КРИМИНОЛОГИЯ

Научная статья
УДК 343.1, 343.7, 343.72 doi: 10.17223/23088451/20/18

ПРОБЛЕМНЫЕ ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ СЛЕДСТВЕННЫХ И ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОВД РФ С РОСКОМНАДЗОРОМ

Ольга Владимировна Ханинева

Краснодарский университет Министерства внутренних дел Российской Федерации, Краснодар, Россия, post_krdu@mvd.ru

Аннотация. В статье описываются основные проблемные вопросы взаимодействия подразделений органов внутренних дел Российской Федерации (ОВД РФ), задействованных в расследовании мошенничеств, совершенных посредством сети Интернет, с Роскомнадзором. Освещаются основные недочеты и неправильное толкование существующих нормативно-правовых актов Российской Федерации, регламентирующих полномочия Роскомнадзора, при направлении сотрудниками ОВД РФ запросов о предоставлении информации, имеющей значение для уголовного дела.

Ключевые слова: мошенничество, сеть Интернет, сайт, взаимодействие, запрос

Для цитирования: Ханинева О.В. Проблемные вопросы взаимодействия следственных и оперативных подразделений ОВД РФ с Роскомнадзором // Уголовная юстиция. 2022. № 20. С. 106–1110. doi: 10.17223/23088451/20/18

Original article
doi: 10.17223/23088451/20/18

PROBLEM ISSUES OF INTERACTION BETWEEN INVESTIGATING AND OPERATIONAL DIVISIONS OF THE RF INTERNAL AFFAIRS AGENCIES AND ROSKOMNADZOR

Olga V. Khanineva

Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia, post_krdu@mvd.ru

Abstract. The author analyzes the procedure and legal grounds for sending requests from law enforcement agencies involved in identifying, disclosing, and investigating fraud committed using information and telecommunication technologies to Roskomnadzor to obtain information relevant to the criminal case. The author also discusses the main shortcomings and misinterpretations of the current laws governing the interaction of these bodies and proposes ways to solve the problems.

Keywords: fraud, Internet, site, interaction, request

For citation: Khanineva, O.V. (2022) Problem issues of interaction between investigating and operational divisions of the RF Internal Affairs Agencies and Roskomnadzor. *Ugolovnaya yustitsiya – Russian Journal of Criminal Law.* 20. pp. 106–110. (In Russian). doi: 10.17223/23088451/20/18

Тематика рассматриваемого вопроса еще долгое время не перестанет быть актуальной в связи с глобальной цифровизацией всех сфер жизнедеятельности общества, на которую с 2020 г., в том числе, повлияла пандемия новой короновирусной инфекции во всем мире.

Российская Федерация оказалась в числе стран, в которых этот процесс произошел скачкообразно, что повлекло экстренную необходимость в освоении специалистами многих сфер новых для себя технологий, изучении способов работы с информацией и регламентирующей эту работу документацией и законодательства. В связи с чем не обошлось без наличия пробелов в знаниях и неправильного толкования существующих нормативно-правовых актов должностными лицами, так или иначе связанными с рассматриваемой сферой жизнедеятельности общества.

Автор считает необходимым сделать в данной статье акцент на существующих недоработках во взаимоотношениях сотрудников правоохранительной сферы и общественных организаций, действующих в поле информационных технологий.

Рассмотрим данный вопрос на примере такого важного в деятельности правоохранительных органов элемента борьбы с преступностью, как взаимодействие следственных и оперативных подразделений органов внутренних дел Российской Федерации (ОВД РФ), в частности с Роскомнадзором, касающегося наиболее

актуального вида преступлений – мошенничеств, совершаемых с использованием средств связи, сети Интернет и информационно-телекоммуникационных технологий.

Подробно останавливаться на этом виде преступлений и способах его совершения не будем, так как многим они уже известны. Упомянем лишь, что при его совершении преступники продолжают использовать активнее всего возможности сети Интернет. Данный факт продолжает влиять на латентность преступлений, сложность их выявления, раскрытия и расследования возбужденных уголовных дел.

Итак, если по полномочиям, функциям и задачам следственных и оперативных подразделений ОВД РФ большему числу граждан известна информация, то по Роскомнадзору автор считает необходимым дать некие разъяснения.

Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) – федеральный орган исполнительной власти, в задачи которого входят надзор в сфере связи, информационных технологий и средств массовой информации (СМИ), а также надзор по защите персональных данных согласно закону и деятельность по организации радиочастотной службы. Служба подведомственна Минцифры России. Создана в декабре 2008 г. указом Президента России [1].

О деятельности известно, что в 2019 г. Роскомнадзором разработана Российская национальная система доменных имен [2]. По состоянию на 2021 г. Роскомнадзор обязывает переключать рекурсивные DNS-серверы российских интернет-провайдеров и организаторов распространения информации. Система расположена на MSK-IX и предназначена для обеспечения работы Российского сегмента сети Интернет в случае отключения или изоляции от глобальной сети.

В конце 2015 г. начала использоваться система «Ревизор» – это программно-аппаратный комплекс для осуществления мониторинга сайтов провайдерами и контроля соответствия локальной базы запрещенных сайтов и IP-адресов с реестром. Разработана компанией «МФИ Софт» по заказу Роскомнадзора. После внедрения в работу данной системы в 2017 г. произошел наибольший пик блокировки сайтов службой по решению судов в России [3].

Таким образом, исходя из целей и задач, поставленных перед Роскомнадзором, а также в связи с имеющимися полномочиями у данной организации, можно сделать вывод о том, что это организация, которая может выступать партнером при взаимодействии в борьбе с мошенничествами.

В результате совместной работы органы следствия и дознания могут направлять в Роскомнадзор запросы о предоставлении контактной информации в отношении владельцев интернет-ресурсов, сетевых адресов и электронных почтовых ящиков, а также по вопросам ограничения доступа к сайтам по различным причинам.

Однако автор считает, что некоторые моменты все же необходимо изучить детально, чтобы не переоценить возможности Роскомнадзора по вопросам оказания помощи в борьбе с преступностью.

Так, в 2019 г. руководством указанной выше организации в адрес руководителей структурных подразделений системы МВД России было направлено несколько информационных писем, суть которых состояла в разъяснении функций и полномочий Роскомнадзора при исполнении запросов, поступающих из МВД РФ по расследуемым уголовным делам и материалам предварительной процессуальной проверки, в частности по мошенничествам.

В результате их изучения было установлено, что в Роскомнадзор, а также его территориальные органы периодически поступают запросы и представления территориальных подразделений МВД России о предоставлении контактной информации в отношении владельцев интернет-ресурсов, сетевых адресов и электронных почтовых ящиков, а также по вопросам ограничения доступа к сайтам в сети Интернет, содержащим запрещенную информацию.

В информационном письме указано, что сотрудниками правоохранительных органов неверно понимаются некоторые специализированные понятия, указанные в законодательстве, в связи с чем разъяснены их определения. Так, Роскомнадзор дал разъяснения, что в соответствии со ст. 8 Закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» [4] сайт в информационно-телекоммуникационной сети Интернет может быть зарегистрирован как сетевое издание. Сайт в информационно-телекоммуникационной сети Интернет, не зарегистрированный в качестве средства массовой информации, средством массовой информации как таковым не является. Таким образом, данная регистрация является добровольной и остается на усмотрение владельца сайта. Законодательством Российской Федерации механизм обязательной регистрации интернет-ресурсов не установлен.

Из этого следует, что Роскомнадзор располагает сведениями официального характера относительно владельцев интернет-ресурсов, зарегистрированных в качестве средств массовой информации. В отношении незарегистрированных в качестве СМИ сайтов в сети Интернет Роскомнадзор официальными сведениями об их владельце не располагает.

Кроме этого, исходя из закрепленных законодательством полномочий, Роскомнадзор уполномочен осуществлять контрольно-надзорную деятельность за распространением информационных материалов (в том числе их мониторинг) в зарегистрированных в установленном законом порядке средствах массовой информации. С ними можно ознакомиться самостоятельно на официальном сайте Роскомнадзора: www.rkn.gov.ru/mass-communications/reestr/media/.

Из этого следует, что при возникновении необходимости узнать, относится ли интересующий правоохранительные органы сайт к официально зарегистрированным, по расследуемым уголовным делам, делам оперативного учета и материалам предварительной процессуальной проверки по фактам мошенничеств,

совершенных в сети Интернет, следователям и сотрудникам органа дознания перед составлением и направлением запросов в Роскомнадзор надлежит должным образом самостоятельно обращаться к открытой информации в имеющихся официальных источниках.

В том числе сведения об администраторе доменного имени и провайдере хостинга интернет-ресурса или его сетевом адресе можно уточнить через общедоступные справочные whois-сервисы (например, https://2ip.ru, https://www.nameserver.ru/, https://1whois.ru и др.). Кроме того, такую информацию возможно получить у регистратора соответствующего доменного имени. Администратором национальных доменов верхнего уровня «.RU» и «.РФ» является «Координационный центр национального домена сети Интернет» (https://cctld.ru).

Сведениями в отношении владельцев адресов электронной почты Роскомнадзор также не располагает. Поэтому при подготовке и направлении запросов инициатору следует понимать, что в целях получения данных, указанных интернет-пользователями при регистрации электронной почты, целесообразно обращаться к администрации интернет-ресурса, оказывающего такие услуги.

В контексте запросов, связанных с блокировкой сайтов в сети Интернет, содержащих противоправную информацию, также следует учитывать, что Роскомнадзор является уполномоченным федеральным органом исполнительной власти, осуществляющим ограничение доступа к информации в сети Интернет в рамках реализации ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [5].

Федеральный закон № 149-ФЗ гласит, что к основаниям внесудебного ограничения доступа, определенным ст. 15.1, относится только распространение:

– материалов с порнографическими изображениями несовершеннолетних;

– информации о способах изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств и культивирования наркосодержащих растений;

– информации о способах совершения самоубийств, призывов к совершению самоубийства;

– информации о деятельности по организации и проведению азартных игр и лотерей;

– информации о незаконной розничной продаже дистанционным способом алкогольной продукции.

Как можно видеть, ни один из пунктов не относится к расследуемым ОВД РФ способам мошенничеств. Поэтому требовать в направляемых запросах от Роскомнадзора блокировать определенные интернет-сайты, посредством которых путем обмана и злоупотребления доверием похищались денежные средства под видом продаж товаров и услуг, некорректно.

Кроме того, решение о признании вышеуказанной информации запрещенной к распространению на территории Российской Федерации принимают уполномоченные Правительством Российской Федерации федеральные органы исполнительной власти согласно закрепленным за ними полномочиями (Роскомнадзор, МВД России, Роспотребнадзор, ФНС России, Росалкогольрегулирование соответственно) [6].

Ограничение доступа к сайтам в сети Интернет в соответствии со ст. 15.1 Федерального закона № 149-ФЗ осуществляется также на основании решения суда о признании информации, содержащейся на интернет-ресурсе, запрещенной к распространению на территории нашей страны.

Приведем примеры некорректно составленных запросов в Росфинмониторинг, исполнить которые не представилось возможным по вышеназванным причинам.

Так, в 2018 г. сотрудником отдела уголовного розыска Отдела полиции по Прикубанскому округу УМВД России по городу Краснодару по материалу предварительной процессуальной проверки по факту мошенничества в адрес руководителя Роскомнадзора направлен запрос. Согласно сведениям, указанным в запросе, гражданин П. заказал в сети Интернет на сайте info@gadget-awesome.ru и оплатил покупку мобильного телефона. В связи с вышеизложенным инициатор запроса просил руководителя Роскомнадзора рассмотреть вопрос о блокировке вышеупомянутого сайта с целью недопущения совершения аналогичных мошенничеств в отношении неопределенного количества граждан [7].

В 2019 г. следователь ОРПТО ОП по Центральному округу УМВД России по городу Краснодару при расследовании уголовного дела по факту мошенничества, совершенного посредством интернет-сайта «Телевизор.ру», направил запрос в Роскомнадзор с просьбой предоставить сведения о владельце данного интернет-сайта с указанием анкетных данных лица, дате регистрации и создания сайта, что не входит в полномочия указанной организации [8].

Кроме того, в ходе анализа данного обращения Роскомнадзора установлено, что в адрес указанной организации направляются представления о принятии мер по устранению обстоятельств, способствующих совершению преступления.

Так, в 2019 г. следователем СО Костромского ЛО МВД России на транспорте, в ходе расследования уголовного дела по ч. 4 ст. 159 УК РФ, в адрес руководителя Роскомнадзора было направлено такое представление, из содержания которого следует, что причиной, способствовавшей совершению мошенничества неустановленным лицом, стало то, что оно имело свободный доступ в сети Интернет к сайту «N.ру». Сайт использовлся преступником для обмена текстовыми сообщениями с жертвами преступления и медиафайлами, содержащими фото несуществующих товаров и изделий. В качестве предложений по устранению причин и условий, способствовавших совершению преступлений, следователь предложил указать сотрудникам Роскомнадзора, отвечающим за данную линию работы, на «осуществление более жесткого контроля за электронными ресурсами, находящимися в свободном доступе и информации в них содержащейся» [9].

Исходя из проведенного анализа полномочий Роскомнадзора по исполнению запросов органов предварительного следствия и органов дознания, в том числе по уголовным делам о мошенничествах, совершен-

ных в сфере IT-технологий, можно сделать несколько выводов и практических рекомендаций, которые повлияют на качество уровня взаимодействия и профессионализма сотрудников полиции.

1. Необходимо совершенствование уровня профессиональных знаний и умений у сотрудников следственных и оперативных подразделений, задействованных в выявлении, раскрытии и расследовании мошенничеств рассматриваемой категории. В частности, изучение нормативно-правовой базы, регламентирующей деятельность Роскомнадзора.

2. На постоянной основе проводить занятия с личным составом по вопросам правильности заполнения запросов, направляемых в Роскомнадзор, с изучением структуры запроса, правильного указания наименования организации, адреса ее места нахождения и данных руководителя.

3. При направлении запросов по расследуемым уголовным делам и материалам предварительной процессуальной проверки по фактам совершения мошенничеств с использованием информационно-телекоммуникационных технологий и сети Интернет, необходимо особое внимание уделять полномочиям Роскомнадзора, закрепленным в федеральном законодательстве, не ставить невыполнимые задачи и в связи с их неисполнением исключить факты направления необоснованных представлений. Это поможет сократить сроки ожидания ответов на некорректные запросы и принятые меры по представлениям, тем самым не нарушать принцип разумного срока уголовного судопроизводства, избегая необоснованных продлений сроков проверки и расследования уголовных дел.

4. Перед обращением в Роскомнадзор за получением сведений, имеющих значение для выявления, раскрытия и расследования мошенничеств, сотрудникам ОВД РФ необходимо самостоятельно проводить мониторинг доступной информации о полномочиях указанного органа, а также устанавливать верного исполнителя запросов провайдеров сети и владельцев интернет-сайтов и доменных имен.

Список источников

1. *Указ* Президента Российской Федерации от 03.12.2008 г. № 1715. Kremlin.ru (3 декабря 2008). «О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций» // СПС «КонсультантПлюс» (дата обращения: 13.04.2022).
2. *Об утверждении* Положения о национальной системе доменных имен.rkn.gov.ru // СПС «КонсультантПлюс» (дата обращения: 13.04.2022).
3. *РБК.* Сетевой «Ревизор»: как работает система контроля за запрещенным контентом. URL: http://www.rbc.ru (дата обращения: 13.04.2022).
4. *Федеральный* закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» // СПС «КонсультантПлюс» (дата обращения: 05.05.2022).
5. *Федеральный* закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс» (дата обращения: 05.05.2022).
6. *Постановление* Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе “Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено”» // СПС «КонсультантПлюс» (дата обращения: 05.05.2022).
7. *Архив* уголовных дел Прикубанского районного суда г. Краснодара (дата обращения: 15.04.2022).
8. *Архив* уголовных дел Первомайского районного суда г. Краснодара (дата обращения: 21.04.2022).
9. *Архив* уголовных дел Костромского областного суда (дата обращения: 30.05.2022).

References

1. Consultant Plus. (2006) *Decree of the President of the Russian Federation of December 3, 2008, No. 1715 “On some issues of public administration in the field of communications, information technology and mass communications”.* Moscow: Consultant Plus. (Accessed: 13.04.2022). (In Russian).
2. Consultant Plus. (2006) *Approval of the Regulations on the National System of Domain Names*. Moscow: Consultant Plus. (Accessed: 13.04.2022). (In Russian).
3. RBK. (2022) *Network “Inspector”: how the control system for prohibited content works*. [Online] Available from: http://www.rbc.ru (Accessed: 13.04.2022). (In Russian).
4. Consultant Plus. (1991) *Federal Law of the Russian Federation of December 27, 1991, No. 2124-1 “On Mass Media”*. Moscow: Consultant Plus. (Accessed: 05.05.2022). (In Russian).
5. Consultant Plus. (2006) *Federal Law of July 27, 2006, No. 149-FZ “On Information, Information Technologies and Information Protection”*. Moscow: Consultant Plus. (Accessed: 05.05.2022). (In Russian).
6. Consultant Plus. (2012) *Decree of the Government of the Russian Federation of October 26, 2012, No. 1101 “On a unified automated information system Unified Register of the Domain Names, Website References and Network Addresses That Allow Identifying Websites Containing Information Circulation of Which Is Forbidden in the Russian Federation”.* Moscow: Consultant Plus. (Accessed: 05.05.2022). (In Russian).
7. Archive of Criminal Cases of the Pervomaisky District Court of Krasnodar. (Accessed: 15.04.2022). (In Russian).
8. Archive of Criminal Cases of the Pervomaisky District Court of Krasnodar. (Accessed: 21.04.2022). (In Russian).
9. Archive of Criminal Cases of the Kostroma Regional Court. (Accessed: 30.05.2022). (In Russian).

Информация об авторе:
Ханинева О.В. – старший преподаватель кафедры уголовного процесса Краснодарского университета Министерства внутренних дел Российской Федерации (Краснодар, Россия). E-mail: post_krdu@mvd.ru

Автор заявляет об отсутствии конфликта интересов.

Information about the author:
O.V. Khanineva, senior lecturer, Department of Criminal Procedure, Krasnodar University of the Ministry of Internal Affairs of Russia (Krasnodar, Russia). E-mail: post_krdu@mvd.ru

The author declares no conflicts of interests.

Статья поступила в редакцию 1.11.2022;
одобрена после рецензирования 17.11.2022; принята к публикации 12.12.2022.

The article was submitted 1.11.2022;
approved after reviewing 17.11.2022; accepted for publication 12.12.2022.

.