УДК 343.1 Вестник СПбГУ. Право. 2023. Т. 14. Вып. 1

Новые источники уголовно-процессуальных и иных судебных доказательств в цифровой реальности

А. Р. Шарипова

Башкирский государственный университет,
Российская Федерация, 450076, Уфа, ул. Заки Валиди, 32

Для цитирования: Шарипова, Алия Р. 2023. «Новые источники уголовно-процессуальных и иных судебных доказательств в цифровой реальности». *Вестник Санкт-Петербургского университета. Право* 1: 73–89. https://doi.org/10.21638/spbu14.2023.105

Отношение закона, практики и науки к активно появляющимся источникам доказательственной информации противоречиво и запоздало. Уголовно-процессуальный кодекс РФ практически не содержит особых правил обращения с электронной информацией. Между тем основной массив правил доказывания сформулирован более полувека назад и сориентирован на получение аналоговой информации. Электронные следы и способы отображения содержащейся в них юридически значимой информации настолько специфичны, что прежние процессуальные формы доказывания в современных условиях уже непригодны. Процессуальная наука разрабатывает теорию электронного доказывания по отраслевому принципу. Однако общность информационно-цифровых технологий, лежащая в основе бурного роста значения электронной информации, предопределяет возможность выработки единых межотраслевых правил. Примеры зарубежной науки показывают успешность такого подхода. Уголовно-процессуальная практика использует в доказывании только те источники, бумажные аналоги которых можно получить или в отношении которых можно провести экспертизы. Некоторые электронные доказательства появляются в уголовном процессе позже, чем в арбитражном. Традиционные осмотры, выемки, обыски и экспертизы сориентированы на отыскание и изъятие традиционных предметов материального мира. Вносимые частные изменения в уголовно-процессуальный закон, прямо касающиеся электронной информации, не способны кардинально изменить эту ситуацию. Огромный пласт электронной информации остается вне процессуального доказывания. Ее реальная ценность подтверждается использованием в оперативно-разыскной деятельности. Сторона защиты в уголовном процессе лишена даже немногих доказательственных возможностей применительно к цифровой информации. Арбитражный, гражданский и административный процессы более открыты к новейшим доказательствам. Равные права состязающихся сторон способствуют развитию электронного доказывания. Уголовный процесс с монополией обвинения на него усиливает обвинительный уклон и обедняет доказывание в целом. Дальнейшее увеличение доли электронных доказательств в уголовно-процессуальном доказывании требует изменения подходов к нему, отказа от исключительно классических правил обращения с такими доказательствами, распространения цивилистических подходов на соответствующую деятельность стороны защиты.

Ключевые слова: уголовный процесс, судебное право, электронные доказательства, арбитражный процесс, скриншот, цифровизация, обеспечение доказательств.

1. Введение

Тема электронных, цифровых доказательств и информационных технологий в уголовном процессе переживает настоящий бум в науке в последние пять-десять лет. Трудно найти сопоставимый по масштабам внимания объект исследования в эти годы. Защищены десятки тематических диссертаций, отдельным аспектам цифровизации уголовно-процессуального права посвящаются выпуски журналов и конференции. Такие же явления наблюдаются в науке цивилистического и административного процессуального права.

Тенденции формирования научных мнений предсказуемы: сформировались два крайних полюса отношения к цифровизации уголовного процесса (частью которой будем считать электронно-доказательственное право) и множество промежуточных точек зрения. Один полюс условно обозначим как позицию «всеобъемлющего приоритета цифровизации», через которую авторы глобально определяют будущее уголовного процесса; в литературе этот полюс чаще всего связывают с именем А. С. Александрова (Александров 2018a; Александров 2018b). Противоположной точки зрения придерживается Л. В. Головко, стоящий на позиции «локальной оптимизации» уголовного судопроизводства без его коренных изменений в связи с количественным ростом использования цифровых технологий (Головко 2019). Эта позиция сопряжена с бескомпромиссной критикой процессуального футуризма. Такая полярность мнений характерна не только для отечественной науки: необходимость доказывания права на существование науки цифровой криминалистики, или электронно-доказательственного права, характерна не только для отечественной юриспруденции, но и для других правовых систем (Arshad, Jantan, Abiodun 2018).

2. Основное исследование

2.1. Современный научный контекст

Помимо принципиальных взглядов на судьбы уголовного процесса, электронно-доказательственное право породило разные подходы к частным вопросам доказывания, связанным с новыми источниками информации. В последние годы в литературе активно обсуждаются процессуальные способы извлечения, оформления, хранения таких разновидностей электронных доказательств, как переписка по электронной почте, в мессенджерах, социальных сетях, включая тексты, аудио- и видеофайлы, содержимое профилей в социальных сетях, содержимое сайтов. В научной литературе и правоприменительной практике стало часто упоминаться понятие скриншота (изображения, сделанного устройством и отражающего то, что видит пользователь в данный момент), являющегося доступным и распространенным способом «материализации» электронной информации.

Даже поверхностный анализ сказанного в литературе об использовании цифровых технологий и электронной техники в доказывании по уголовным делам позволяет утверждать, что у проблемы этой есть два трудно совместимых между собою блока: собственно технический и юридический, т. е. уголовно-процессуальный. Создается впечатление, что значительная часть дискуссий порождена, как нередко

бывает в юриспруденции, неопределенностью предмета спора. Именно поэтому попытаемся выяснить, по поводу чего в науке существует хотя бы относительное единодушие. Во-первых, ни один из авторов не отрицает того, что уголовному процессу не удастся отгородиться от постоянно развивающейся электронной техники, от интернета, социальных сетей, мессенджеров и т. п. Во-вторых, неизбежное проникновение искусственного интеллекта в уголовное судопроизводство имеет естественные ограничения: он не сможет полностью вытеснить оттуда человека, принимающего властные решения и несущего ответственность за них, в том числе негативную юридическую ответственность в виде неблагоприятных последствий лично для него, в виде таких лишений, которые имеют для каждого человека отнюдь не виртуальное значение. В-третьих, глобальное проникновение информационных технологий во все сферы социальной и частной жизни человека, сама техническая возможность такого проникновения и даже все возрастающая доступность его для все более широкого круга лиц никогда не снимут с повестки дня необходимости охраны личной и семейной, а также иной охраняемой законом тайны, в частности тайны предварительного расследования. Эти зоны относительного согласия можно перечислять и дальше; их анализ как раз и позволяет совместить технико-программное и собственно правовое обеспечение цифровизации доказывания по уголовным делам и всего уголовного процесса в целом. То, что процессы такого совмещения будут болезненными, стало очевидным с момента появления первых ЭВМ в СССР. То, что болезненность эта не снята до сих пор, — проблема, требующая решения. При всей специфике российского, как и любого континентально-европейского, уголовного процесса цифровизация правосудия, по крайней мере в технико-кибернетической части, имеет межотраслевой характер, что объясняет уместность и разумность межотраслевых аналогий и иных межотраслевых сопоставлений при поиске оптимальных способов решения этой глобальной проблемы. Рискнем предположить, что и здесь именно уголовный процесс проявляет наибольшую косность при сопоставлении с другими сферами правосудия, если судить по доле дел, в доказывании по которым использована электронная информация (например, по сравнению с арбитражными делами), и это притом что технические службы органов, осуществляющих оперативно-разыскную деятельность, большей частью совпадающих с субъектами уголовного судопроизводства, именуемыми органами дознания, т. е. имеющими прямое отношение к уголовному процессу, обладают самыми мощными техническими возможностями в выявлении интересующей их информации. Нельзя не увидеть в этом парадокса.

2.2. Скриншот как пример аналогового подхода к электронной информации

Уголовный процесс не сразу признал скриншот как доказательство. В 2015 г. мы опубликовали статью, в которой анализировалась практика использования скриншотов в доказывании в разных видах судебных процессов (Шарипова 2015). На тот момент развитой практике использования их в арбитражном процессе соответствовали значительно более редкие случаи использования в доказывании по уголовным делам с немыслимыми аналоговыми процедурами помещения скриншотов в опломбированные в присутствии понятых конверты. Для сравнения, в 2012 г.

в УПК Китая был внесен новый вид доказательств — электронные данные, — перешедший затем и в новый закон 2018 г.; с 2016 г. действует разъяснительное Положение о сборе, извлечении и рассмотрении электронных данных по уголовным делам[1] (Wang, Liu 2019), а с 2017 г. функционируют интернет-суды по гражданским делам (Шереметьева, Батуро, У Шуан 2020).

Главенствующей идеей обращения с цифровой информацией в уголовном процессе остается идея ее превращения в аналоговую информацию, в отношении которой нужно применять традиционные действия — осмотр, обыск, выемку и экспертизу. Изменения УПК РФ, связанные с электронными доказательствами, сводятся преимущественно к правилам изъятия и хранения электронных носителей как разновидности вещественных доказательств.

2.3. Условность осмотра в отношении электронных доказательств

Производимые с цифровой информацией операции можно отнести к названным выше традиционным действиям с большой долей условности. Все-таки соответствующие уголовно-процессуальные нормы создавались даже не в 2001 г., когда был принят Уголовно-процессуальный кодекс (УПК) РФ от 18.12.2001 № 174-ФЗ[2], они во многом текстуально совпадают еще с законом середины XX в. (УПК РСФСР, утв. Верховным Советом РСФСР 27.10.1960), поэтому просто не могут учитывать нюансы обращения с «цифрой». Например, правоохранительные органы используют для получения из мобильных телефонов, заблокированных паролями, содержащих удаленную и неочевидную пользователю информацию, устройство криминалистического исследования сотовых телефонов UFED (Universal Forensics Extraction Device). Это прибор с собственным программным обеспечением (обновляемым в соответствии с обновлениями операционных систем самих телефонов), который взламывает их и делает доступной оператору всю содержащуюся в телефоне информацию в виде файлов (таких как «Сообщения», «Телефонная книга», «Видео» и т. п.). Оператор производит осмотр этих файлов, и через протокол осмотра информация из телефона попадает в уголовное дело в качестве доказательства. Но разве это не традиционный осмотр предмета, производимый человеком при помощи собственных органов чувств, пусть и усиленных многократно специальной техникой?

Традиционное понимание осмотра сориентировано на отображение материальных, т. е. не идеальных, следов, и с такой точки зрения описываемое следственное действие — это именно осмотр. Однако природа электронных следов сама по себе настолько нетрадиционна и спорна (Россинская 2019, 570), что и попытки втиснуть способы их отображения в привычные процессуальные формы представляются несколько искусственными и лишенными будущего.

Отличие цифровой информации в том, что необходимость интерпретации для восприятия человеком заложена в ее природе: она по определению зашифрована двоичным кодом и в первозданном виде только машиночитаема. Однако это сущ-

[1] Китайское законодательство приводится по Порталу законов Китая. Дата обращения 16 декабря, 2022. https://ru.chinajusticeobserver.com/law.

[2] Здесь и далее все ссылки на российские нормативно-правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». Дата обращения 20 июня, 2021. http://www.consultant.ru.

ностное отличие цифровой информации от аналоговой по большей части нивелируется тем, что устройства, хранящие ее, мгновенно декодируют информацию в привычный для человеческого восприятия вид. Исключения составляют неисправные и заблокированные устройства, устройства, применяющие специальное защитное программное обеспечение, а также устройства с удаленной информацией.

2.4. Особенности электронной информации, ускользающие от обыденного восприятия

Свойства компьютерных программ и мобильных приложений по большей части стали восприниматься как обыденные знания. То, что текстовые редакторы отображают те наборы слов и мессенджеры отправляют именно те сообщения, которые ввел оператор, а не какие-то другие, нам известно и без компьютерной экспертизы. Однако, например, то, что у фотофайла, пересылаемого в мессенджере WhatsApp, меняются размер и качество (уменьшаются во много раз), а значит, полученный файл не идентичен отправленному, знают уже не все. Привычное нам копирование файлов подразумевает их содержательную идентичность; это приводит к тому, что применяется оно и в отношении файлов, подвергающихся судебно-компьютерной экспертизе, например для перенесения на более подходящий в конкретной ситуации электронный носитель информации (диск, USB-накопитель и др.). Метаданные исходного и скопированного файла в таком случае не одинаковы, что, в свою очередь, вызывает сомнения и в общих результатах исследования[3].

Подобных и гораздо более сложных нюансов, включая баги (ошибки) у компьютерных программ и особенно мобильных приложений, масса. Не за всеми приложениями стоят корпорации информационных технологий. Сейчас создать приложение и разместить его в официальных App Store и Google Play может любой программист, если приложение пройдет проверку на отсутствие вирусной угрозы. Следовательно, заявленные производителем и ожидаемые потребителем свойства приложений могут отличаться от реальных. Например, популярные фитнес-браслеты и умные часы оснащены элементарной функцией шагомера, т. е. определения пройденного расстояния. Подобная информация может быть значимой в уголовном деле, однако разные устройства и разное программное обеспечение на них поразному определяют одно и то же перемещение в пространстве: какие-то не замечают маленькие и медленные шаги, какие-то принимают за шаги интенсивные движения рук и др. Подобные погрешности встречаются в приложениях, определяющих геолокацию, информация о которой может быть более чем востребована в уголовно-процессуальном доказывании.

Аутентичность извлеченной информации, связанная с принципиальной способностью адекватно ее регистрировать, вызывает сомнения не только в связи с персональными мобильными устройствами. Так, следователям по делам о дорожно-транспортных происшествиях рекомендуется собирать информацию о событии с регистратора данных, установленного на блоке управления подушки безопасности. Он содержит важные сведения о скорости автомобиля в момент столкновения,

[3] См., напр.: Определение Шестого кассационного суда общей юрисдикции от 26.01.2021 № 77-338/2021.

нажатии на педаль тормоза и др. В одних уголовных делах суд принимает соответствующие доказательства в качестве допустимых[4], а в других отклоняет со ссылкой на то, что SRS (Supplemental Restraint System, система активной безопасности) не является измерительным прибором (интересное совпадение: это происходит в тех делах, где его показания свидетельствуют в пользу версии защиты)[5].

Еще сложнее обстоит дело с функциями программ и приложений, замаскированными или неочевидными для пользователей. Так, сайт, распространяющий компьютерные вирусы, не имеет на страницах, предназначенных для пользователей, никаких указаний на это. Никакими скриншотами самого сайта это не установить. Только экспертиза кода может подтвердить, что в нем заложены вредоносные программы, но в таком случае объектом экспертизы является не то же самое, с чем взаимодействовали потерпевшие.

Иными словами, сводить цифровую информацию к тому, что выводится на экраны устройств, неверно.

2.5. Ситуативность выбора способов взаимодействия с электронной информацией

В простой ситуации, когда необходимо ознакомиться с неудаленной перепиской в мессенджере на устройстве, которым пользовался один человек, не отрицающий этого и не удалявший приложение, не форматировавший память, не блокировавший операционную систему, можно ограничиваться осмотром. Однако в конфликтных ситуациях, когда применены действия по сокрытию цифровой информации, восстановление доступа к соответствующим файлам называть осмотром неверно.

Свойства цифровой информации неоднозначны и применительно к технологиям ее обработки и восприятия. С одной стороны, скрыть объемный цифровой документ путем уничтожения от такого процессуального действия, как осмотр (без применения криминалистических устройств), значительно проще, чем бумажный. Если представить, что это сводная информация о финансовых результатах деятельности организации на сотнях страниц, то нескольких секунд достаточно, чтобы удалить его с устройства или переслать на другое, т. е. скопировать. Чтобы физически уничтожить или размножить сотни листов бумаги, нужно гораздо больше времени и усилий. С другой стороны, если бумаги сожжены, то информация потеряна безвозвратно. С цифровой информацией иначе: способов избавиться от нее окончательно очень мало (и действуют они только в отношении информации, не попадавшей в интернет), а возможности восстановления зависят от умений программиста и почти безграничны.

Другая неоднозначность электронных доказательств состоит в возможности установления их связи с конкретным человеком. С одной стороны, IP-адреса, ICCID сим-карт, IMEI устройств, электронные подписи, логи интернет-ресурсов позволяют с высокой степенью надежности устанавливать, кем именно совершены какие-то электронные действия. В этом смысле от цифровых идентификационных

[4] Апелляционное постановление Воронежского областного суда от 03.02.2020 № 22-162/2020.

[5] Апелляционное постановление Верховного суда Карачаево-Черкесской Республики от 29.10.2019 по делу № 22-268/2019.

следов избавиться гораздо сложнее, чем, например, от собственных отпечатков пальцев. С другой стороны, все эти следы в массе своей приводят к идентификации устройств, а не людей. При этом вероятность использования электронных устройств, помимо воли их владельца, гораздо выше, чем его пальцев. Низкую способность электронной цифровой подписи подтверждать волю человека на совершение каких-то действий отмечают в уголовно-процессуальной литературе. Такая подпись более уместна там, где человек вправе принять на себя риски ее использования: ради удобства пользования сервисом «Госуслуги»[6] человек соглашается на презумпцию того, что его электронная подпись поставлена им, или отказывается от нее и пользуется личным способом совершения юридически значимых действий. В уголовно-процессуальном доказывании такая презумпция неуместна. В то же время отказываться вовсе от электронной цифровой подписи на основании ее небезупречности, как это предлагает Л. В. Головко, избыточно консервативно (Головко 2019, 19). Развивая тему небезупречности, нетрудно поставить под сомнение и любой аналоговый документ, любой физический след, любое вещественное доказательство и уж тем более любое личное доказательство по причине общей склонности всех людей лгать. Однако многовековая практика судебного доказывания не отвергла ни одного из этих видов доказательств, а лишь выработала целую систему способов их проверки и правил оценки. Более того, система собирания, проверки и оценки доказательств все это время неизменно совершенствовалась и приспосабливалась к особенностям новых источников информации. Электронная информация — такой же плод исторического развития общества, и странно было бы настаивать на неизменности способов процессуального доказывания в связи с ее появлением и развитием. Темпы этого развития возросли в тысячи раз, но и это тоже закономерно для общей истории человечества.

Удаленное вторжение в компьютер или иное устройство и совершение «от имени» его владельца каких-то действий злоумышленником или созданной им программой рискует быть не отличенным от преступных действий самого владельца. В большой статье, посвященной исследованию проблем цифровой криминалистики, упоминаются случаи необоснованного осуждения за распространение порнографических материалов человека, на компьютере которого первоначально не были обнаружены вредоносные программы, занимавшиеся этим без его ведома (Arshad, Jantan, Abiodun 2018).

2.6. Усугубление неравенства доказательственных возможностей обвинения и защиты

Большинство исследователей приходят к выводу, что имеющихся в УПК РФ процессуальных действий достаточно для работы с цифровыми доказательствами, особенно с учетом того, что практика приспосабливает одно к другому (Головко 2019). Скорее всего, это действительно так. Их достаточно, только для кого: для обвинения, проводящего осмотры, обыски, выемки и назначающего подавляющее большинство экспертиз? Да, многочисленные примеры использования результатов оперативных мероприятий в качестве доказательств это подтверждают. Другой

[6] Госуслуги. Дата обращения 20 июня, 2021. https://www.gosuslugi.ru.

пример — назначение обязательной экспертизы для определения причины смерти при отсутствии трупа. Мы подробно писали об этом применительно к отраслевым особенностям экспертиз: невозможность проведения судебно-медицинской экспертизы причины смерти без трупа преодолевается следствием путем проведения ситуационной экспертизы, имеющей очень малую информационную ценность, но позволяющей формально исполнить предписание закона об обязательном назначении исследования (Шарипова 2021, 32).

Однако отсутствие законодательного понятия электронных доказательств и особых способов их получения и фиксации полностью исключает из числа субъектов доказывания сторону защиты. А. А. Хайдаров описывает случаи использования стороной защиты данных из социальных сетей в качестве ориентирующей информации, которая послужила для обоснования перед следователем ходатайств о проверке некоторых обстоятельств (Хайдаров 2020). «Некоторые обстоятельства» сводились к тому, что оперативные сотрудники, «потерпевшие» и понятые знакомы между собой и являются «друзьями» в социальных сетях. Вслед за этим следствие раскрыло глаза на «подставную», а не контрольную закупку, проделанную оперативниками, и уголовное дело развалилось. Для стороны обвинения, конечно, удобно, когда процессуальный оппонент преподносит в виде просьбы важные для дела факты, а не представляет их перед судом, опозорив органы уголовного преследования. Такое положение вещей — хорошая демонстрация состояния состязательности в уголовном процессе.

Противники состязательности (и по совпадению противники цифровизации) убедительно аргументируют преимущества инквизиционного процесса, но недооценивают недостатки современного расследования, ориентированного на судебную перспективу дела. Сначала правоохранительные органы не возбуждают уголовное дело (раньше не принимали заявления о преступлении, теперь пускают заявителей по бесконечному кругу обжалования отказов в возбуждении), но если возбуждают, то не могут прекратить (по реабилитирующим основаниям), а непременно должны передать в суд. Электронные доказательства игнорировать зачастую проще других. Так, В. Н. Григорьев описывает в статье уголовное дело, по которому состоялся необоснованный обвинительный приговор (впоследствии отмененный) из-за представления в качестве доказательства обвинением записи только одной из нескольких уличных камер, заснявших происшествие, при наличии всех записей (Григорьев 2020). Суд, привыкший к доказательственной монополии обвинения, не принял записи от стороны защиты.

Приведенные примеры показывают, что в отношении электронных доказательств (как и всех остальных) сохраняется практически полная невозможность для стороны защиты собирать их и представлять на должном, процессуальном уровне, а не в качестве помощника стороны обвинения. Вся доказательственная мощь уголовного процесса привычно сосредоточена в руках органов уголовного преследования. Однако опыт цивилистического (гражданского и арбитражного) процесса показывает, что равные и состязающиеся стороны могут развивать доказывание на достаточно высоком уровне даже без властных полномочий.

2.7. Состояние электронного доказывания в цивилистическом процессе

Гражданская процессуальная и особенно арбитражная практика принимает значительно больше электронных доказательств, чем уголовно-процессуальная, — по инициативе стороны защиты. Так, дистанционное зондирование (определение местоположения и размеров объектов на Земле со спутников) широко используется по арбитражным делам примерно с 2015 г.[7] Именно этот метод формирования электронных доказательств показательно высмеян сторонниками идеи «локальной оптимизации» (Головко 2019), что не совсем справедливо, потому что Главному управлению криминалистики Следственного комитета РФ в 2015 г. была поставлена задача изучить возможности проведения экспертных исследований снимков космосъемки для последующего использования их в доказывании по уголовным делам (Смехнов 2018). Случаи использования таких снимков уже есть, например, в делах об экологических преступлениях[8], но далеко не повсеместно.

Необходимо, чтобы масса общедоступной информации из социальных сетей или других интернет-ресурсов могла быть своевременно закреплена стороной защиты для представления в качестве доказательства в уголовное дело. Все возражения, связанные с достоверностью этих доказательств (принадлежат ли аккаунты в социальных сетях тем людям, чьи имена в них названы, действительно ли они вели переписку или размещали на страницах какой-то контент, выходили ли в сеть в определенное время и т. п.), не являются основаниями для их непринятия.

2.8. Обилие источников электронной информации и скудность их реального использования в качестве доказательств

Правоохранительные органы признают, что электронная информация опережает законные способы ее собирания. Существует масса разновидностей цифровых сведений, которые невозможно подтвердить доказательствами в уголовно-процессуальном смысле. Например, ознакомиться с удаленными или заблокированными данными иностранных социальных сетей и мессенджеров оперативным путем возможно, а получить официальный ответ с соответствующих серверов хранения информации — нет. Хотя электронная информация крайне многообразна и может быть задействована едва ли не в каждом уголовном деле, в действительности широта ее доказательственного использования весьма скромная. Большинство электронных доказательств в уголовном судопроизводстве, судя по проведенному нами анализу почти тысячи судебных актов из базы СПС «КонсультантПлюс», — это неудаленная переписка в мессенджере Telegram, где указывается место «закладки» наркотических средств, используемая для подтверждения их сбыта и хранения (122 акта из 988 изученных преимущественно за 2020 г.).

Аналоговый подход к цифровой реальности обедняет возможности судебных процессов. В коммерческом использовании давно обращаются результаты анализа big data (больших данных) — программной обработки открытой информации

[7] См., напр.: Постановление Семнадцатого арбитражного апелляционного суда от 02.11.2016 № 17АП-121/2015-ГК по делу № А71-3867/2014.

[8] Апелляционное определение Верховного суда Республики Коми от 14.03.2019 № 22-419/2019.

огромного объема без участия человека. Государство делает шаги по использованию подобного анализа в контролирующей деятельности, в том числе в отношении охраняемой информации. В налоговом администрировании анализ больших данных используется для выявления необоснованного применения вычета по НДС (путем сопоставления по специальным алгоритмам всех сделок всех налогоплательщиков), для сопоставления расходов и доходов физических лиц и др. Применительно к экономическим преступлениям этот вид работы с информацией имеет огромный потенциал, но нет никаких способов ее ввода в судебный процесс.

Претензии к недостаточности реквизитов у электронных доказательств общи для всех видов процесса: в диссертации «Процессуальная форма доказательств в современном гражданском судопроизводстве» Н. И. Борискина обращает внимание на широко распространенную практику смешения понятий достоверности и допустимости, приводящую к необоснованному исключению из материалов дела информации, вызывающей сомнения (Борискина 2020).

Если бы УПК РФ содержал особые правила обращения с электронными доказательствами, хотя бы частично применимые к деятельности обвиняемого и его защитника, это способствовало бы реализации принципа состязательности и усилению роли защиты в процессе.

2.9. Достоинства и недостатки нотариального обеспечения электронных доказательств

Пока что основным способом удостоверения электронной информации по гражданским, арбитражным и административным делам остается нотариальное обеспечение доказательств. Согласно ст. 102 Основ законодательства о нотариате нотариус по просьбе заинтересованных лиц обеспечивает доказательства, необходимые в случае возникновения дела в суде или административном органе, если имеются основания полагать, что представление доказательств впоследствии станет невозможным или затруднительным. Исключений для уголовного процесса в этой норме нет, но нет и практики представления в процесс обеспеченных нотариусом доказательств.

Постепенно все более ровное отношение к электронным доказательствам демонстрирует российский арбитражный процесс. Скриншоты принимаются в качестве доказательств без всякого заверения в случае, если их содержание активно не опровергается другой стороной. Казалось бы, позитивная практика нотариального удостоверения скриншотов имеет одну скрытую проблему: сами нотариусы зачастую отказываются это делать. Различное понимание рамок применимости нотариального обеспечения доказательств к разным видам электронной информации (содержание сайтов, аудио- и видеозаписи) в силу отсутствия современной регламентации этих действий отражено в тематической литературе (Мышко, Любимцева 2019).

Еще одно ограничение нотариального удостоверения доказательств связано с двух- и трехфакторной аутентификацией пользователей, когда вход на определенный интернет-ресурс под собственным логином возможен не с любого, а только с определенного компьютера (это используется на некоторых электронных торговых площадках). Соответственно, проделать этот путь на компьютере нотариуса, чтобы он удостоверился, что перед ним не сайт-двойник, просто невозможно.

2.10. Защита охраняемой тайны, содержащейся в электронных устройствах

Еще одна причина необходимости выделения особого вида доказательств для электронной информации заключается в том, что теперь огромное количество информации и доступов к ней, включая охраняемые законом банковскую, налоговую, медицинскую тайны, находится в мобильных устройствах, а в отношении этих устройств проводятся не санкционируемые судом осмотры. Конечно, подобными хранилищами тайн и раньше были персональные компьютеры (хотя все же в гораздо меньшей степени), но находились они, как правило, в жилище у граждан, а поэтому доступ к ним правоохранительных органов осуществлялся все-таки посредством обыска, т. е. с разрешения суда. Необходимостью защиты тайны личной жизни и аналогией с уголовным судопроизводством США аргументирует необходимость проведения обыска в отношении электронных носителей информации Р. И. Оконенко (Оконенко 2016, 12–13). Полагаем, что речь должна идти о судебном санкционировании подобного обыска, включая дистанционный обыск, понятие которого тоже разрабатывается в науке (Балашова 2020, 133). Американский специалист по цифровым технологиям в уголовном процессе из Беркли О. Керр, анализируя обыск компьютера и возможность распространения на него Четвертой поправки к Конституции США (касающейся проведения обыска по судебному ордеру), приходит к положительному выводу. При этом он отмечает, что «компьютеры похожи на контейнеры в физическом смысле, дома — в виртуальном смысле и огромные склады — в информационном смысле», а значит, нужно выбирать, какие правила наиболее применимы к ним (Kerr 2005, 533).

Прецедентная система права открывает безграничные возможности для такого выбора, и касается это не только собственно компьютерных следов. Однако полагаем, что и в отечественном уголовном процессе указанные возможности имеются, как в относительно недавней российской истории находящийся в собственности участок земли стал объектом обыска (т. е. принудительного визуального обследования), а не осмотра, предполагающего недопустимость возражений. Аналогично осмотр жилища при отсутствии согласия проживающих в нем лиц лишь относительно недавно стал производиться только на основании судебного решения. Бóльшие или меньшие трансформации правил доказывания по уголовным делам всегда были неизменным спутником развития российского уголовного процесса.

2.11. Вопрос об электронном доказывании в зарубежных научных исследованиях

Общность информационных технологий, единство носителей цифровой информации, имеющей значение для разных видов судопроизводства, означают, что развивать теорию электронных доказательств и формировать практику их использования необходимо в общепроцессуальном масштабе. Показательной в этом плане является англоязычная монография «Проверка цифровых доказательств», раскрывающая правила и примеры проверки в суде цифровых доказательств безотносительно отраслевой принадлежности дел (Grimm, Capra, Joseph 2017). Нужно предотвратить формирование различных отраслевых правил собирания и фикса-

ции электронных доказательств для уголовного, арбитражного, гражданского и административного процесса.

Использование электронных доказательств в американских судах по гражданским делам уже в 2006 г. потребовало внесения поправок в Федеральные правила гражданского судопроизводства[9], которые, однако, не уберегли судопроизводство от сложных вопросов, связанных с аутентификацией электронных доказательств. Поскольку развитие ESI (electronically stored information, информация, хранимая в электронном виде) опережает готовность судопроизводства к ее восприятию, попытки всеобъемлющего определения этого понятия пока безуспешны.

Способы проверки подлинности электронных данных могут быть разными: в одних случаях суды ограничивались показаниями свидетеля, видевшего информацию на интернет-сайте, в других — запрашивали у организации, которая ведет этот сайт, она ли разместила там соответствующую информацию, в третьих — был допрошен специалист, обнаруживший в интернете что-то, интересующее суд. Кроме того, суды возлагают бремя опровержения электронной информации на другую сторону (приводятся примеры из гражданских дел, а также из уголовных, в которых обвинению не удалось опровергнуть подобный довод защиты), если она опровергает эту информацию (Moore 2010, 158–161). Уже в 2010 г. в науке и практике обсуждались и применялись электронные способы верификации электронных доказательств при условии обоснования перед судом их надежности с научной точки зрения. К ним относились, например, хеш-функции для фиксации доказательств в том виде, в каком они обнаружены, чтобы «внесение даже одной запятой на тысячи страниц текста» не осталось незамеченным (Moore 2010, 183–184).

По нашим данным, технологичные способы собирания доказательств (по крайней мере по гражданским делам) наиболее активно применяются в Китае, где с 2017 г. функционирует стандартизированное интернет-судопроизводство (с электронной подачей заявлений и доказательств, онлайн-заседаниями и биометрической идентификацией личности, стенограммами на основе автоматического распознавания речи и иными атрибутами будущего) (Харитонова 2020).

2.12. Перспективные возможности судебного доказывания

Российскому информационному праву также известны научно обоснованные способы проверки электронной информации (например, WIPO PROOF) (Благополучная 2020), однако до судебной практики эти методы не доходят, не в последнюю очередь ввиду отсутствия приемлемых процессуально-правовых форм их использования.

В науке цивилистического процесса значительно раньше началось обсуждение изменения традиционного собирания и исследования доказательств применительно к их электронной разновидности. В 2013 г. в диссертации «Электронные доказательства и принцип непосредственности в арбитражном процессе» предлагалась схема аутентификации электронных доказательств, позволяющая представлять их непосредственно суду, определялись неотложные меры обеспечения таких доказательств, в том числе с участием суда, хотя и до подачи иска (Митрофанова 2013).

[9] Federal Rules of Civil Procedure as added April, 12 2006. Дата обращения 20 июня, 2021. https://www.uscourts.gov/sites/default/files/federal_rules_of_civil_procedure_-_december_2020_0.pdf.

Судебной практикой в достаточной мере апробирован и принят единственный способ фиксации электронных доказательств — их нотариальное удостоверение. Однако на современном уровне цифровизации разных сфер социальной жизни требуется поиск иных, более приспособленных к цифровой реальности способов. В диссертации «Обеспечение доказательств в гражданском и арбитражном процессе» К. А. Сергеева еще в 2012 г. предлагала наделить соответствующими полномочиями адвокатов и судебных приставов (Сергеева 2012).

3. Выводы

Конвергенция в сфере электронного доказывания между процессуальными отраслями права заключается в распространении средств, используемых сторонами в состязательных цивилистическом и административном процессах, на доказательственную деятельность стороны защиты в уголовном процессе. Мощное развитие цифровой криминалистики не предоставляет равные доказательственные возможности уголовно-процессуальным оппонентам, поэтому стороне защиты в поиске средств самостоятельного, не опосредованного правоохранительными органами подтверждения своих аргументов стоит ориентироваться на аналоги из гражданского, арбитражного и уголовного процессов. Осмотры, обыски, выемки и экспертизы в отношении цифровой информации, какими бы фантастическими ни были их результаты, остаются недоступными для защиты способами собирания доказательств.

Приведенные примеры подтверждают, по нашему мнению, идею о том, что для процессуального права перспективны новейшие технологии взаимодействия с цифровой информацией, а не попытки приспособить ее под традиционные аналоговые методы. Стремление закрепить электронную информацию в привычных документальных формах непредосудительно и вполне понятно: будучи зафиксированной на бумаге, она перестает быть такой изменчивой и нереальной, позволяет оперировать ею как обычными доказательствами. В этом смысле цифровая информация уникальна: когда речь идет о той ее разновидности, что не связана с материальным носителем, доступным для изъятия правоохранительными органами, она может продолжать меняться или удаляться в процессе и даже после «собирания доказательств». Она подобна скоропортящемуся предмету, только порча ее зависит не от времени, а от действий других лиц, в том числе прямо в ней заинтересованных. Органы уголовного преследования пока не привыкли к тому, что факт изъятия улики не означает ее автоматическое попадание под их полную власть, борьба за электронную улику продолжается и после ее попадания в их руки.

Если вместо создания новых процессуальных способов введения цифровой информации в судопроизводство на базе технологических методов обращения с ней отечественный процесс останется на позициях приспособления ее к старым формам, разрыв возможностей формы и содержания будет увеличиваться. Форма окажется все менее способной передавать свойства содержания, все большее число подробностей станет исчезать из-под судебного контроля, оставаясь прерогативой экспертов. Например, хеширование как цифровой способ фиксации содержания файлов для контроля факта внесения последующих изменений предлагается только на внутрикриминалистическом уровне, для использования специалиста-

ми и экспертами, хотя, по сути, оно доступно для самостоятельного применения и оценки любыми участниками судопроизводства.

Новейшие методы собирания и проверки доказательственной информации не попадают в судебные процессы, потому что лишены процессуальных форм, они остаются в лучшем случае в недрах оперативной деятельности, обедняя и уголовно-процессуальное доказывание, и остальные виды судебного доказывания.

Библиография

Александров, Александр С. 2018a. «Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий». *Судебная власть и уголовный процесс* 3: 130–139.

Александров, Александр С. 2018b. «Русский уголовно-процессуальный догматизм или цифровой мир: что победит?» *Юридическая истина в уголовном праве и процессе. Материалы Всероссийской научно-практической конференции*, 24–34. СПб.: Петрополис.

Балашова, Анна А. 2020. «Электронные носители информации и их использование в уголовно-процессуальном доказывании». Дис. … канд. юрид. наук, Академия управления Министерства внутренних дел РФ.

Благополучная, Камила В. 2020. «О новой системе верификации цифровых файлов WIPO PROOF». *Авторское право и смежные права* 7: 37–44.

Борискина, Надежда И. 2020. «Процессуальная форма доказательств в современном гражданском судопроизводстве». Дис. … канд. юрид. наук, Московский государственный университет имени М. В. Ломоносова.

Головко, Леонид В. 2019. «Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция?». *Вестник экономической безопасности* 1: 15–25.

Григорьев, Виктор Н. 2020. «О тревожных тенденциях в доказывании фактических обстоятельств вмененного деяния». *Российская академия юридических наук. Научные труды* 20: 302–305.

Митрофанова, Маргарита А. 2013. «Электронные доказательства и принцип непосредственности в арбитражном процессе». Дис. … канд. юрид. наук, Саратовская государственная юридическая академия.

Мышко, Федор Г., Людмила П. Любимцева. 2019. «Обеспечение нотариусом доказательств в гражданском процессе, в том числе при их размещении в сети Интернет». *Вестник Московского университета МВД России* 6: 271–281.

Окоменко, Роман И. 2016. «"Электронные доказательства" и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации». Дис. … канд. юрид. наук, Московский государственный юридический университет имени О. Е. Кутафина.

Россинская, Елена Р. 2019. *Избранное.* М.: Норма.

Сааков, Тигран А. 2020. «Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора». *Законы России: опыт, анализ, практика* 4: 96–103.

Сергеева, Ксения А. 2012. «Обеспечение доказательств в гражданском и арбитражном процессе». Дис. … канд. юрид. наук, Уральская государственная юридическая академия.

Смехнов, Вадим А. 2018. «Использование снимков дистанционного зондирования Земли в качестве доказательств по уголовным делам». *Вестник Главного управления криминалистики* 1: 19–22.

Хайдаров, Альберт А. 2020. «Использование возможностей социальных сетей и мобильных устройств для защиты адвокатами прав и законных интересов подозреваемых (обвиняемых) и выявления прокурорами нарушений по уголовным делам». *Актуальные проблемы российского права* 15 (5): 179–187.

Харитонова, Юлия С. 2020. «Платформизация правосудия: опыт Китая и будущее судебных систем мира». *Вестник арбитражной практики* 3: 3–11.

Шарипова, Алия Р. 2015. «Доказывание в уголовном и арбитражном процессах: “невынужденные” различия». *Библиотека криминалиста. Научный журнал* 4: 180–185.
Шарипова, Алия Р. 2021. «Назначение судебной экспертизы по уголовным делам: насколько оправдана отраслевая специфика?» *Эксперт-криминалист* 3: 31–34.
Шереметьева, Наталья В., Илья В. Батуро, Шуан У. 2020. «Особенности электронного правосудия в КНР». *Право и практика* 2: 159–163.
Arshad, Humaira, Aman B. Jantan, Oludare I. Abiodun. 2018. “Digital forensics: Review of issues in scientific validation of digital evidence”. *Journal of Information Processing Systems* 14 (2): 346–376. https://doi.org/10.3745/JIPS. 03.0095
Grimm, Paul, Daniel Capra, Gregory Joseph. 2017. “Authenticating digital evidence”. *Baylor Law Review* 69 (1). Дата обращения 12 июня, 2021. https://www.baylor.edu/law/review/doc.php/286449.pdf.
Kerr, Orin S. 2005. “Searches and seizures in a digital world”. *Harvard Law Review* 119: 531–585.
Moore, Jonathan L. 2010. “Time for an upgrade: Amending the federal rules of evidence to address the challenges of electronically stored information in civil litigation”. *Jurimetrics Journal* 50: 147–193.
Wang, Bo, Yuxian Liu. 2019. “Collection and judgment of electronic data evidence in criminal cases: From the perspective of investigation and evidence collection by public security organs”. *Journal of Forensic Science and Medicine* 5: 187–194. https://doi.org/10.4103/jfsm.jfsm_26_19

Статья поступила в редакцию 14 марта 2021 г.;
рекомендована к печати 28 октября 2022 г.

Контактная информация:

Шарипова Алия Рашитовна — канд. юрид. наук, доц.; Nord-wind23@mail.ru

New sources of criminal procedural and other judicial evidence in digital reality

A. R. Sharipova

Bashkir State University,
32, ul. Zaki Validi, Ufa, 450076, Russian Federation

For citation: Sharipova, Aliya R. 2023. “New sources of criminal procedural and other judicial evidence in digital reality”. *Vestnik of Saint Petersburg University. Law* 1: 73–89. https://doi.org/10.21638/spbu14.2023.105 (In Russian)

The attitude of law, practice and science to actively appearing sources of evidentiary information is controversial and belated. Besides some exceptions Criminal Procedure Code does not contain special rules for handling electronic information. Meanwhile evidentiary rules were formulated more than half a century ago and were principally oriented only on receiving analog information. Electronic traces and ways of displaying legally relevant information contained in them are sospecific that previous procedural forms are not usable nowadays. Procedural science develops the theory of electronic evidence on a sectoral basis. However, thecommunity of information-digital technologies which is lying in the core of impetuous growth of importance of electronic information predetermines the possibility of producing consolidated intersectoral rules. Examples of foreign science show the success of this approach. Criminally-remedial practice uses only sourcesby which you can get paper analogs or conduct an examination while proving. The extension of traditional inspection, seizure, search and examination to electronic information lowers its efficiency and does not provide a regime of secrets protected by law. A huge layer of electronic information remains outside the procedural proof. Its real value is confirmed by its use in law enforcement intelligence-gathering activities. Defensive side in criminal proceedings is deprived of even a few evidentiary opportunities in relation to digital information. Civil, Arbitral, Administrative proceedings

are more open to recent evidences. Equal rights of the contestants contribute to the development of electronic evidence. A criminal procedure with a monopoly of the prosecution on it strengthens the accusatory bias and impoverishes the proof as a whole. A further spread in the share of electronic evidence in criminal procedural proving requires a change in approaches to it, a rejection of the exclusively classical rules for dealing with them, the extension of civilistic approaches to the relevant activities of the defense.

Keywords: criminal process, judicial law, electronic evidence, arbitration process, screenshot, digitalization, provision of evidence.

References

Aleksandrov, Aleksandr S. 2018a. "Problems of the theory of criminal procedural proof, which must be solved in connection with the transition to the era of digital technologies". *Sudebnaia vlast' i ugolovnyi protsess* 3: 130–139. (In Russian)

Aleksandrov, Aleksandr S. 2018b. "Russian criminal procedure dogmatism or the digital world: What will win?" *Iuridicheskaia istina v ugolovnom prave i protsesse. Materialy V*serossiiskoi *nauchno-prakticheskoi konferentsii*, 24–34. St Petersburg, Petropolis Publ. (In Russian)

Arshad, Humaira, Aman B. Jantan, Oludare I. Abiodun. 2018. "Digital forensics: Review of issues in scientific validation of digital evidence". *Journal of Information Processing Systems* 14 (2): 346–376. https://doi.org/10.3745/JIPS. 03.0095

Balashova, Anna A. 2020. "Electronic media and their use in criminal procedure evidence". PhD Thesis in Law, Akademiia upravleniia Ministerstva vnutrennikh del Rossiiskoi Federatsii. (In Russian)

Blagopoluchnaia, Kamila V. 2020. "On the new WIPO PROOF digital file verification system". *Avtorskoe parvo i smezhnye prava* 7: 37–44. (In Russian)

Boriskina, Nadezhda I. 2020. "Procedural form of evidence in modern civil litigation". PhD Thesis in Law, Lomonosov Moscow State University. (In Russian)

Golovko, Leonid V. 2019. "The Digitalization in criminal procedure: Local optimization or global revolution?" *Vestnik ekonomicheskoi bezopasnosti* 1: 15–25. (In Russian)

Grigor'ev, Viktor N. 2020. "On disturbing trends in proving the factual circumstances of an imputed act". *Rossiiskaia akademiia iuridicheskikh nauk. Nauchnye trudy* 20: 302–305. (In Russian)

Grimm, Paul, Daniel Capra, Gregory Joseph. 2017. "Authenticating digital evidence". *Baylor Law Review* 69 (1). Accessed June 12, 2021. https://www.baylor.edu/law/review/doc.php/286449.pdf.

Kerr, Orin S. 2005. "Searches and seizures in a digital world". *Harvard Law Review* 119: 531–585.

Khaidarov, Al'bert A. 2020. "The use of social networks and mobile devices capabilities for the protection of lawyers' rights and legitimate interests of suspects (accused) and identification of violations in criminal cases by prosecutors". *Aktual'nye problem rossiiskogo prava* 15 (5): 179–187. (In Russian)

Kharitonova, Yuliia S. 2020. "Platformization of justice: China's experience and the future of the world's judicial systems". *Vestnik arbitrazhnoi praktiki* 3: 3–11. (In Russian)

Mitrofanova, Margarita A. 2013. "Electronic evidence and the principle of immediacy in the arbitration process". PhD Thesis in Law, Saratovskaia gosudarstvennaia iuridicheskaia akademiia. (In Russian)

Moore, Jonathan L. 2010. "Time for an upgrade: Amending the federal rules of evidence to address the challenges of electronically stored information in civil litigation". *Jurimetrics Journal* 50: 147–193.

Myshko, Fedor G., Lyudmila P. Lyubimtseva. 2019. "Ensuring a notary of the notary's evidence in the civil process, including their occupation in the Internet network". *Vestnik Moskovskogo universiteta MVD Rossii* 6: 271–281. (In Russian)

Okonenko, Roman I. 2016. "'Electronic evidence' and the problems of ensuring the rights of citizens to protect privacy in criminal proceedings: A comparative analysis of the legislation of the United States of America and the Russian Federation". PhD Thesis in Law, Moskovskii gosudarstvennyi iuridicheskii universitet imeni O. E. Kutafina. (In Russian)

Rossinskaia, Elena R. 2019. *Selected works.* Moscow, Norma Publ. (In Russian)

Saakov, Tigran A. 2020. "Forensic author's examination of objects from the digital environment in establishing the demographic characteristics of the author". *Zakony Rossii: opyt, analiz, praktika* 4: 96–103. (In Russian)

Sergeeva, Kseniia A. 2012. "Securing evidence in civil and arbitration proceedings". PhD Thesis in Law, Ural'skaia gosudarstvennaia iuridicheskaia akademiia. (In Russian)
Sharipova, Aliia R. 2015. "Evidence in criminal and arbitration proceedings: "Unforced" differences". *Biblioteka kriminalista. Nauchnyi zhurnal* 4: 180–185. (In Russian)
Sharipova, Aliia R. 2021. "Appointment of a forensic examination in criminal cases: Is the industrial specifics justified?" *Ekspert-kriminalist* 3: 31–34. (In Russian)
Sheremet'eva, Natal'ia V., Il'ia V. Baturo, Shuan U. 2020. "Features of e-justice in the PRC". *Pravo i praktika* 2: 159–163. (In Russian)
Smekhnov, Vadim A. 2018. "The use of remote sensing images of the Earth as the evidence in criminal cases". *Vestnik Glavnogo upravleniia kriminalistiki* 1: 19–22. (In Russian)
Wang, Bo, Yuxian Liu. 2019. "Collection and judgment of electronic data evidence in criminal cases: From the perspective of investigation and evidence collection by public security organs". *Journal of Forensic Science and Medicine* 5: 187–194. https://doi.org/10.4103/jfsm.jfsm_26_19

Received: March 14, 2021
Accepted: October 28, 2022

Author's information:

Aliya R. Sharipova — PhD in Law, Assistant Professor; Nord-wind23@mail.ru