УДК 343.422
ББК Х408.16
DOI: 10.14529/law190103

ДЕЙСТВИЕ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ЗАКОНА В «КИБЕРПРОСТРАНСТВЕ»: ПРОБЛЕМА ТРАНСГРАНИЧНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

С. В. Зуев
Южно-Уральский государственный университет, г. Челябинск,
В. С. Черкасов
Дальневосточный юридический институт МВД России, г. Хабаровск

В статье рассматривается действие уголовно-процессуального закона в «киберпространстве». Анализируются основные теоретические подходы. Раскрываются недостатки международного правового регулирования. Предлагается рассматривать «киберпространство» с точки зрения режима общих международных территорий. Обосновываются условия допустимости производства трансграничных следственных действий.

Ключевые слова: информационные технологии, электронная информация, киберпространство, действие уголовно-процессуального закона в пространстве, трансграничность, следственное действие.

Современные информационные технологии образуют особую среду взаимодействия между индивидами и технологиями. Одним из распространенных определений названной среды информационного взаимодействия является «киберпространство».

В действующем законодательстве не закреплена юридическая категория, отражающая дефиницию киберпространства. Несмотря на это, в науке существуют различные подходы к определению названного явления. Так, А. И. Халиуллин утверждает, что «виртуальное пространство, образуемое потоками информации в рамках подобных сетей, получило условное наименование в научных исследованиях – «киберпространство» [2].

Как указывают Т. Л. Тропина, В. А. Номоконов, в модельном законе международного союза электросвязи 2009 года «под киберпространством определяется физическое или нефизическое пространство, созданное или сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных и пользователи» [1, с. 48].

Таким образом, киберпространство представляет собой нематериальную среду информационного взаимодействия, реализующуюся на основе программно-аппаратных средств. При этом участником информационного взаимодействия в киберпространстве может быть лицо, находящееся в любой точке планеты Земля, а программно-аппаратные средства могут быть физически расположены на территории одного или одновременного неограниченного количества государств.

Отметим, что действия в «киберпространстве» могут носить конкретные материальные последствия, так как посредством «киберпространства» можно организовывать взаимодействие не только между индивидами, но и между индивидом и техникой.

Важной особенностью является то, что в «киберпространстве» отсутствуют физические границы. Оно является трансграничным. Это вызывает проблематику при определении пространственного действия законодательства какого-либо государства.

Не является исключением уголовно-процессуальное законодательство Российской Федерации. Согласно ч. 1 ст. 2 УПК РФ производство по уголовному делу на территории Российской Федерации независимо от места совершения преступления ведется в соответствии с УПК РФ, если международным договором Российской Федерации не установлено иное. В свою очередь ч. 2 ст. 2 УПК РФ определяет, что действие уголовно-процессуального закона распространяется на воздушное, морское или речное судно под флагом РФ, находящееся за пределами территории РФ, но приписанное к порту РФ. В соответствии с ч. 3 ст. 2 УПК РФ отдельные про-

цессуальные действия могут проводиться за пределами территории Российской Федерации в случаях, предусмотренных ст. 12 УК РФ. Таким образом, действие уголовно-процессуального закона в пространстве определяется физическими, материальными границами или лицом, которое существует в материальном мире. Данное положение вступает в противоречие с таким явлением, как «киберпространство».

Например, при осмотре изъятого мобильного телефона можно получить доступ не только к информации, которая хранится непосредственно в памяти электронного устройства, но и к информации, которая расположена на серверах удаленно в «облаке». Необходимо учитывать, что организация, владеющая и управляющая серверами, может физически находиться в одном государстве, а серверы располагаться совершенно в другом.

Не исключена и такая ситуация, когда лицо совершило преступление в Российской Федерации или против интересов Российской Федерации, но находится за пределами территории Российской Федерации, и есть необходимость исследовать электронное устройство удаленно лица. На данное обстоятельство обращал внимание И. И. Карташов, указывая, что «УПК РФ оставляет открытым вопрос о возможности обыска в компьютерных сетях, если они находятся за пределами обыскиваемых помещений» [5, с. 25].

Следовательно, достаточно сложно определить, каким образом будут реализовываться нормы, регулирующие действие уголовно-процессуального закона в пространстве относительно «киберпространства».

На данную проблему уже было обращено внимание в международном праве. Э. Л. Ансельмно указывает: «Новые особенности пространства, обусловленные Интернетом, указывают на неэффективность понятия географической территориальности в международном праве, поскольку в киберпространстве ослабевает связь с физическим местоположением… По сути внетерриториальность создает конфликт в сфере права государств на юрисдикцию» [3, с. 25–26].

Обосновывая свое умозаключение, автор приводит следующий пример по делу компании «Yahoo!» против Франции. На сайте компании «Yahoo!» была выставлена реликвия времен нацисткой Германии. Во Франции был подан иск против «Yahoo!» в связи с тем, что подобные предметы запрещено реализовывать на территории Франции. В свою очередь компания «Yahoo!» подала встречный иск на территории США, так как юридический адрес компании был в штате Калифорния. Французский суд указал, что компания должна исключить доступ граждан Франции к информации, расположенной на сайте. В свою очередь суд США пришел к выводу, что определения национального французского суда не имеет юридической силы в отношении американских компаний, которые физически расположены на территории США. Компания «Yahoo!» заявила, что не разрабатывала сайт для какого-то государства. Поскольку сайт не является французским, «Yahoo!» не нарушила законов как Франции, так и США [3, с. 20].

На рассматриваемую проблему обращал внимание А. Л. Осипенко, который указывал, что от разрешения вопроса о юрисдикции конкретного государства на раскрытие трансграничного преступления зависят пределы полномочий национальных оперативно-розыскных органов в сетевом информационном пространстве, а, следовательно, и допустимость осуществления действий разведывательно-поискового характера [6, с. 20].

Подтверждая данное суждение, автор приводит следующий пример. Так, в 2000 году ФБР США произвело удаленное обследование компьютеров, находящихся на территории России, которые использовались российскими хакерами в противоправных целях. Данные, полученные агентами ФБР, были использованы в качестве доказательств в судебном процессе. Однако проведение подобных мероприятий вызвало возмущение со стороны ФСБ России, так как ФБР проигнорировало необходимость обращения с запросом к правоохранительным органам России [6, с. 20].

В юридической литературе рассматриваются различные точки зрения относительно решения вопроса о юрисдикции. Их обобщение позволяет выделить несколько подходов. Согласно первому подходу, «киберпространство» надлежит воспринимать как общую территорию, по аналогии с открытым морем, космосом, Антарктикой. Правила по использованию «киберпространства» должны быть аналогичны правилам, действующим в отношении общих территорий [3, с. 25].

Критически оценивая данный подход, А. Л. Осипенко указывает, что вряд ли возможно сегодня всерьез обсуждать вопрос о

признании киберпространства суверенной территорией с независимым внутренним правовым регулированием… последствия противоправных действий наступают не только в «киберпространстве», но и в физическом мире, затрагивая интересы, защищаемые национальным законодательством конкретного государства. Исходя из этого, право на осуществление уголовного преследования должно распространяться на сетевые события, которые являются территориально неопределенными, но имеют последствия на территории конкретного государства [6, с. 21].

На наш взгляд, общественно опасные деяния, совершенные на физически существующих «общих» международных территориях, также могут иметь реальные последствия для определенного государства, что соотносится с деятельностью в киберпространстве.

Второй подход можно обобщить в необходимость определения юрисдикции государства, исходя из места совершения преступления или наступления последствий общественно-опасного деяния [6, с. 21–22; 4, с. 56–57].

Данный подход достаточно сложно реализовать на практике. Несмотря на то, что существуют технологии, которые позволяют достаточно точно определить, с какой территории произошел выход в сеть «Интернет», с целью совершения преступления [4, с. 56], есть общедоступные VPN-программы, позволяющие скрыть источник выхода или намеренно указать неверный территориальный адрес.

Не исключена и такая ситуация, когда «проникновение» в компьютерную сеть банка Германии с целью совершения преступления совершает гражданин Франции, который перемещается по территории Китая. В данном случае представляется проблематичным определить место совершения преступления. Определение юрисдикции по общественно опасным последствиям также может представлять значительные трудности. К примеру, к юрисдикции какой страны можно отнести расследование преступления, связанного с использованием вируса «Wanna Cry», который заразил компьютеры в более чем 70 странах мира?

Третий подход заключается в том, что юрисдикция государства и правомерность получения доказательств в «киберпространстве» определяется международными договорами и нормативно-правовыми актами. Данная модель реализуется практически и рассматривается в научной среде как основной вектор правового регулирования [6, с. 23; 4, с. 57].

На сегодняшний день действует Конвенция о преступности в сфере компьютерной информации ETS № 185 от 23 ноября 2001 г. Международный документ содержит нормы, подлежащие имплементации в национальное законодательство участников конвенции. Нормы конвенции определяют совокупность составов преступлений, а также перечень процессуальных мероприятий, направленных на трансграничное получение компьютерной информации в качестве доказательства по уголовному делу.

Международное сотрудничество определяется главой III названной конвенции. Статья 32 регулирует трансграничный доступ к охраняемой законом информации. В соответствии с п. «a» ст. 32 Конвенции сторона-участник имеет право без согласия получать доступ к общедоступным компьютерным данным. На основании п. «b» ст. 32 Конвенции сторона-участник имеет право без согласия другого государства-участника «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему».

На основании ст. 27 Конвенции взаимодействие государств-участников осуществляется через направление запросов о взаимной помощи, компетентному органу, который определяется государством-участником конвенции. Статья 35 обязывает создать контактный центр, который будет работать 24 часа в сутки 7 дней в неделю для оказания неотложной помощи при расследовании уголовного дела.

Анализ норм Конвенции о преступности в сфере компьютерной информации позволяет сделать вывод, что государствам-участникам необходимо получать разрешение о производстве трансграничных следственных действий. Участниками Конвенции являются не только страны Европы, но и другие государства, к примеру, США, Израиль, Япония, Канада и др. (общее количество участников 56). Российская Федерация стала участником Конвенции в 2005 году, но уже в 2008 году вышла из Конвенции (Распоряжение Президента РФ

№ 144-рп от 22 марта 2008 г.). На наш взгляд, присоединение к названной конвенции сказалось бы положительно на возможности российских правоохранительных органов производить трансграничные следственные действия, однако не разрешит все поставленные проблемы в рамках российского уголовно-процессуального закона.

Во-первых, направление запроса о правовой помощи в порядке ст. 453 УПК РФ является сложным процессуальным действием, которое производится с участием высшего руководства органов исполнительной и судебной власти Российской Федерации. Более того, направление запроса о правовой помощи и исполнение данного запроса иностранным государством могут занимать достаточно длительное время.

Представляется, что достаточно сложно реализовать международный механизм, позволяющий получать электронные доказательства по каждому уголовному делу, которое находится в производстве. На наш взгляд, необоснованно будет инициировать запрос о международной правовой помощи, например в США, для предоставления электронной переписки пользователя интернет-сервиса, когда отсутствует согласие лица, имеющего полномочия на раскрытие данных, а сама электронная информация хранится удаленно в «облаке». При этом сам интернет-сервис или лицо могут физически находиться в иностранном государстве.

Допустимыми представляются действия, направленные на получение электронной информации с использованием возможностей национальной правоохранительной системы, когда электронное устройство уже изъято или существует техническая возможность произвести процессуальные действия, направленные на получение электронной информации «дистанционно», с учетом соблюдения прав и безопасности третьих лиц.

Во-вторых, исполнение Конвенции о преступности в сфере компьютерной информации может быть обусловлено геополитической обстановкой, которая в настоящий момент является неблагоприятной для Российской Федерации.

В-третьих, как показывает опыт, получение электронной информации может быть обусловлено политикой частной организации. Ярким примером служит ситуация 2018 года с интернет-мессенджером «Telegram», владелец которого отказался передавать Российской Федерации ключи дешифровки сообщений.

Таким образом, международный механизм трансграничного получения электронной информации юридически сконструирован так, что в большинстве случаев необходимо получать согласие страны участника Конвенции о преступности в сфере компьютерной информации. Подобное обстоятельство является негативной стороной международного регулирования действия уголовно-процессуального закона в «киберпространстве», так как потребность на получение электронной информации при производстве по уголовному делу является повсеместной, а взаимодействие в рамках международной правовой помощи будет значительно замедлять производство по уголовному делу. Поэтому следует предусмотреть возможность производства следственных действий в рамках уголовно-процессуального закона Российской Федерации. Пользователи сети «Интернет» не знают и не интересуются физическим местонахождением интернет-сервиса, которым они пользуются. В настоящее время невозможно установить объем юрисдикции конкретного государства в определенной области «киберпространства».

Исходя из этого, «киберпространство» необходимо рассматривать с точки зрения режима общих международных территорий. Однако при этом следует учитывать, что производство процессуальных действий в «киберпространстве» может затрагивать права и интересы, а также аппаратно-программные средства граждан и организаций, которые могут находиться в любой точке планеты Земля.

Необходимо определить возможную степень «проникновения» в информационно-телекоммуникационную сеть (социальную сеть, базы данных и т.д.), с учетом интересов третьих лиц (государства, распространителя информации в сети «Интернет»), понимая, что «киберпространство» обладает режимом общих международных территорий.

В ст. 2 Конвенции об открытом море от 29 апреля 1958 г. и ст. 3 Договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела от 27 января 1967 г., определяется свобода доступа и использования международных территорий при условии обеспечения международного мира и безопасности.

Отметим, что механизм получения информации через изъятый электронный носитель является распространенным явлением в уголовно-процессуальной деятельности (США, Канада, Россия, Бельгия и т.д.). Более того, к примеру, в Бельгии предусмотрена уголовная ответственность за отказ в сотрудничестве при производстве «электронного обыска» [7, с. 93–114].

Основываясь на имеющейся практике, мы приходим к выводу, что существующий механизм сбора информации через изъятый электронный носитель не вызывает противоречий в международных отношениях, так как обеспечивает соблюдение международного мира и безопасности при производстве трансграничных действий в «киберпространстве».

По нашему мнению, данная ситуация обусловлена тем, что доступ через изъятое электронное устройство производится только к определенной области киберпространства, которая относится к конкретному лицу.

В случаях, когда может возникнуть необходимость проведения трансграничных следственных действий без изъятого электронного носителя информации (удаленный обыск), нужно учитывать область «киберпространства», которая будет затрагиваться при производстве трансграничных следственных действиях.

На наш взгляд, объектом трансграничных следственных действий может выступать только индивидуально-определенная область «киберпространства», которая привязана к лицу посредством данных, которые позволяют его идентифицировать (сетевой адрес, электронная почта и т.д.). Если производство по уголовному делу ведется в отношении неустановленного лица, то допустимо производить трансграничные следственные действия по идентификационным данным пользователя в киберпространстве при наличии достаточных сведений, указывающих на то, что идентификационные данные относятся к лицу, совершившему преступление.

При этом допустимо выходить за пределы «киберпространства», привязанного к физической памяти электронного носителя информации, если имеются достаточные данные полагать, что могут быть обнаружены сведения, имеющие отношение к уголовному делу. Данный принцип производства трансграничных следственных действий можно обозначать как «электронное домино». Например, в ходе производства «дистанционного обыска» компьютера у следователя возникает предположение, что чертежи созданного взрывного устройства или переписки между соучастниками преступления содержатся в «облачном сервисе» (Яндекс, Google диск, WhatsApp Web). При наличии технической возможности допустимо исследовать область «киберпространства», даже если есть необходимость преодолеть защиту профиля «облачного хранилища». Исследование «киберпространства» может вестись и в обратном направлении, начиная с «облачного сервиса».

Недопустимо производить трансграничные следственные действия в тех случаях, когда может создаться угроза безопасности какого-либо государства. К примеру, интернет-сервис, который используется гражданами и на территории конкретного государства (национальный интернет-банк, госуслуги и т.д.). В данном случае следственное действие необходимо произвести в рамках международной правовой помощи.

Таким образом, уголовно-процессуальная юрисдикция государства в «киберпространстве» в настоящий момент не получила должного регулирования. По своим юридическим свойствам «киберпространство» наиболее похоже на общие международные территории. При определении допустимости и пределов производства трансграничных следственных действий необходимо учитывать положения ст. 2 УПК РФ с учетом обозначенных в статье ограничений.

Литература

1. ITU Toolkit For Cybercrime Legislation. ITU, 2009 Цит. по: Тропина Т. Л., Номоконов В. А. . Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–55.

2. Mungo P. The Extraordinary underworld of Hackers, Phreakers, Virus writers, and Keyboard criminals / P. Mungo, B. Clough. New York: Random house, 1992, pp. 200–202. Цит. по: Халиуллин А. И. Подходы к определению киберпреступления // СПС «КонсультантПлюс».

3. Ансельмно, Э. Л. Киберпространство в международном законодательстве: опровергает ли развитие интернета принцип территориальности в международном праве? / Э. Л. Ансельмно // Экономические стратегии. – 2006. – № 2. – С 24–31.

4. Искевич, И. С. Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект / И. С. Искевич, М. Н. Кочеткова, А. М. Попов // Проблемы правоохранительной деятельности. – 2016. – № 2. – С. 54–58.

5. Карташов, И. И. «Цифровые доказательства» в уголовном процессе / И. И. Карташов // Центральный научный вестник. – 2016. – № 15. – С. 23–25.

6. Осипенко, А. Л. О правовом регулировании действий оперативно-розыскных органов при раскрытии трансграничных преступлений в сети Интернет / А. Л. Осипенко // Оперативник (сыщик). – 2011. – № 2. – С. 18–23.

7. Сергеев, М. С. Правовые основы применения электронной информации и электронных носителей информации в уголовном судопроизводстве: дис. … канд. юрид. наук / М. С. Сергеев. – Казань, 2018. – 322 с.

Зуев Сергей Васильевич – доктор юридических наук, заведующий кафедрой правоохранительной деятельности и национальной безопасности. Южно-Уральский государственный университет, г. Челябинск. E-mail: zuevsergej@inbox.ru.

Черкасов Виктор Сергеевич – адъюнкт, Дальневосточный юридический институт МВД России, г. Хабаровск. E-mail: viktor.kmsx@gmail.com.

Статья поступила в редакцию 20 декабря 2018 г.

DOI: 10.14529/law190103

FUNCTIONING OF THE CRIMINAL PROCEDURE LAW IN “CYBERSPACE”: THE PROBLEM OF CROSS-BORDER INVESTIGATIVE ACTIONS

S. V. Zuev
South Ural State University, Chelyabinsk, Russian Federation,
V. S. Cherkasov
Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, Khabarovsk, Russian Federation

The article deals with the effect of the criminal procedure law in the‘cyberspace’. The shortcomings of international legal regulation are revealed. It is proposed to consider “cyberspace” from the point of view of the regime of common international territories. The conditions for the admissibility of the production of cross-border investigative actions are justified.

Keywords: information technologies; electronic information; cyberspace; action of criminal procedure law in space; cross-border; investigative action.

References

1. ITU Toolkit For Cybercrime Legislation. ITU, 2009 cyte. by: T. L. Tropina, V. A. Nomokonov. [Criminal Cybercrime as new threat]. *Kriminalogiya: vchera, segodnya, zavtra [Criminologia: yesterday, today, tomorrow],* 2012, no. 24, pp. 45–55. (in Russ.)

2. Mungo P., Clough B. The Extraordinary underworld of Hackers, Phreakers, Virus writers, and Keyboard criminals. New York: Random house, 1992. pp. 200–202. Cyte. by: Khaliullin A. I. *Podkhody k opredeleniyu kiberprestupleniya* [Approaches to the definition of cybercrime]. Available at: reference system “Consultantplus”.

3. Anselmo E. L. [Cyberspace in international law: denies the development of the Internet, the principle of territoriality in international law?]. *Ekonomicheskie strategii [Economic strategy],* 2006, no. 2, pp. 24–31. (in Russ.)

4. Icevic I. S., Kochetkova N. M., Popov A. M. [Actual problems of definition of jurisdiction in the investigation of crimes in the information space: the international legal aspect]. *Problemy pravookhranitel'noj deyatel'nosti [Problems of law enforcement]*, 2016, no. 2, pp. 54–58. (in Russ.)

5. Kartashov I. I. [«Digital evidence» in criminal proceedings]. *Tsentral'nyj nauchnyj vestnik [Central scientific Bulletin]*, 2016, no. 15, pp. 23–25. (in Russ.)

6. Osipenko A. L. [On the legal regulation of the actions of the investigative authorities in the disclosure of cross-border crime on the Internet]. *Operativnik (syshhik) [The field investigator (sleuth)],* 2011, no. 2, pp. 18–23. (in Russ.)

7. Sergeyev M. S. *Pravovye osnovy primeneniya ehlektronnoj informatsii i ehlektronnykh nositelej informatsii v ugolovnom sudoproizvodstve:* dis. … kand. jurid. nauk [Legal basis for the use of electronic information and electronic media in criminal proceedings Diss. Kand. (Law)]. Kazan, 2018, 322 p.

Sergey Vasilievich Zuev – Doctor of Sciences (Law), Head of the Department of Law Enforcement and National Security, South Ural State University, Chelyabinsk, Russian Federation. E-mail: zuevsergej@inbox.ru.

Victor Sergeevich Cherkasov – Full-time post-graduate student of the Far East Home Ministry Law Institute of the Russian Federation, Khabarovsk, Russian Federation. E-mail: viktor.kmsx@gmail.com.

Received 20 December 2018.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Зуев, С. В. Действие уголовно-процессуального закона в «киберпространстве»: проблема трансграничных следственных действий / С. В. Зуев, В. С. Черкасов // Вестник ЮУрГУ. Серия «Право». – 2019. – Т. 19, № 1. – С. 17–23. DOI: 10.14529/law190103.

FOR CITATION

Zuev S. V., Cherkasov V. S. Functioning of the criminal procedure law in “cyberspace”: the problem of cross-border investigative actions. *Bulletin of the South Ural State University. Ser. Law*, 2019, vol. 19, no. 1, pp. 17–23. (in Russ.) DOI: 10.14529/ law190103.