (2) Директивы), то Директива предоставляет подробную информацию о значении и сфере применения термина «судебный орган» и перечисляет следующие органы: судьи, суды, судьи по расследованию и государственные прокуроры, компетентные в соответствующем уголовном деле.

Директива закрепляет правила получения электронных доказательств в случаях запросов на идентификацию абонентских номеров и IP-адреса мобильных устройств (ст. 10 (2) (e) Директивы).

По запросам о перехвате телекоммуникаций Директива определяет предельные сроки принятия органом-исполнителем решения о признании или исполнении европейского ордера на расследование и дополнительный срок для проведения следственных действий (Losavio et al. 2018).

В связи с ростом направленных в адрес операторов связи запросов об электронных доказательствах Европейской комиссии было предложено изучить возможности общего подхода ЕС к правоприменительной юрисдикции киберпространства

---

[16] European Convention on Mutual Assistance in Criminal Matters 20.04.1959. Дата обращения 1 января, 2020. https://rm.coe.int/16800656ce.

[17] Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common borders. 19.06.1990. Дата обращения 1 января, 2020. https://www.jus.uio.no/english/services/library/treaties/02/2-07/implementing-schengen-agreement.xml.

[18] Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. 29.10.2000. Дата обращения 1 января, 2020. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF.

[19] Council Framework Decision 2008/978/JHA. Дата обращения 1 января, 2020. https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32008F0978.

[20] Framework Decision 2003/577/JHA. 22.07.2003. Дата обращения 1 января, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577.

в ситуациях, когда существующие правовые рамки недостаточны. Яркий пример — ситуация, в которой соответствующие электронные доказательства перемещаются между юрисдикциями в короткие промежутки времени.

В связи с этим зачастую возникают вопросы к Европейской комиссии со стороны правоохранительных органов об основании определения юрисдикции в киберпространстве, а также о возможности осуществлять процессуальные действия, которые могут проводиться независимо от физических границ государств. Аналогичные вопросы задаются и по поводу процесса взаимной правовой помощи в рамках произошедших изменений по инициативе Министерства юстиции США, отраженных в документе под названием «Трансграничные требования правоохранительных органов: анализ предлагаемого законопроекта Министерства юстиции США», подготовленном в августе 2016 г.[21] Ответы сформулированы в письме от 17.04.2018 «Оценка влияния предложения о регламентации Европейского парламента и Совета по регламентации европейского производства и сохранения запросов на электронные доказательства по уголовным делам» (Herrera-Flanigan, Ghosh 2010).

Основная цель проведенной оценки заключается в создании правового документа ЕС, позволяющего органам предварительного расследования (производства по делу) запрашивать или истребовать у операторов связи информацию о пользователе в иностранном государстве — участнике соглашения о взаимной правовой помощи о предоставлении электронной информации (Brown 2015).

17 апреля 2018 г. Европейская комиссия предложила новые правила для лучшего оснащения правоохранительных и судебных органов[22]. По сути, процедуры взаимной правовой помощи по-прежнему будут существовать, но появятся новые направления, или «быстрые пути», для конкретных случаев электронных доказательств.

Предлагаемое урегулирование направлено на решение проблемы, обусловленной хрупкостью электронных доказательств и их трансграничным характером. Указанные правила направлены на адаптацию механизмов сотрудничества в современных реалиях, предоставление судебных и правоохранительных инструментов для решения проблем, связанных с противодействием современным формам преступности. Однако использование таких инструментов должно происходить в условиях строгого соблюдения механизмов защиты конституционных прав граждан.

Рассматриваемый документ призван сосуществовать с действующими документами о сотрудничестве государств, поскольку они считаются релевантными и могут использоваться в соответствующих случаях компетентными органами. Это относится к двусторонним соглашениям между ЕС и странами, не входящими в ЕС, таким как соглашение о взаимной правовой помощи между ЕС и США, а также между ЕС и Японией (Borka, Klobučar 2019, 1000).

Новая правовая основа, опирающаяся на положения Конвенции, которая эффективно обеспечивает сотрудничество между правоохранительными и судебны-

[21] Cross-border requirements of law enforcement agencies: analysis of the proposed bill US Department of Justice. 2016. Дата обращения 1 января, 2020. https://www.justice.gov/file/969001/download.

[22] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters 17.04.2018. Дата обращения 1 января, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

ми органами в различных государствах — членах ЕС, дополнит ее путем разработки комплекса четких и последовательных принципов, позволяющих правоохранительным и судебным органам в одном государстве-члене обращаться непосредственно к поставщику услуг в другом государстве-члене с просьбой о раскрытии данных. Этот новый свод правил состоит из двух предложений: 1) предложения о регламентации европейских постановлений о производстве и хранении электронных доказательств по уголовным делам и 2) предложения о директиве, устанавливающей согласованные правила назначения юридических представителей для сбора доказательств в уголовном судопроизводстве[23].

Европейский производственный ордер позволит судебному органу в одном государстве-члене запрашивать электронные доказательства непосредственно у поставщика услуг, предлагающего услуги в ЕС и созданного или представленного в другом государстве-члене, независимо от местонахождения данных. Операторы связи будут обязаны отреагировать в течение 10 дней и в течение 6 часов в случае возникновения чрезвычайной ситуации. Эта мера будет дополнена Европейским порядком сохранения, который в соответствии с теми же условиями, изложенными выше, обяжет операторов связи сохранять конкретные данные, с тем чтобы орган мог запрашивать указанную информацию позднее через механизмы взаимной правовой помощи.

В новых предлагаемых постановлениях содержатся строгие гарантии обеспечения неприкосновенности частной жизни и права на судебную защиту. Фактически выдача таких приказов станет возможна только в рамках уголовного судопроизводства с учетом новых норм, устанавливающих обязанность органов власти получать одобрение от судебного органа, который будет проверять законность, необходимость и соразмерность этих приказов (Buono 2019). Кроме того, производственные запросы на производство транзакционных (источник и место назначения сообщения, данные о местоположении устройства) или содержательных данных (текст, голос и т. д.) ограничиваются в рамках уголовных преступлений, наказуемых в государстве выдачи максимальным сроком наказания не менее трех лет, или в отношении конкретных киберпреступлений и связанных с терроризмом преступлений, определенных в предложении. Поэтому среди гарантий можно перечислить следующие: постановления должны быть утверждены судебным органом, физические лица будут уведомлены о том, что их данные были запрошены, они будут проинформированы о своих правах и уголовно-правовых процессуальных правах (Dronova, Smagorinskiy, Yastrebov 2019).

3. Выводы

Международные нормативные акты, посвященные процедурам получения электронной информации у операторов связи иностранных государств, остаются вне поля зрения российского законодательства, что, безусловно, негативно отражается на данном направлении деятельности правоохранительных органов. Целесо-

[23] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Strasbourg, 17.04.2018 COM, 2018, 226 final. Дата обращения 1 января, 2020. https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf.

образно пересмотреть существующую правовую доктрину в связи с нарастающей угрозой наступления последствий от преступной абонентской активности лиц, учетные записи которых регистрируются в иностранных государствах

При решении указанных проблем считаем невозможным оставить без должного внимания и национальное законодательство РФ. Вопросы, касающиеся получения электронной информации по уголовным делам в рамках международного сотрудничества, должны быть закреплены в Уголовно-процессуальном кодексе РФ от 18.12.2001 № 174-ФЗ (далее — УПК РФ), а также в некоторых других отраслевых законах, в частности в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В УПК РФ должны быть предусмотрены общие нормы, регламентирующие правила, порядок и особенности получения электронных данных по уголовным делам, а также с учетом предписаний международных соглашений детализирующие положения, определяющие основания, условия и порядок направления запросов об оказании правовой помощи по уголовным делам. Вместе с тем необходима проработка по некоторой аналогии с УПК РФ и положений Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-разыскной деятельности» в части определения общих оснований и условий направления правоохранительным органам иностранных государств запросов об оказании содействия в рамках международного полицейского сотрудничества.

Затронутые в статье проблемы и предложенные в общих чертах пути их решения не исчерпывают всего комплекса вопросов сотрудничества государств в указанной сфере. Мы коснулись наиболее актуальных аспектов межгосударственного взаимодействия в рассматриваемой области, имеющих большое значение для правоохранительных органов РФ. Озвученные предложения по совершенствованию международной и национально-правовой базы, без сомнения, носят дискуссионный характер. Однако их выделение представляется в целом необходимым для определения общего вектора решения проблем, связанных с получением электронной информации в рамках расследования уголовных дел.

Библиография

Волеводз, Александр Г. 2018. «Международное сотрудничество в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты: постановка проблемы». *Современное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования: сб. материалов науч.-практ. конф., посвященной 300-летию российской полиции*, 66–75. Орел: Орловский юридический институт МВД России.

Литвишко, Петр А. 2015. «Интеграция предварительного расследования и оперативно-розыскной деятельности: иностранный и международный опыт». *Библиотека криминалиста: научный журнал* 3: 309–319.

Малов, Александр 2018. «Получение электронных доказательств от иностранных юрисдикций (на примере США)». *Законность* 9: 56–60.

Шестак, Виктор А., Александр Г. Волеводз. 2019. «Современные потребности правового обеспечения искусственного интеллекта: взгляд из России». *Всероссийский криминологический журнал* 13 (2): 197–206.

Щерба, Сергей П. 2016. «Международное сотрудничество России в сфере выдачи для уголовного преследования на основе принципа взаимности». *Международное уголовное право и международная юстиция* 4: 3–8.

Borka, Jerman Blažič, Tomaž Klobučar. 2019. "Advancement in Cybercrime Investigation — the New European Legal Instruments for Collecting Cross-border e-Evidence". *International Conference on Information Technology & Systems*, 858–867. Ljubljana.

Broadhurst Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and Cybercrime: an analysis of the nature of groups engaged in cybercrime". *International Journal of Cyber Criminology* 8 (1): 1–20.

Brown, Cameron, S. D. 2015. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice". *International Journal of Cyber Criminology* 9 (1): 55–119.

Buono, Laviero. 2019. "The genesis of the European Union's new proposed legal instrument(s) on e-evidence". *ERA Forum* 19 (3): 307–312.

Collin, Barry. 1997. "The Future of Cyberterrorism". *Crime & Justice International Journal* 13 (2): 51–71.

Cox, Joseph. 2016. "Staying in the Shadows: The Use of Bitcoin and Encryption in Cryptomarkets". *The Internet and Drug Markets.* Eds Jane Mounteney, Alberto Oteo, Paul Griffiths, 41–47. Lisbon: EMCDDA.

Dronova, Olga B., Boris P. Smagorinskiy, Vladislav B. Yastrebov. 2019. "Counteraction to e-commerce crimes committed with the use of online stores". *Studies in Systems, Decision and Control* 181: 121–131.

Foley, Sean, Jonathan R. Karlsen, Talis J. Putnins. 2018. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" *Review of Financial Studies, Forthcoming. SSRN.* Дата обращения 1 января, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645.

Herrera-Flanigan, Jessica R., Sumit Ghosh. 2010. "Criminal Regulations". *Cybercrimes: A Multidisciplinary Analysis*. Eds Sumit Ghosh, Elliot Turrini, 265–308. Berlin: Springer.

Leukfeldt, Eric R. 2015. "Organised cybercrime and social opportunity structures: a proposal for future research directions". *The European Review of Organised Crime* 2: 91–103.

Lievens, Eva. 2014. "Bullying and sexting in social networks: protecting minors from criminal acts or empowering minors to cope with risky behaviour?" *International Journal of Law, Crime and Justice* 42 (3): 251–270.

Losavio, Michael M., K. P. Chow, Andras Koltay, Joshua James. 2018. "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security". *Security and Privacy* 1 (3): e23. https://doi.org/10.1002/spy2.23.

Статья поступила в редакцию 6 февраля 2020 г.;
рекомендована в печать 17 декабря 2020 г.

Контактная информация:

Клевцов Кирилл Константинович — канд. юрид. наук, доц.; k.klevtsov@inno.mgimo.ru
Васюков Виталий Федорович — д-р юрид. наук, доц.; vvf0109@yandex.ru

Obtaining electronic information on criminal cases within the framework of international cooperation

K. K. Klevtsov[1], V. F. Vasyukov[1,2]

[1] Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation, 76, pr. Vernadskogo, Moscow, 119454, Russian Federation
[2] Oryol Institute of Internal Affairs of the Russian Federation named after V. V. Lukyanov, 2, ul. Ignatova, Oryol, 302025, Russian Federation

For citation: Klevtsov, Kirill K., Vitaliy F. Vasyukov. 2021. "Obtaining electronic information on criminal cases within the framework of international cooperation". *Vestnik of Saint Petersburg University. Law* 1: 36–51. https://doi.org/10.21638/spbu14.2021.103 (In Russian)

The explosive growth of information and communication technologies, which has affected human social communication institutions, has become commensurate with the increase in

potential risks to the security and rights of citizens. The authors of the article attempt to highlight the issues of international cooperation between law enforcement agencies of the Russian Federation and other countries in the framework of obtaining electronic information that is important for proving criminal cases. Attention is paid to procedures for ensuring the collection and use of electronic data in the response to crime occurring in the current fine line of confidentiality of privacy and security. Despite the mutual agreements signed between many countries of the world, the practical implementation of regulations that ensure the provision of electronic information in the framework of international cooperation is currently fraught with certain problems. Meanwhile, in the context of countering such dangerous phenomena for the world community as terrorism, extremism, drug trafficking, weapons, and people, a single mechanism for exchanging information stored on a gigantic scale on the servers of Telecom operators and providers has not yet been developed. The actual search for data stored on mobile devices usually requires a warrant in common law countries. In situations where there is a significant risk of loss of evidence, such as when data detection and other computer forensics tools are actively used, some jurisdictions allow law enforcement agencies to perform limited searches of devices without a warrant due to alleged data vulnerability. Another problem is the retention of stored data, since different practices apply in different countries. In this regard, it is essential that investigators and prosecutors are well informed about geo-specific data mapping issues, including "embargoes" or bans on the exchange of computer information.

Keywords: international cooperation, international agreement, procedural actions, investigative actions, computer information, legal assistance, electronic evidence, criminal proceedings, electronic messages, subscriber information, competent authorities.

References

Borka, Jerman Blažič, Tomaž Klobučar. 2019. "Advancement in Cybercrime Investigation — the New European Legal Instruments for Collecting Cross-border e-Evidence". *International Conference on Information Technology & Systems*, 858–867. Ljubljana.

Broadhurst Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and Cybercrime: an analysis of the nature of groups engaged in cybercrime". *International Journal of Cyber Criminology* 8 (1): 1–20.

Brown, Cameron, S. D. 2015. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice". *International Journal of Cyber Criminology* 9 (1): 55–119.

Buono, Laviero. 2019. "The genesis of the European Union's new proposed legal instrument(s) on e-evidence". *ERA Forum* 19 (3): 307–312.

Collin, Barry 1997. "The Future of Cyberterrorism". *Crime & Justice International Journal* 13 (2): 51–71.

Cox, Joseph 2016. "Staying in the Shadows: The Use of Bitcoin and Encryption in Cryptomarkets". *The Internet and Drug Markets.* Eds Jane Mounteney, Alberto Oteo, Paul Griffiths, 41–47. Lisbon, EMCDDA.

Dronova, Olga B., Boris P. Smagorinskiy, Vladislav B. Yastrebov. 2019. "Counteraction to e-commerce crimes committed with the use of online stores". *Studies in Systems, Decision and Control* 181: 121–131.

Foley, Sean, Jonathan R. Karlsen, Talis J. Putnins. 2018. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" *Review of Financial Studies, Forthcoming. SSRN.* Accessed January 1, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645.

Herrera-Flanigan, Jessica R., Sumit Ghosh. 2010. "Criminal Regulations". *Cybercrimes: A Multidisciplinary Analysis,* eds Sumit Ghosh, Elliot Turrini, 265–308. Berlin, Springer.

Leukfeldt, Eric R. 2015. "Organised cybercrime and social opportunity structures: a proposal for future research directions". *The European Review of Organised Crime* 2: 91–103.

Lievens, Eva 2014. "Bullying and sexting in social networks: protecting minors from criminal acts or empowering minors to cope with risky behaviour?" *International Journal of Law, Crime and Justice* 42 (3): 251–270.

Litvishko, Petr A. 2015. "Integration of the preliminary investigation and operational-search activity: foreign experience". *Biblioteka kriminalista: nauchnyi zhurnal* 3: 309–319. (In Russian)

Losavio, Michael M., K. P. Chow, Andras Koltay, Joshua James. 2018. "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security". *Security and Privacy* 1 (3): e23. https://doi.org/10.1002/spy2.23.

Malov, Aleksandr. 2018. "Obtaining electronic evidence from foreign jurisdictions (for example USA)". *Zakonnost'* 9: 56–60. (In Russian)

Shcherba, Sergei P. 2016. "International cooperation of Russia in the sphere of extradition for criminal prosecution on the basis of reciprocity". *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaia iustitsiia* 4: 3–8. (In Russian)

Shestak, Viktor A., Aleksandr G. Volevodz. 2019. "Modern requirements of legal security artificial intelligence: a view from Russia". *Vserossiiskii kriminologicheskii zhurnal* 13 (2): 197–206. (In Russian)

Volevodz, Aleksandr G. 2018. "International cooperation in the field of criminal justice in cases of crimes committed with the use of cryptocurrency: problem". *Sovremennoe ugolovno-protsessual'noe pravo — uroki istorii i problemy dal'neishego reformirovaniia: sb. materialov nauch.-prakt. konf., posviashchennoi 300-letiiu rossiiskoi politsii*, 66–75. Orel, Orlovskii iuridicheskii institut MVD Rossii Publ. (In Russian)

Received: February 6, 2020
Accepted: December 17, 2020

Authors' information:

Kirill K. Klevtsov — PhD in Law, Associate Professor; k.klevtsov@inno.mgimo.ru
Vitaliy F. Vasyukov — Dr. Sci. in Law, Associate Professor; vvf0109@yandex.ru