УГОЛОВНЫЙ ПРОЦЕСС

УДК 343.13
DOI: 10.19073/2306-1340-2017-14-1-59-64

О ПРОТИВОРЕЧИВОМ ХАРАКТЕРЕ НОВЕЛЛЫ В ЗАКОНОДАТЕЛЬНОМ РЕГУЛИРОВАНИИ СЛЕДСТВЕННОГО ДЕЙСТВИЯ «НАЛОЖЕНИЕ АРЕСТА НА ПОЧТОВО-ТЕЛЕГРАФНЫЕ ОТПРАВЛЕНИЯ»

СУПРУН Сергей Владимирович*
✉ prozess_khv@mail.ru
Пер. Казарменный, 15, г. Хабаровск, 680020, Россия
ЧЕРКАСОВ Виктор Сергеевич▲
✉ artful_jew@mail.ru
Пер. Казарменный, 15, г. Хабаровск, 680020, Россия

Аннотация. *В статье анализируются законодательная новелла, относящаяся к производству следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» и связанная с возможностью производить выемку и осмотр электронных и иных сообщений, передаваемых по сетям электросвязи. Авторами делается вывод о том, что указанная новелла не согласуется с предметом, формой следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» и противоречит нормативным правовым актам, регулирующим общественные отношения в сфере электронной информации.*

Ключевые слова: *почтово-телеграфные отправления, следственное действие, электронное сообщение, электросвязь, законодательная новелла.*

On the Opposing Nature of Novella in the Legislative Regulation of the Investigatory Action "Arrest Of Postal And Telegraph"

Suprun Sergei V.**
✉ prozess_khv@mail.ru
Kazarmennyi lane, 15, Khabarovsk, 680020, Russia
Cherkasov Viktor S.▲▲
✉ artful_jew@mail.ru
Kazarmennyi lane, 15, Khabarovsk, 680020, Russia

Abstract. *The article analyzes the legislative innovation relating to the investigative action "arrest of postal and telegraph dispatches, their inspection and seizure" and associated with the ability to seize and inspect electronic and other messages transmitted via telecommunication networks. The Authors*

* Начальник кафедры уголовного процесса Дальневосточного юридического института МВД России, кандидат юридических наук, доцент.

▲ Адъюнкт Дальневосточного юридического института МВД России.

** Head of the Criminal Procedure Department of the Far Eastern Law Institute of the Ministry of Internal Affairs of the Russia, Candidate of Legal Sciences, Docent.

▲▲ Post-graduate student of the Far Eastern Law Institute of the Ministry of Internal Affairs of the Russia.

conclude that these novellas do not agree with the subject, the form of investigative action "arrest of postal and telegraph dispatches, their inspection and seizure" and contrary to the normative legal acts regulating public relations in the field of electronic information.

Keywords: *postal and telegraph dispatches, investigative action, e-mail message, telecommunications, legislative innovation.*

Информационные технологии прочно вошли в жизнь современного общества. Интеграция экономических, культурных, социальных и политических отношений с киберпространством не вызывает сомнения. Подобное положение подтолкнуло использовать электронно-информационную сферу в качестве инфраструктуры для совершения преступлений.

Статистические данные свидетельствуют об активном использовании киберпространства для преступных целей. Так, по результатам ежегодного исследования Norton Cybercrime Report – 2012[1] ущерб от киберпреступности за 2012 г. оценивается в 110 млрд долларов во всем мире и в 2 млрд долларов в России. Всего от киберпреступлений за год в мире пострадали около 556 млн человек – это 1,5 млн человек в день и 18 человек в секунду. Средний ущерб от кибератаки на одного среднестатистического пользователя составляет 197 долларов (по состоянию на 2012 г. – около 6 000 долларов). Подобное исследование проводилось Norton Cybercrime Report и в 2015 г.[2] По данным исследования, ущерб от киберпреступности за 2015 г. составил около 150 млрд долларов при 594 млн пострадавших. Возрастающая динамика киберпреступности очевидна.

Исходя из статистических данных Главного информационно-аналитического центра МВД России за 2015 г., количество совершаемых преступлений при помощи компьютерных и телекоммуникационных технологий растет[3]. Всего за 2015 г. было зарегистрировано 43 657 преступлений, что на 298,5 % больше, чем в аналогичном периоде прошлого года (далее – АППГ). Из них наибольшее количество приходится на преступления, направленные против собственности. К ним относятся мошенничества (ст. 159 Уголовного кодекса Российской Федерации (далее – УК РФ) и кражи чужого имущества (ст. 158 УК РФ). В 2015 г. было совершено 13 464 преступления, предусмотренных ст. 159 УК РФ, что на 515,6 % больше, чем в АППГ, и 8 446 краж чужого имущества, предусмотренных ст. 158 УК РФ, что на 262,5 % больше, чем в АППГ. Всего в суд было направлено 11 223 уголовных дела от общего количества дел о киберпреступности, находившихся в производстве органов предварительного расследования за 2015 г., что на 137,7 % больше, чем в АППГ. При этом было приостановлено 25 541 уголовное дело о киберпреступности за неустановлением лиц, подлежащих привлечению в качестве обвиняемого, что на 477,3 % больше, чем в АППГ.

По статье 158 УК РФ в суд за аналогичный период времени было направлено 753 уголовных дела о киберпреступности, что на 57,2 % больше, чем в АППГ. При этом было приостановлено 6 283 уголовных дела за неустановлением лиц, подлежащих привлечению в качестве обвиняемого, что на 397,1 % больше, чем в АППГ. По статье 159 УК РФ в суд направлено 1 350 уголовных дел о киберпреступности, что на 195,4 % больше, чем в АППГ. Приостановлено 9 473 дела, что на 578,6 % больше, чем в АППГ.

Таким образом, количество киберпреступлений по сравнению с 2014 г. в 2015 г. увеличилось в 3 раза, при этом количество нераскрытых преступлений увеличилось практически в 5 раз. Подобные обстоятельства должны были подтолкнуть государство на создание эффективных средств по борьбе с преступлениями в электронно-информационной сфере. Так, 7 июля 2016 г. был принят антитеррористический законодательный пакет, известный как «пакет Яровой». Принятые законодательные изменения внесли новеллы и в уголовно-процессуальные отношения, которые позволяют расширить возможности по получению сведений, имеющих

[1] *2012* Norton Cybercrime Report. URL: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[2] *2015* Norton Cybersecurity Insights Report. URL: http://us.norton.com/norton-cybersecurity-insights-report-global

[3] *Статистика* преступлений, совершаемых при помощи компьютерных и телекоммуникационных технологий, за 2015 год / ГИАЦ МВД России. Доступ из СТРАС «Юрист».

значение для уголовного дела, в том числе для органов предварительного расследования.

В частности, в рамках указанного законодательного пакета был принят Федеральный закон от 6 июля 2016 г. № 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»[4], которым в ст. 185 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) включена ч. 7. Согласно этой части, «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».

В соответствии с п. 10 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[5] (далее – ФЗ «Об информации») под электронным сообщением понимается «информация, переданная или полученная пользователем информационно-телекоммуникационной сети». Также в соответствии с п. 35 ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[6] под электросвязью понимаются любые «излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам».

Исходя из указанного выше определения, под категорию «электронные и иные сообщения» попадает широкий спектр информации, которая удовлетворяет потребностям органов, осуществляющих предварительное расследование, и на основе которой может быть получена доказательственная информация из электронно-информационной сферы, например, «Вконтакте», WhatsApp, Skype и другие интернет-сервисы.

Однако внесение в ст. 185 УПК РФ положения об осмотре и выемке электронных и иных сообщений, передаваемых по сетям электросвязи, создает сложности для органов предварительного расследования в ее реализации. Исходя из логики, если новелла была внесена в законодательные нормы, регулирующие производство следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», то предусмотренные ею предписания должны учитывать содержание, предмет и форму этого следственного действия, соответствовать нормативным правовым актам, регулирующим общественные отношения в области распространения информации в сети «Интернет». В действительности между данными категориями возникает юридическая коллизия, которая не позволит получать электронные и иные сообщения, передаваемые по сетям электросвязи. Необходимо разобраться в причинах возникновения указанной коллизии.

Среди ученых еще до внесения ч. 7 в ст. 185 УПК РФ не было единого мнения относительно допустимости распространения данного следственного действия на электронные сообщения. Е. Р. Россинская и А. И. Усов считают, что действия по изъятию электронной почты, адресованной абоненту, подпадают под выемку почтово-телеграфной корреспонденции и должны осуществляться в соответствии со ст. 185 УПК РФ [3, с. 99]. А. Н. Гуев в своей работе отмечает, что «в практике возник вопрос: относятся ли правила ч. 1 ст. 185 УПК к отправлениям по электронным средствам связи, в т. ч. по сетям Интернета? К сожалению, в ч. 1 ст. 185 УПК пробел, поскольку такие отправления нельзя приравнять к почтово-телеграфным сообщениям. Пробел надо устранять (учитывая большую распространенность таких отправлений), впредь до этого следует исходить из буквального текста ст. 185 УПК РФ» [2].

Исследуя предмет данного следственного действия, можно обоснованно предположить, что оно было предназначено для получения имеющих значение для уголовного дела сведений, возникающих в сфере почтово-телеграфных отправлений. Предметом данного следственного действия, исходя из содержания ч. 1 ст. 185 УПК РФ, являются бандероли, посылки,

---

[4] *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 : федер. закон от 6 июля 2016 г. № 375-ФЗ // Рос. газ. 2016. 11 июля.

[5] *Об информации,* информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // Рос. газ. 2006. 29 июля.

[6] *О связи* : федер. закон от 7 июля 2003 г. № 126-ФЗ // Рос. газ. 2003. 10 июля.

другие почтово-телеграфные отправления либо телеграммы или радиограммы. До 2016 г. электронные сообщения в данной норме уголовно-процессуального закона прямо не обозначались.

Рассмотрим подробнее, что понимается под другими почтово-телеграфными отправлениями. Перечень почтовых отправлений содержится в приказе Министерства связи и массовых коммуникаций Российской Федерации от 31 июля 2014 г. № 234 «Об утверждении правил оказании услуг почтовой связи»[7]. Согласно приложению № 2 приказа к ним относятся почтовая карточка, письмо, бандероль, секограмма, мелкий пакет, мешок «М», посылка. Также в пунктах 51–62 приказа предусмотрены положения, предусматривающие особенности приема и доставки (вручения) простых и заказных почтовых отправлений, пересылаемых в форме электронных документов, что фактически является электронным сообщением. Однако стоит учитывать, что в п. 51 анализируемого приказа предусмотрено, что данные электронные сообщения передаются с использованием информационной системы организации федеральной почтовой связи.

Если рассмотреть этот вопрос с позиции соотношения понятий, в соответствии с которой понятие «электронные сообщения» шире по объему и включает в себя понятие «электронные документы», передаваемые именно с использованием информационной системы организации федеральной почтовой связи, тогда законодательная поправка вписывается в текст уголовно-процессуального закона и выглядит логично. Однако если рассматривать производство этого следственного действия с позиции возможности и допустимости получать все электронные и иные сообщения, которые передаются по сетям электросвязи, то тогда возникает коллизия между новым предметом данного следственного действия, формой его осуществления и смежными нормативно-правовыми актами, регулирующими отношения, возникающие в области распространения информации в сети Интернет.

В пользу обоснования сформулированной нами выше научной позиции можно привести следующие аргументы. Содержание ст. 185 УПК РФ четко описывает форму производства следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка». Так, основными индивидуализирующими признаками субъекта следственного действия, на почтово-телеграфные отправления которого будет наложен арест, являются фамилия, имя, отчество и адрес лица (п. 1 ч. 3 ст. 185 УПК РФ). Указанные выше признаки субъекта подходят для наложения ареста на его почтово-телеграфные отправления. Вместе с этим они не подходят для наложения ареста на электронные сообщения, содержащиеся в сети Интернет. В отличие от традиционной почты в сети Интернет пользователь может придумать себе любое имя, фамилию, адрес, которые не будут препятствовать обмену электронными сообщениями и индивидуализировать его как конкретного пользователя. В рамках нового предмета следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» законодателю необходимо было ввести новые индивидуализирующие признаки субъекта для сети Интернет, например, сетевой адрес (IP-адрес), доменное имя, адрес электронной почты и т. д. Однако подобных поправок законодатель в УПК РФ не внес, чем существенно затруднил порядок производства данного следственного действия.

Также в правовой конструкции ст. 185 УПК РФ говорится о том, что следственное действие «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» производится в учреждениях связи. Законодатель не разъясняет, что понимается под учреждениями связи, охватывает ли категория «учреждение связи» выемку электронных сообщений в сети Интернет и какой субъект должен выдавать электронные сообщения в сети Интернет для их осмотра и выемки.

Отвечая на поставленные нами выше вопросы, обратимся к научной позиции А. В. Смирнова и К. Б. Калиновского, которые утверждают, что используемый законодателем в ст. 185 УПК РФ термин «учреждение связи» вносит неясность в деятельность органов предварительного расследования, прокуратуры и суда. Сформулированное ими суждение объясняется тем, что Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи»[8] предусматривает как минимум три сходных, но разных понятия: операторы почтовой связи, организации почтовой

[7] *Об утверждении* правил оказании услуг почтовой связи : приказ М-ва связи и массовых коммуникаций Рос. Федерации от 31 июля 2014 г. № 234 // Рос. газ. 2014. 31 дек.

[8] *О почтовой* связи : федер. закон от 17 июля 1999 г. № 176-ФЗ // Российская газета. 1999. 22 июля.

связи и объекты почтовой связи (ст. 2). В смысле ст. 185 УПК РФ наиболее верно считать, что арест исполняется оператором почтовой связи – организациями почтовой связи и индивидуальными предпринимателями, имеющими право на оказание услуг почтовой связи [4].

Более того, п. 1 ст. 10.1 ФЗ «Об информации» вводит категорию «организатор распространения информации в сети Интернет, под которым понимается «лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет, например, «Вконтакте», WhatsApp, Skype и т. д.

Согласно подп. 2 п. 3 ст. 10.1 ФЗ «Об информации» – еще одной новелле, предусмотренной Федеральным законом от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[9], на организатора распространения информации в сети Интернет возлагается следующая обязанность: текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео- или иные электронные сообщения пользователей сети Интернет хранить до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

Из указанного выше можно предположить, что категория «учреждение связи» охватывает категорию «организатор распространения информации в сети Интернет.

Однако с вышеуказанным предположением также связаны определенные противоречия. Так, в п. 3.1. ст. 10.1 ФЗ «Об информации» говорится, что «организатор распространения информации в сети Интернет обязан предоставлять указанную в пункте 3 настоящей статьи информацию (о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях (подп. 1 п. 3 ст. 10.1), текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет (подп. 2 п. 3 ст. 10.1) уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами». Из данного положения следует, что организаторы распространения информации в сети Интернет не обязаны предоставлять электронные сообщения органам, осуществляющим предварительное расследование.

Однако даже если электронные сообщения предоставляются силами и средствами Бюро специальных технических мероприятий МВД России, по аналогии с производством следственного действия «контроль и запись телефонных переговоров», то и в данном случае из-за прямого указания закона органы, осуществляющие оперативно-розыскную деятельность, получить электронные сообщения не смогут. Причина этого видится в том, что подп. 2 п. 3 ст. 10.1 ФЗ «Об информации», регламентирующий обязанность для организатора распространения информации в сети Интернет хранить содержание электронных сообщений на территории Российской Федерации, вступает в силу только с 1 июля 2018 г.

Необходимо отметить тот факт, что содержащиеся в «пакете Яровой» поправки в ФЗ «Об информации» приняты в связи с тем, что оперативным подразделениям в настоящий момент крайне сложно дается взаимодействие и, соответственно, получение электронных сообщений от организаторов распространения информации в сети Интернет, находящихся за границей. Причины этого детально описаны в работе В. В. Важенина и Т. З. Имакова. Так, в качестве одной из причин авторы выделяют факт того, что «большинство протоколов и технологий сети Интернет разработаны в США. Корпорации по управлению доменными именами и IP-адресами (ICANN) созданы при участии американского правитель-

[9] *О внесении* изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федер. закон от 6 июля 2016 г. № 374-ФЗ // Российская газета. 2016. 8 июля.

ства и находятся на территории США. Большинство корневых сервисов DNS, содержащих информации о доменах верхнего уровня и поддерживающие работу этих доменов, также находятся на территории США либо стран Западной Европы. Получение информации для российских правоохранительных органов представляет сложнейшую задачу, чаще всего невыполнимую» [1, с. 21].

Из всего сказанного следует, что если новелла ч. 7 ст. 185 УПК РФ распространяется только на электронные сообщения, передаваемые по сетям федеральной почтовой связи, то тогда она представляется логичной. Если же поправка задумывалась как охватывающая все электронные сообщения, которые передаются по сетям электросвязи, то возникают указанные выше коллизии в части определения предмета данного следственного действия, формы его осуществления, а также противоречия между смежными нормативно-правовыми актами, регулирующими отношения в сети Интернет.

В целом законодатель правильно обозначил вектор дальнейшего развития уголовно-процессуального законодательства, потому что нормы права, позволяющие правоприменителю получать широкий спектр сведений, имеющих значение для уголовного дела, безусловно, ему необходимы. Вместе с этим законодатель искусственно, без всестороннего юридического и логического анализа внедрил в уголовно-процессуальное законодательство норму о выемке и осмотре электронных и иных сообщений, передаваемых по сетям электросвязи, которая существенно снизила эффективность производства следственного действия «наложение ареста на почтово-телеграфные отправления, их осмотр и выемка».

Список литературы

1. Важенин В. В., Имаков Т. З. Проблемы противодействия экстремизму в сети Интернет // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2015. № 1. С. 19–26.

2. Гуев А. Н. Постатейный комментарий к Уголовно-процессуальному кодексу Российской Федерации. М. : Юридическая фирма «Контракт» : ИНФРА-М, 2003. 928 с.

3. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. 416 с.

4. Смирнов А. В., Калиновский К. Б. Комментарий к Уголовно-процессуальному кодексу Российской Федерации. Постатейный / под общ. ред. А. В. Смирнова. 4-е изд., перераб. и доп. Доступ из СПС «Гарант».

References

1. Vazhenin V. V., Imakov T. Z. Problemy protivodeistviia ekstremizmu v seti «Internet» [Problems of Counteraction to Extremism in the Internet]. *Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologii: problemy preduprezhdeniia, raskrytiia i rassledovaniia prestuplenii – Crime in the Field of Information and Telecommunication Technologies: Preventing Problems, Detection and Investigation of Crimes,* 2015, no. 1, pp. 19–26.

2. Guev A. N. *Postateinyi kommentarii k Ugolovno-protsessual'nomu kodeksu Rossiiskoi Federatsii* [Commentaries to the Criminal Procedure Code of the Russian Federation]. Moscow, Iuridicheskaia firma «Kontrakt» Publ., INFRA-M Publ., 2003. 928 p.

3. Rossinskaia E. R., Usov A. I. *Sudebnaia komp'iuterno-tekhnicheskaia ekspertiza* [Forensic Computer-Technical Expertise]. Moscow, Pravo I Zakon Publ., 2001. 416 p.

4. Smirnov A. V., Kalinovskii K. B. Kommentarii k Ugolovno-protsessual'nomu kodeksu Rossiiskoi Federatsii. Postateinyi [Commentary on the Code of Criminal Procedure of the Russian Federation. By-article]. 4th ed. *Garant,* 2016.