Александр Николаевич ПЕРШИН,
профессор кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА) доктор юридических наук, доцент
an.pershin75@yandex.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ЦИФРОВЫЕ ПРАВА ЛИЦ, ОСУЩЕСТВЛЯЮЩИХ ПРЕДВАРИТЕЛЬНОЕ РАССЛЕДОВАНИЕ

Аннотация. *Появление сети Интернет и нематериальных цифровых объектов, представляющих ценность для человека, привело к появлению в гражданском материальном праве понятия «цифровые права человека». В уголовно-процессуальном праве данный термин отсутствует. При этом следователь собирает сведения об обстоятельствах, подлежащих доказыванию по уголовному делу в условиях цифровизации всех процессов жизнедеятельности человека. Сеть Интернет объединила множество информационных массивов данных государственных органов, коммерческих организаций и частных лиц. Доступ следователя к этим массивам данных и их изучение позволили бы оптимизировать деятельность следователя путем оперативного сбора необходимых сведений для уголовного дела и использования их в качестве доказательств. С этой целью в статье дано понятие «цифровые права следователя», предложен подход к созданию таких прав в уголовно-процессуальном законодательстве, определены проблемы организации собирания криминалистически значимых сведений из государственных и частных информационных систем в сети Интернет.*
Ключевые слова: *цифровые права следователя, информационные системы, электронные доказательства, следователь, сеть Интернет, поиск информации, расследование, цифровая информация в уголовном процессе.*

DOI: 10.17803/2311-5998.2021.78.2.108-115

A. N. PERSHIN,
Professor of the Department of Criminalistics of the Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Associate Professor
an.pershin75@yandex.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, 9

DIGITAL RIGHTS PERSONS CARRYING OUT A PRELIMINARY INVESTIGATION

Abstract. *The emergence of the Internet and intangible digital objects of value to humans led to the proclamation of the concept of "digital human rights" in civil substantive law. In criminal procedure law this term is not absent. In this case, the investigator collects information about the circumstances to be proved in a criminal case under the conditions of digitalization of all human life processes. The Internet network has combined a large number of data sets of government agencies, commercial organizations, and individuals. The*

investigator's access to these data sets and their study would allow optimizing the investigator's activities by quickly collecting the necessary information for the criminal case and using it as evidence. To this end, the article gives the concept of" digital rights " of an investigator, suggests an approach to creating such rights in criminal procedure legislation, and defines the problems of organizing the collection of criminally significant information from public and private information systems on the Internet.
Keywords: *digital rights of the investigator, information systems, electronic evidence, investigator, the Internet, information retrieval, investigation, digital information in criminal proceedings.*

XXI век — это эпоха цифровых технологий. Человечество охвачено процессами оптимизации всех сфер деятельности при помощи использования информационных технологий. Особенно показательным стал 2020 г., на долю которого выпало общемировое испытание пандемией от коронавирусной инфекции COVID-19. Вследствие этого введенный временный режим закрытия государственных границ, приостановление деятельности организаций, учреждений и предприятий, самоизоляция населения только усилили цифровизацию общества.

Широкое внедрение и использование таких цифровых активов, как криптовалюта, токены, объекты интеллектуальной собственности, электронные страховые полисы, бездокументарные акции, и других объектов в электронной форме невозможно без создания различных групп правовых норм, регулирующих общественные отношения в сфере информации, информационных технологий и защиты информации. Разработка таких норм в отечественном праве началась задолго до 2020 г. Однако лишь в 2019 г. в материальном праве появился термин «цифровые права», которыми признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам[1].

Цифровые активы в широком смысле представляют собой все, что может быть отнесено к информационным объектам, имеет нематериальную (бестелесную) природу, сохранено в электронном виде и имеет ценность[2].

Масштабные высокотехнологические процессы в стране, а также появление нового института цифровых прав в гражданском законодательстве заставляет обратиться к проблеме рассмотрения цифровых прав в рамках уголовного процесса, а именно касающихся лиц, осуществляющих предварительное расследование. При этом отметим, что стремительная цифровизация общества, вызванная как

[1] Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СПС «КонсультантПлюс».

[2] *Овчинников А. И., Фатхи В. И.* Цифровые права как объекты гражданских прав // Философия права. 2019. № 3 (90). С. 107.

естественными, так и чрезвычайными обстоятельствами, не оказывает сильного и позитивного влияния на уголовно-процессуальное право.

Отечественное уголовно-процессуальное законодательство допускает использование информационно-телекоммуникационных технологий лишь в редких случаях. Цифровые технологии используются в качестве вспомогательного средства процессуального получения доказательств, например, в судебном заседании применяются системы видео-конференц-связи для проведения допросов (ч. 4 ст. 240 УПК РФ).

Технологии являются объектом, на который в качестве меры пресечения по судебному решению возлагается запрет на использование подозреваемым (обвиняемым), речь идет о средствах связи и информационно-телекоммуникационной сети Интернет (п. 5 ч. 6 ст. 105.1 УПК РФ). Иногда такие технологии используются в качестве средства распространения данных предварительного расследования через информационно-телекоммуникационную сеть Интернет (п. 2 ч. 4 ст. 161 УПК РФ) или трансляции открытого судебного заседания (ч. 5 ст. 241 УПК РФ).

Цифровые технологии позволили создать информационную область размещения обращений государственных органов, органов местного самоуправления, иных органов, организаций, должностных лиц или граждан в суд (ч. 3 ст. 8.1 УПК РФ). Кроме того, сеть Интернет в уголовном судопроизводстве может использоваться как технологическая система, предназначенная для подачи в суд непроцессуальных электронных документов в виде ходатайств, заявлений, жалоб, представлений и материалов, приложенных к ним, а также для направления судом копии судебного решения участнику уголовного судопроизводства (ст. 474.1 УПК РФ).

Анализ норм Уголовно-процессуального кодекса РФ показал, что информационно-телекоммуникационные технологии получили свое скромное распространение в значительной степени лишь в стадиях судебного производства по уголовному делу или как средство обеспечения деятельности суда. На досудебных стадиях IT-технологиям практически не уделяется внимание и уж тем более не говорится о цифровых правах следователя (дознавателя). Вместе с тем лицу, осуществляющему предварительное расследование, приходится собирать доказательства и иные сведения в условиях функционирования широкой сети государственных информационных систем, повсеместного использования цифровых технологий обществом и преступной средой. В этой связи тема цифровых прав следователя (дознавателя) при собирании доказательств весьма актуальна.

Рассмотрение потенциальной возможности наделения следователя (дознавателя) цифровыми правами было бы невозможным без провозглашения в законодательстве таких принципов регулирования отношений в сфере информации, как свобода поиска, получения, передачи, производства и распространения информации любым законным способом; открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации; достоверность информации и своевременность ее предоставления; неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (ст. 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об

информации, информационных технологиях и о защите информации»; далее — Закон об информации).

Цифровое право в упрощенном виде — это право, которое предусмотрено информационной системой. В соответствии со ст. 2 Закона об информации под информационной системой понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Поэтому содержание и условия осуществления цифровых прав следователя или дознавателя будет определять именно информационная система, к которой имеют доступ указанные лица, а закон только установит ее признаки. Система может быть государственной, региональной, местной или частной. Доступ к информационной системе может быть открытым (т.е. информационный контент доступен неограниченному кругу пользователей системы) либо закрытым (т.е. ограничен для большинства пользователей).

Закон гарантирует следователю (дознавателю) процессуальную самостоятельность и предоставляет свободу выбора действий по собиранию доказательств с учетом конкретных обстоятельств дела. Такими доказательствами могут быть сведения, размещенные обладателем информации в информационной системе. Федеральный закон об информации наделяет граждан и юридических лиц правом осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных федеральным законодательством в сфере информации, информационных технологий и защиты информации. В этой связи цифровое право лиц, осуществляющих предварительное расследование, следует рассматривать как *право следователя (дознавателя) осуществлять поиск, изучение, фиксацию криминалистически значимой информации в информационно-телекоммуникационных системах, а также подтверждать правомерность ее получения и использования в качестве доказательств.*

Реализация «цифровых прав» следователя (дознавателя) при осуществлении им деятельности по раскрытию и расследованию преступления может быть связана с функционированием информационных систем, условно разделенных на две группы:

1) системы (банки данных, реестры) оперативно-справочной, розыскной, криминалистической, статистической, научно-технической и иной информации правоохранительных органов (например: информационных центров территориальных органов МВД России) и иных государственных органов и органов местного самоуправления (например, Единый государственный реестр недвижимости (ЕГРН); Единый государственный реестр записей актов гражданского состояния, Единый государственный реестр налогоплательщиков и проч.), создание которых обязательно;
2) системы негосударственных юридических лиц, индивидуальных предпринимателей и физических лиц, создание и ведение которых определяется их обладателем.

Информационные системы (банки данных, реестры) государственных органов исполнительной власти (в том числе правоохранительных органов) и органов местного самоуправления формируются в соответствии с федеральным, региональным и местным законодательством. Так, во исполнение Федерального

закона от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» на интернет-ресурсах государственных органов и органов местного самоуправления размещаются информационные системы, банки данных, реестры, регистры, находящиеся в ведении государственного органа, органа местного самоуправления, подведомственных организаций; статистическая информация о деятельности государственного органа, органа местного самоуправления и другие данные[3].

Информационный контент таких систем, банков данных, реестров и регистров зачастую представляет ценность для установления обстоятельств, подлежащих доказыванию при производстве по уголовному делу. Однако прямой доступ к таким ресурсам у лиц, осуществляющих предварительное расследование, отсутствует. Цифровые права следователя (дознавателя) в системах (банках) данных оперативно-справочной, розыскной, криминалистической, статистической, научно-технической и иной информации, а также системах иных государственных органов и органов местного самоуправления реализуются опосредовано, т.е. только через письменный запрос.

Для получения сведений оперативно-справочного, розыскного и криминалистического учетов запрос направляется в информационный центр или экспертно-криминалистическое подразделение территориального органа МВД России или Главный информационно-аналитический центр МВД России. В иных случаях — непосредственно в государственный орган или орган местного самоуправления, который располагает криминалистически значимой информацией.

Согласно ч. 4 ст. 21 УПК РФ требования, поручения и запросы следователя (дознавателя), предъявленные в пределах их полномочий, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами. При этом исполнение письменных запросов может длиться несколько суток, а иногда ответ вообще не поступает, что отрицательно сказывается на оперативности принятия организационных, тактических и процессуальных решений по уголовному делу.

Выстроить оперативное информационное взаимодействие лиц, осуществляющих предварительное расследование, с учреждениями и организациями, располагающими криминалистически значимой информацией, считаем возможным, если сделать следователя (дознавателя) участником «сделки» в цифровой среде. Для этого требуется нормативно закрепить перечень должностей в следственных органах и органах дознания, при замещении которых сотрудники правоохранительного органа могут иметь право доступа к информационным системам федеральных, региональных и местных органов исполнительной власти.

Затем следует определить перечень государственных информационных систем и систем органов местного самоуправления, к которым следователь (дознаватель) может иметь право доступа. Лицо, осуществляющие предварительное

[3] Распоряжение Правительства РФ от 10.07.2013 № 1187-р «Об утверждении перечня общедоступной информации о деятельности федеральных государственных органов, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, размещаемой в информационно-телекоммуникационной сети “Интернет” в форме открытых данных» // СПС «КонсультантПлюс».

расследование, должно располагать однозначным уровнем прав в системе, т.е. быть, например, только пользователем либо полным или частичным администратором системы. Следователь (дознаватель), подключающейся к системе через пароль или посредством усиленной квалифицированной электронной подписи, должен быть авторизован в цифровой среде.

Кроме того, предоставление цифровых прав следователю (дознавателю) в государственных информационных системах потребует решения более частных задач, а именно: подключения следственных органов и дознавателей к Единой системе межведомственного электронного взаимодействия (далее — СМЭВ); создания на компьютерах, подключенных к СМЭВ, учетных записей для каждого пользователя — следователя (дознавателя); создания системы документирования всех сеансов подключения к СМЭВ и обращения к государственным массивам данных и данным органов местного самоуправления каждого участника СМЭВ и проч. В виртуальных личных кабинетах следователей (дознавателей) должна храниться история использования ими СМЭВ, должна быть создана возможность проверки законности и обоснованности обращения к информационным системам.

Криминалистически значимая информация, полученная следователем (дознавателем) из СМЭВ, может быть оформлена протоколом осмотра интернет-ресурса федерального, регионального или местного органа исполнительной власти. Приложением к протоколу служит скриншот экрана с криминалистически значимой информацией. На скриншоте, помимо информации, должен отображаться уникальный адрес ресурса (URL), по которому она размещена в сети Интернет. Протокол осмотра интернет-ресурса приобщается к материалам уголовного дела и может служить основанием для принятия процессуальных и организационно-тактических решений по делу.

Цифровые права лиц, осуществляющих предварительное расследование в части информационных систем негосударственных юридических лиц, индивидуальных предпринимателей и физических лиц, могут быть реализованы следователем (дознавателем) самостоятельно в ходе их поисково-познавательной деятельности на интернет-ресурсах.

Поиск и изучение криминалистически значимой информации в сети Интернет относится к актуальным направлениям деятельности следователя (дознавателя) по уголовному делу. Нет сомнения, что сведения, собранные из сети Интернет, могут иметь организационно-тактическое значение (служить основанием для выдвижения и проверки следственных версий, планирования следственных действий, способствовать розыску похищенного имущества и лиц, скрывающихся от следствия и проч.), а в некоторых случаях могут быть доказательством по уголовному делу.

Однако сбор следователем (дознавателем) информации в сети Интернет предполагает знание основ информационного права, специфики размещения информации в системе и распространения ее в сети, средств и методов доступа к криминалистически значимой информации и допустимости использования ее в следственной работе.

Прежде всего следует отметить, что негосударственные (частные) информационные системы (сайты или страницы сайтов в сети Интернет, страницы в социальных сетях, чаты, форумы, базы данных и т.п.) юридических и физических лиц

могут быть как открытыми для пользователей, так и иметь закрытый характер. Федеральный закон об информации в ст. 7 определил, что «к общедоступной информации относятся общеизвестные сведения и иная информации, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации».

Обладатель информации самостоятельно или через администрацию ресурса определяет уровень конфиденциальности сведений. Поэтому некоторая криминалистически значимая информация, размещенная в сети Интернет, может быть доступна для следователя (дознавателя) только после прохождения процедур регистрации с последующей авторизацией, а к некоторым ресурсам доступ возможен только определенному кругу пользователей, установленному самим обладателем информации.

Уголовно-процессуальный закон в Российской Федерации не содержит прямого упоминания о праве следователя (дознавателя) осуществлять какие-либо действия по собиранию доказательств в интернет-среде. Отсутствуют также ведомственные инструкции и рекомендации, разъясняющие порядок действий следователя (дознавателя) в сети Интернет при собирании криминалистически значимой информации. Не всегда однозначно мнение ученых, занимающихся проблемами поисково-познавательной деятельности в информационной среде и допустимости ее результатов в процессе доказывания. Остро и неоднозначно обозначена проблема использования в доказывании сведений, собранных из закрытых аккаунтов социальных сетей, чатов, форумов и т.п.

Неоднозначность взглядов на рассматриваемую проблему не позволяет следователям (дознавателям) смело и уверенно реализовывать свои цифровые права в частных информационных системах для решения профессиональных задач с помощью цифровых технологий. Чаще всего следственная практика идет по пути дачи письменных поручений органу дознания о проведении оперативно-розыскных мероприятий в сети Интернет с целью получения криминалистически значимой информации.

Автор настоящей статьи неоднократно обращался к проблематике использования цифровых технологий в расследовании преступлений[4]. При этом следует отметить, что проблема цифровых технологий в уголовном процессе только

[4] См., например: *Першин А. Н.* Информационное пространство — новый вид места размещения криминалистически значимой информации // Уголовно-процессуальные и криминалистические чтения на Алтае : материалы ежегодной Всероссийской научно-практической конференции (17—18 ноября 2016 г.). Барнаул : Барнаульский юридический институт МВД России, 2016. С. 88—90 ; *Он же.* Государственные информационные системы как источники доказательств по уголовным делам // Борьба с правонарушениями в сфере экономики: правовые, процессуальные и криминалистические аспекты : сборник материалов международной научно-практической конференции, г. Новосибирск, 22 мая 2019 г. / отв. ред. Д. А. Савченко. Новосибирск : Новосибирский государственный университет экономики и управления ; Новокузнецк : Кузбасский институт ФСИН России, 2019. С. 130—134 ; *Он же.* Осмотр сетевых информационных ресурсов — новый вид следственного действия? // Российский следователь. 2020. № 1. С. 13—16.

набирает свои обороты, подталкивает, хотя и медленно, законодателя к внесению изменений в процессуальное законодательство с учетом существования современных цифровых технологий обеспечения жизнедеятельности человека.

Таким образом, с внедрением информационно-телекоммуникационных технологий необходимо, помимо совершенствования некоторых процессуальных институтов, практически реализовать идею наделения лиц, осуществляющих предварительное расследование, цифровыми правами и создать механизм их реализации. Это позволит повысить качество и эффективность деятельности следователей (дознавателей) по уголовным делам.

БИБЛИОГРАФИЯ

1. *Воронин М. И.* Электронные доказательства в УПК: быть или не быть? // Lex russica. — 2019. — № 7 (152). — С. 74—84.
2. *Ищенко Е. П.* У истоков цифровой криминалистики // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 3 (55). — С. 15—28.
3. *Овчинников А. И., Фатхи В. И.* Цифровые права как объекты гражданских прав // Философия права. — 2019. — № 3 (90). — С. 104—111.
4. *Першин А. Н.* Государственные информационные системы как источники доказательств по уголовным делам // Борьба с правонарушениями в сфере экономики: правовые, процессуальные и криминалистические аспекты : сборник материалов Международной научно-практической конференции, г. Новосибирск, 22 мая 2019 г. / отв. ред. Д. А. Савченко. — Новосибирск : Новосибирский государственный университет экономики и управления ; Новокузнецк : Кузбасский институт ФСИН России, 2019. — С. 130—134.
5. *Першин А. Н.* Информационное пространство — новый вид места размещения криминалистически значимой информации // Уголовно-процессуальные и криминалистические чтения на Алтае : материалы ежегодной Всероссийской научно-практической конференции (17—18 ноября 2016 г.). — Барнаул : Барнаульский юридический институт МВД России, 2016. — С. 88—90.
6. *Першин А. Н.* Осмотр сетевых информационных ресурсов — новый вид следственного действия? // Российский следователь. — 2020. — № 1. — С. 13—16.
7. Электронные доказательства в уголовном судопроизводстве : учебное пособие для вузов / С. В. Зуев [и др.] ; отв. ред. С. В. Зуев. — М. : Юрайт, 2020. — 193 с.