Полицейская деятельность
Правильная ссылка на статью:
Количенко А.А., Мушаков В.Е., Грачева О.А. Особенности обеспечения конфиденциальности сведений о защищаемом участнике уголовного процесса в условиях цифровизации // Полицейская деятельность. 2024. № 4. DOI: 10.7256/2454-0692.2024.4.71325 EDN: RRTPAI URL: https://nbpublish.com/library_read_article.php?id=71325

Особенности обеспечения конфиденциальности сведений о защищаемом участнике уголовного процесса в условиях цифровизации

Количенко Артем Андреевич

ORCID: 0000-0002-1962-197X

кандидат юридических наук

преподаватель; кафедра криминалистики; Нижегородская академия МВД России

603950, Россия, Нижегородская область, г. Нижний Новгород, Анкудиновское шоссе, 3

kolichenkoaa@mail.ru

Мушаков Виталий Евгеньевич

преподаватель; кафедра деятельности органов внутренних дел в особых условиях; Омская академия МВД России

644092, Россия, Омская область, г. Омск, пр-т Комарова, 7

mushakov.2018@mail.ru

Грачева Олеся Александровна

старший преподаватель; кафедра криминалистики; Нижегородская академия МВД России

603950, Россия, Нижегородская область, г. Нижний Новгород, Анкудиновское шоссе, 3

olesya_leushkina@mail.ru

Статья из рубрики "Актуальный вопрос"

DOI:

10.7256/2454-0692.2024.4.71325

EDN:

RRTPAI

Дата направления статьи в редакцию:

22-07-2024

Дата публикации:

29-07-2024

Аннотация: Применение информационных технологий, бесспорно, является катализатором развития общества и государства, но в тоже время порождает определенные риски защиты персональных данных рядовых граждан, в том числе граждан-участников уголовного судопроизводства. Настоящая статья посвящена нарастающей и требующей особого внимания – проблеме обеспечения конфиденциальности сведений о защищаемом участнике уголовного судопроизводства в условиях цифровизации. Названная проблема видится актуальной ввиду того, что граждане, зачастую, самостоятельно предают гласности различные аспекты своей повседневной жизни, размещая информацию о себе в сети «Интернет», включая публикацию текстовых, фото- и видеоматериалов и т.п. По данной причине в целях обеспечения конфиденциальности сведений о защищаемом лице в условиях цифровизации особой актуальностью обладает изъятие из публичного доступа персональных данных, позволяющих установить личность защищаемого участника уголовного судопроизводства. В статье проанализированы положения нормативных правовых актов, регулирующих правоотношения в сфере государственной защиты участников уголовного судопроизводства. Методологическая основа исследования представлена, первоочередно, диалектическим методом познания; авторами статьи применялись общенаучные методы исследования (анализ, синтез, дедукция, индукция, формально-логический, прогнозирования) и частнонаучные методы исследования (статистический и формально-юридический). В статье рассмотрены актуальные проблемы обеспечения конфиденциальности сведений о защищаемом участнике уголовного судопроизводства. Особое внимание уделено недостаточной эффективности действующего механизма изъятия из сети «Интернет» информации о защищаемом лице. Делается акцент на распространенности и широкодоступности теневых сегментов виртуальной среды как проблеме обеспечения конфиденциальности сведений защищаемых лиц. По результатам исследования авторы статьи пришли к выводу о неразрешимости в современных условиях задачи изъятия из публичного доступа исчерпывающего объема персональных данных, в связи с чем следует стремиться к минимизации возможностей раскрытия конфиденциальных сведений о защищаемых лицах посредством сети «Интернет». Авторы предлагают в целях обеспечения конфиденциальности сведений защищаемого участника уголовного судопроизводства следователю, дознавателю или прокурору, инициировавшим применение рассматриваемой меры безопасности, осведомлять участников уголовного судопроизводства о необходимости принятия самостоятельных мер к удалению цифровых следов в сети «Интернет».

Ключевые слова:

уголовное судопроизводство, цифровизация, персональные данные, информационная безопасность, следователь, взаимодействие, правоохранительная деятельность, свидетель, потерпевший, идентификация личности

Введение. В современных условиях научно-технического прогресса в информационно-телекоммуникационной сети «Интернет» накоплен массив сведений, позволяющий тем или иным образом идентифицировать граждан, либо получить о них иную необходимую информацию. Так, только по предварительным подсчетам в 2023 году в сети было

незаконно размещено 1,12 млрд. персональных данных, что почти на 60% выше показателя 2022-го года [1]. А, к примеру, по данным Роскомнадзора уже в 2024 году за один случай в сети было незаконно размещено 500 млн. данных россиян [2]. Распространенность публичной информационной сети, а также доступность транслируемого ею контента, обуславливают возникновение проблем в сфере охраны прав и свобод человека и гражданина в уголовном судопроизводстве, что, в свою очередь, может поставить под угрозу реализацию положения, закрепленного в статье 2 Конституции Российской Федерации – «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства»[1].

Складывающаяся ситуация требует решительных действий. Как минимум, необходима проработка вопроса о том, как в таких условиях обеспечить безопасность участников уголовного судопроизводства, на которых может быть оказано как физическое, так и психологическое воздействие. И в первом, и во втором случаях это может стать возможным вследствие получения заинтересованными лицами-злоумышленниками из сети «Интернет» (в т.ч. из соответствующих баз данных) персональных данных о месте рождения человека, адресе регистрации и проживания, сведениях о страницах в социальных сетях и пр. – т.е. тех сведений, которые позволят оказать влияние на человека, например: оказать психологическое давление на человека, а именно запугать его через сообщения в мессенджерах и социальных сетях. Усугубляет ситуацию и тот факт, что «каждый день, каждый час умные устройства, социальные сети и поисковые системы собирают личную информацию пользователей … банковские, страховые, медицинские организации также требуют предоставления персональных данных для оказания услуг» [3, с. 101].

Обзор литературы. Представленное к обозрению направление является малоисследованным, несмотря на многократное увеличение трудов ученых-процессуалистов о рисках и преимуществах цифровизации применительно к уголовному судопроизводству.

На недостаточную исследованность, во-первых, указывает факт отсутствия исследований монографического уровня, и, во-вторых, наличие единичных публикаций, тем или иным образом затрагивающих тему обеспечения конфиденциальности сведений о защищаемом участнике уголовного процесса в условиях цифровизации. Обозначим некоторые из них.

Так, одной из таких публикаций является работа Р.М. Рамазанова, в которой акцент делается на использовании информационных технологий при обеспечении безопасности участников уголовного процесса. Однако, по результатам исследования названный автор, лишь констатирует факт наличия проблем, связанных с обеспечением информационной безопасности лиц, участвующих в уголовном судопроизводстве [4, с. 620].

Также следует обратить внимание на статью Н.О. Никурадзе, рассуждающей об обеспечении кибербезопасности данных при применении электронных средств обработки и хранения информации в сфере уголовного судопроизводства. По заверению Натальи Олеговны эффективность защиты информации в электронном виде, включая процесс её обработки, хранения и передачи, «прямо пропорциональная качеству расследования и разрешения уголовного дела по существу, а также обеспечению защиты прав и законных интересов участников уголовного процесса» [5, с. 137].

О порождении проблемы обеспечения защиты персональных данных участников уголовного процесса известно из исследования Н.В. Софийчук и Л.А. Колпаковой – но лишь в том случае, если на сайтах судов будут размещаться записи веб-заседаний (что по уверению названных ученых уже практикуется) [6, с. 76].

Материалы и методы. В статье проанализированы положения нормативных правовых актов, регулирующих правоотношения в сфере государственной защиты участников уголовного судопроизводства. Методологическая основа исследования представлена, первоочередно, диалектическим методом познания; авторами статьи применялись общенаучные методы исследования (анализ, синтез, дедукция, индукция, формально-логический, прогнозирования) и частнонаучные методы исследования (статистический и формально-юридический).

Результаты исследования. Во избежание случаев применения физического и психологического воздействия на потерпевших и свидетелей в целях изменения содержания их показаний, либо отказа от дачи показаний по уголовному делу, законодательством Российской Федерации предусмотрено осуществление процессуальных и непроцессуальных мероприятий, обеспечивающих безопасность участников уголовного процесса. Так, при наличии достаточных данных о том, что участникам уголовного судопроизводства, их близким родственникам и близким лицам угрожают убийством, применением насилия, уничтожением или повреждением их имущества либо иными опасными противоправными деяниями, суд, прокурор, а также должностные лица органов следствия или дознания вправе применить в отношении указанных лиц меры безопасности, что следует из ч. 3 ст. 11 Уголовного-процессуального кодекса Российской Федерации (далее – УПК РФ)[2].

Актуальность применения мер безопасности в сфере уголовно-процессуальных отношений подтверждается статистическими данными, представленными Правительством Российской Федерации. Так, в период с 2006 по 2022 г. в отношении 39 тыс. защищаемых лиц осуществлено более 94 тыс. мер безопасности, среди которых приоритетными выступили личная охрана, охрана жилища и имущества, выдача специальных средств индивидуальной защиты, связи и оповещения об опасности, обеспечение конфиденциальности сведений о защищаемом лице, а также временное помещение в безопасное место[3].

Обеспечение конфиденциальности сведений о защищаемом лице в качестве меры безопасности участников уголовного судопроизводства указано в п. 4 ст. 5 Федерального закона от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»[4] и п. 3 ч. 1 ст. 6 Федерального закона от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»[5] (далее – Федеральный закон № 119). При этом в ч. 1 ст. 9 Федерального закона № 119 раскрывается следующий перечень мер, направленных на сохранение конфиденциальности участников уголовного судопроизводства:

1) «запрет на распространение информации, содержащей сведения о защищаемом лице (персональные данные), выдачу находящихся у оператора сведений о защищаемом лице (персональных данных);

2) замена абонентских номеров телефонов защищаемого лица и государственных регистрационных знаков используемых им или принадлежащих ему транспортных

средств»[6].

В правоприменительной практике обеспечение конфиденциальности сведений о защищаемом лице осуществляется посредством изъятия из публичного доступа его персональных данных, что является гарантией сохранения в тайне личности участника уголовного судопроизводства. В системе МВД России органом, ответственным за реализацию рассматриваемой меры безопасности лица, вовлеченного в орбиту уголовно-процессуальных отношений, является Управление по обеспечению безопасности лиц, подлежащих государственной защите (далее – УОГЗ МВД России). Наделенные правоприменительными полномочиями территориальные подразделения УОГЗ МВД России осуществляют оперативно-розыскные и иные мероприятия в целях защиты жизни, здоровья лиц, подлежащих государственной защите, а также обеспечения сохранности их имущества.

Подразделения УОГЗ МВД России в целях реализации возложенных на них обязанностей вправе самостоятельно определять меры безопасности, необходимые для обеспечения государственной защиты участников уголовного процесса. Вместе с тем, Правилами осуществления мер безопасности в виде обеспечения конфиденциальности сведений о защищаемом лице, утвержденными Постановлением Правительства РФ от 14.07.2015 № 705 (далее – Постановление Правительства РФ № 705)[7], предусмотрен механизм изъятия персональных данных защищаемого лица из публичного доступа, как в материальной, так и в виртуальной среде.

Основываясь на материалах, представленных органами следствия, дознания, прокуратуры или суда, должностные лица подразделений УОГЗ МВД России выносят мотивированное постановление о применении меры безопасности в виде обеспечения конфиденциальности сведений в отношении защищаемого лица и вручают его руководителям организаций (учреждений), которые могут обладать такими сведениями. В современных условиях указанными организациями являются различные операторы персональных данных, располагающие информационно-справочными системами (базами и банками данных, картотеками, архивами, реестрами, справочниками), содержащими представленные на материальных и оцифрованных носителях сведения о защищаемом лице.

В каждом конкретном случае перечень рассматриваемых организаций самостоятельно определяется подразделениями УОГЗ МВД России в границах обслуживаемой территории, и, как правило, включает многофункциональные центры предоставления государственных и муниципальных услуг, кредитные организации, операторов сотовой связи, паспортные службы, органы публичной власти, государственные и муниципальные предприятия и учреждения. Удалению и анонимизации подлежат, в частности, установочные данные о лице (его фамилия, имя, отчество, дата рождения и т.п.), контактная информация (мобильный и рабочий телефоны, адреса места жительства, работы и обучения), сведения об основных документах (паспорт гражданина РФ, заграничный паспорт, водительское удостоверение, страховое свидетельство государственного пенсионного страхования, свидетельство ИНН, документы об образовании и др.), биографические сведения (место рождения, обучения, работы и др.). С момента получения мотивированного постановления оператор персональных данных обязуется не только скрыть из обрабатываемых им источников информацию о защищаемом лице, но и ограничить выдачу указанной информации третьим лицам.

Учитывая, что в современную эпоху среди граждан зачастую принято самостоятельно предавать гласности различные аспекты своей повседневной жизни, виртуальная среда

стала первоочередным источником получения каких-либо сведений, позволяющих их идентифицировать. По данной причине в целях обеспечения конфиденциальности сведений о защищаемом лице в условиях цифровизации особой актуальностью обладает изъятие из публичного доступа персональных данных, опосредуемых в сети «Интернет»: данные аккаунтов мессенджеров (WhatsApp, Telegram), привязанных к контактному телефону; цифровых коммуникаций (личные и корпоративные электронные письма, телефонные звонки); банковских транзакций; используемых онлайн-приложений, требующих верификации клиента; данные пользователя социальной сети; опубликованные текстовые, фото- и видеоматериалы; а также иные «цифровые» следы. Нахождение в виртуальной среде перечисленных сведений, позволяющих установить личность свидетеля и потерпевшего по уголовному делу, угрожает их физической и психической безопасности, а также сохранности имущества.

Удаление исчерпывающего объема информации о защищаемом лице зависит от технических возможностей органов, обеспечивающих их безопасность. По этой причине п. 9.5 Постановления Правительства РФ № 705 предусматривает порядок взаимодействия УОГЗ МВД России с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Подразделения УОГЗ МВД России самостоятельно определяют перечень доменных имен, сетевых адресов и указателей страниц сайтов в сети «Интернет», содержащих сведения о защищаемом лице, и направляют его в Роскомнадзор. Последний вносит указанные Интернет-ресурсы в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено[8].

Кроме того, в целях удаления персональных данных защищаемого лица необходимо направлять запросы в администрацию социальной сети «ВКонтакте», наиболее востребованной среди российских граждан. Информация о пользователе социальной сети включает данные его цифрового профиля, текстовые и аудио-сообщения, а также аудио-, фото- и видео-материалы, имеющиеся в свободном доступе и позволяющие идентифицировать защищаемое лицо. Тем самым, обеспечивается конфиденциальность сведений о защищаемом лице в данном сегменте виртуальной среды.

Несмотря на взаимодействие подразделений УОГЗ МВД России с Роскомнадзором и администрациями социальных сетей, в настоящее время механизм изъятия из сети «Интернет» информации о защищаемом лице является недостаточно эффективным.

Во-первых, технология VPN позволяет пользователю установить зашифрованное соединение с сайтом в сети «Интернет» и, тем самым, обойти блокировки виртуальных ресурсов, запрещенных Роскомнадзором.

Во-вторых, в информационной сети функционируют различные виртуальные ресурсы, позволяющие на коммерческой основе получить персональные данные о гражданах РФ, в том числе являющихся участниками уголовного судопроизводства. Так, по исковому заявлению Роскомнадзора Решением Таганского районного суда Москвы от 01.07.2021 деятельность интернет-ресурса «https://t.me/eogdatabotbot» признана незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну[9].

В настоящее время Роскомнадзор в ходе мониторинга сети «Интернет» и рассмотрения обращения граждан на нарушение их прав в сфере обработки персональных данных

продолжает выявлять Telegram-боты, которые предоставляют неограниченному кругу лиц доступ к персональным данным без согласия их владельцев. Однако после блокировки подобные Telegram-боты систематически пересоздаются, поскольку на фоне спроса среди граждан приносят их администраторам денежную выгоду.

Обсуждение и заключения. Учитывая изложенное, распространенность и широкодоступность теневых сегментов виртуальной среды представляет проблему обеспечения конфиденциальности сведений защищаемых лиц.

В обозначенных условиях задача изъятия из публичного доступа исчерпывающего объема персональных данных представляется неразрешимой. Поэтому необходимо стремиться к минимизации возможностей раскрытия конфиденциальных сведений о защищаемых лицах посредством сети «Интернет».

Помимо проводимых непроцессуальных мероприятий по обеспечению конфиденциальности сведений защищаемых лиц со стороны УОГЗ МВД России и Роскомнадзора, защищаемое лицо, располагая информацией об оставленных «цифровых» следах, может самостоятельно принять меры к их удалению из виртуальной среды. Об этом следователю, дознавателю или прокурору, инициировавшим применение рассматриваемой меры безопасности, целесообразно осведомлять участников уголовного судопроизводства.

Таким образом, в условиях цифровизации общества при применении меры безопасности в виде обеспечения конфиденциальности сведений участников уголовного судопроизводства требуется изъятие информации, позволяющей идентифицировать их не только в материальной, но и виртуальной среде. Учитывая динамическое развитие теневых сегментов сети «Интернет», затруднительно изъятие всего массива персональных данных защищаемых лиц.

[1] Конституция Российской Федерации: принята 12 декабря 1993 года всенародным голосованием (с изменениями, внесенным Законом Российской Федерации о поправках к Конституции РФ от 14 марта 2020 г. № 1-ФКЗ и одобренными в ходе общероссийского голосования 1 июля 2020 года) // СПС «КонсультантПлюс».

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 22.04.2024) (с изм. и доп., вступ. в силу с 15.05.2024) // СПС «КонсультантПлюс».

[3] Постановление Правительства РФ от 06.09.2023 № 1454-47 «Об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2024 - 2028 годы» (вместе с «Государственной программой «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2024 - 2028 годы» // СПС «КонсультантПлюс».

[4] Федеральный закон от 20.04.1995 № 45-ФЗ (ред. от 25.12.2023) «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» // СПС «КонсультантПлюс».

[5] Федеральный закон от 20.08.2004 № 119-ФЗ (ред. от 01.07.2021) «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» // СПС «КонсультантПлюс».

[6] Там же.

[7] Постановление Правительства РФ от 14.07.2015 № 705 (ред. от 17.09.2022) «О порядке защиты сведений об осуществлении государственной защиты, предоставления таких сведений и осуществления мер безопасности в виде обеспечения конфиденциальности сведений о защищаемом лице» // СПС «КонсультантПлюс».

[8] Подробнее см.: URL: https://eais.rkn.gov.ru/ (дата обращения: 06.05.2024).

[9] Решение Таганского районного суда г. Москва от 01 июля 2021 г. по делу № 02-2418/2021 // URL: https://clck.ru/3AyQf7 (дата обращения: 20.05.2024).

Библиография

1. Аналитики оценили рост утечек персональных данных в России. URL: https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9 (дата обращения: 28.05.2024).
2. Роскомнадзор сообщил об утечке 500 млн. данных о россиянах за один раз. URL: https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3 (дата обращения: 29.05.2024).
3. Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2020. № 4. С 100-108.
4. Рамазанов Р.М. Использование информационных технологий при обеспечении безопасности участников уголовного процесса // Вестник Казанского юридического института МВД России. 2021. № 4 (46). С. 616-622.
5. Никурадзе Н.О. К вопросу об обеспечении кибербезопасности данных при применении электронных средств обработки и хранения информации в сфере уголовного судопроизводства // Право и государство: теория и практика. 2021. № 11 (203). С. 134-137.
6. Софийчук Н.В., Колпакова Л.А. К вопросу о доступе граждан к правосудию в условиях цифровизации уголовного судопроизводства // Lex russica. 2020. № 11. С. 71-80.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье являются, как это следует из ее наименования, особенности обеспечения конфиденциальности сведений о защищаемом участнике уголовного процесса в условиях цифровизации. Заявленные границы исследования соблюдены авторами.
Методология исследования раскрыта: "Методологическая основа исследования представлена, первоочередно, диалектическим методом познания; авторами статьи применялись общенаучные методы исследования (анализ, синтез, дедукция, индукция, формально-логический, прогнозирования) и частнонаучные методы исследования (статистический и формально-юридический)".
Актуальность избранной авторами темы исследования не подлежит сомнению и обосновывается ими следующим образом: "В современных условиях научно-технического прогресса в информационно-телекоммуникационной сети «Интернет»

накоплен массив сведений, позволяющий тем или иным образом идентифицировать граждан, либо получить о них иную необходимую информацию. Так, только по предварительным подсчетам в 2023 году в сети было незаконно размещено 1,12 млрд. персональных данных, что почти на 60% выше показателя 2022-го года [1]. А, к примеру, по данным Роскомнадзора уже в 2024 году за один случай в сети было незаконно размещено 500 млн. данных россиян [2]. Распространенность публичной информационной сети, а также доступность транслируемого ею контента, обуславливают возникновение проблем в сфере охраны прав и свобод человека и гражданина в уголовном судопроизводстве, что, в свою очередь, может поставить под угрозу реализацию положения, закрепленного в статье 2 Конституции Российской Федерации – «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства»[1]. Складывающаяся ситуация требует решительных действий. Как минимум, необходима проработка вопроса о том, как в таких условиях обеспечить безопасность участников уголовного судопроизводства, на которых может быть оказано как физическое, так и психологическое воздействие" и др. Ученые раскрывают степень изученности поднимаемых в статье проблем: "Представленное к обозрению направление является малоисследованным, несмотря на многократное увеличение трудов ученых-процессуалистов о рисках и преимуществах цифровизации применительно к уголовному судопроизводству. На недостаточную исследованность, во-первых, указывает факт отсутствия исследований монографического уровня, и, во-вторых, наличие единичных публикаций, тем или иным образом затрагивающих тему обеспечения конфиденциальности сведений о защищаемом участнике уголовного процесса в условиях цифровизации" и т.д.

Научная новизна работы проявляется в ряде заключений авторов: "Основываясь на материалах, представленных органами следствия, дознания, прокуратуры или суда, должностные лица подразделений УОГЗ МВД России выносят мотивированное постановление о применении меры безопасности в виде обеспечения конфиденциальности сведений в отношении защищаемого лица и вручают его руководителям организаций (учреждений), которые могут обладать такими сведениями. В современных условиях указанными организациями являются различные операторы персональных данных, располагающие информационно-справочными системами (базами и банками данных, картотеками, архивами, реестрами, справочниками), содержащими представленные на материальных и оцифрованных носителях сведения о защищаемом лице.В каждом конкретном случае перечень рассматриваемых организаций самостоятельно определяется подразделениями УОГЗ МВД России в границах обслуживаемой территории, и, как правило, включает многофункциональные центры предоставления государственных и муниципальных услуг, кредитные организации, операторов сотовой связи, паспортные службы, органы публичной власти, государственные и муниципальные предприятия и учреждения. Удалению и анонимизации подлежат, в частности, установочные данные о лице (его фамилия, имя, отчество, дата рождения и т.п.), контактная информация (мобильный и рабочий телефоны, адреса места жительства, работы и обучения), сведения об основных документах (паспорт гражданина РФ, заграничный паспорт, водительское удостоверение, страховое свидетельство государственного пенсионного страхования, свидетельство ИНН, документы об образовании и др.), биографические сведения (место рождения, обучения, работы и др.). С момента получения мотивированного постановления оператор персональных данных обязуется не только скрыть из обрабатываемых им источников информацию о защищаемом лице, но и ограничить выдачу указанной информации третьим лицам" ; "Кроме того, в целях удаления

персональных данных защищаемого лица необходимо направлять запросы в администрацию социальной сети «ВКонтакте», наиболее востребованной среди российских граждан. Информация о пользователе социальной сети включает данные его цифрового профиля, текстовые и аудио-сообщения, а также аудио-, фото- и видео-материалы, имеющиеся в свободном доступе и позволяющие идентифицировать защищаемое лицо. Тем самым, обеспечивается конфиденциальность сведений о защищаемом лице в данном сегменте виртуальной среды. Несмотря на взаимодействие подразделений УОГЗ МВД России с Роскомнадзором и администрациями социальных сетей, в настоящее время механизм изъятия из сети «Интернет» информации о защищаемом лице является недостаточно эффективным.

Во-первых, технология VPN позволяет пользователю установить зашифрованное соединение с сайтом в сети «Интернет» и, тем самым, обойти блокировки виртуальных ресурсов, запрещенных Роскомнадзором. Во-вторых, в информационной сети функционируют различные виртуальные ресурсы, позволяющие на коммерческой основе получить персональные данные о гражданах РФ, в том числе являющихся участниками уголовного судопроизводства" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан авторами в полной мере.

Структура работы вполне логична. Во вводной части статьи ученые обосновывают актуальность избранной ими темы исследования. В основной части работы авторы рассматривают проблему обеспечения конфиденциальности сведений о защищаемом участнике уголовного процесса в условиях цифровизации и предлагают пути ее решения. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию и не вызывает особых нареканий.

Библиография исследования представлена 6 источниками (научными статьями, аналитическими и статистическими материалами), не считая нормативного и эмпирического материалов. В целом авторам удалось раскрыть тему исследования с необходимой глубиной и полнотой.

Апелляция к оппонентам имеется, но носит общий характер в силу направленности исследования. Научная дискуссия ведется авторами корректно. Положения работы обоснованы в должной степени и проиллюстрированы примерами.

Выводы по результатам проведенного исследования имеются ("Учитывая изложенное, распространенность и широкодоступность теневых сегментов виртуальной среды представляет проблему обеспечения конфиденциальности сведений защищаемых лиц.

В обозначенных условиях задача изъятия из публичного доступа исчерпывающего объема персональных данных представляется неразрешимой. Поэтому необходимо стремиться к минимизации возможностей раскрытия конфиденциальных сведений о защищаемых лицах посредством сети «Интернет». Помимо проводимых непроцессуальных мероприятий по обеспечению конфиденциальности сведений защищаемых лиц со стороны УОГЗ МВД России и Роскомнадзора, защищаемое лицо, располагая информацией об оставленных «цифровых» следах, может самостоятельно принять меры к их удалению из виртуальной среды. Об этом следователю, дознавателю или прокурору, инициировавшим применение рассматриваемой меры безопасности, целесообразно осведомлять участников уголовного судопроизводства.

Таким образом, в условиях цифровизации общества при применении меры безопасности в виде обеспечения конфиденциальности сведений участников уголовного судопроизводства требуется изъятие информации, позволяющей идентифицировать их не только в материальной, но и виртуальной среде. Учитывая динамическое развитие

теневых сегментов сети «Интернет», затруднительно изъятие всего массива персональных данных защищаемых лиц"), обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного процесса.