

### ДОКАЗАТЕЛЬСТВЕННОЕ ПРАВО РОССИЙСКОЙ ФЕДЕРАЦИИ И СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ В ИНФОРМАЦИОННУЮ ЭПОХУ: УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ АСПЕКТ

В статье рассматриваются современные тенденции доказательственного права Российской Федерации и Соединенных Штатов Америки, связанные с появлением информационных технологий. Особое внимание уделяется концепции электронного доказательства как перспективному направлению юридических исследований. Определяются специфические характеристики цифровых устройств (значительный объем памяти, простота копирования данных, неочевидность и относительность содержания, способность к удаленному доступу), которые необходимо учитывать для выработки новых моделей поведения участников уголовного судопроизводства в целях повышения уровня правовой защищенности граждан от чрезмерного вмешательства в их жизнь органов публичного преследования. Кратко характеризуется состояние отечественной юридической доктрины на предмет ее соответствия новым общественным реалиям и темпу научно-технического прогресса, на основании чего делается вывод о необходимости проведения дальнейших исследований в области защиты прав владельцев электронных устройств для повышения эффективности правоприменительной деятельности.

**Ключевые слова:** электронные доказательства, цифровые доказательства, защита персональных данных, тайна личной жизни, электронный носитель информации, информационные технологии, компьютерная информация, удаленный доступ, юридическая доктрина, виды доказательств, доказательственное право, уголовный процесс, право США.

Доказательственное право всегда привлекало внимание юристов, поскольку составляет стержень всей процессуальной деятельности, наполняет ее смыслом и значением [1, с. 17]. Именно доказательственное право изучает способы отражения, описания явлений действительности в такой форме, чтобы они могли составлять основу юридических умозаключений, итогом которых становится разрешение вопроса о судьбе конкретного человека, попавшего в поле внимания органов публичного преследования [2, с. 54].

Помимо этого, можно также утверждать, что доказательственное право представляет собой систему правил, которые тесно связаны с общественной реальностью, ведь именно оно предопределяет условия, порядок и пределы вторжения органов государ-

---

\* © Оконенко Р.И., 2015

Оконенко Роман Иванович (tabularasa-86@mail.ru), помощник судьи, Московский городской суд, 107076, г. Москва, Богородский вал, 8.

ственной власти в повседневную жизнь граждан. Для того чтобы указанное вмешательство воспринималось адекватно, законодатель должен четко представлять условия жизни современного человека, которые во многом зависят от уровня научно-технического прогресса. Говоря более определенно, доказательственное право должно включать в себя систему процессуальных гарантий, принимающих во внимание интересы граждан в области защиты личной жизни с учетом тенденции ко все большему использованию различных информационных технологий.

Трудно не признать, что современные способы передачи данных изменили мир настолько, что жилище и иные социально значимые для человека помещения, а также традиционные каналы связи (почта, телефон, телеграф) более не должны восприниматься как единственные объекты повышенной правовой защиты. Сегодня в кармане любого из жителей развитых стран может оказаться портативное цифровое устройство, хранящее данные, сравнимое по объему с теми, что ранее могли быть обнаружены только в отдельном помещении.

Изложенное позволяет говорить о целесообразности обращения науки о доказательствах к проблемам защиты персональных данных владельцев компьютеров и иных электронных устройств. Только принимая во внимание происходящие с обществом изменения, вызванные высокими темпами развития средств коммуникации, доказательственное право заметно повысит уровень своей эффективности как система регулирования социальных отношений.

Центральным понятием доказательственного права является доказательство и его разновидности, потому наиболее правильной для развития указанного института видится разработка концепции «электронного доказательства» как термина-аттрактора, вбирающего в себя те проблемы, с которыми сталкиваются участники уголовного процесса при собирании, проверке и оценке сведений, выраженных в цифровой форме.

В этой связи следует заметить, что в отечественной доктрине первые упоминания о компьютерной информации как доказательстве вначале были тесно связаны с появлением так называемого электронного документа [3, с. 48–51], а в последующем получили развитие в рамках гражданско-процессуальной юридической науки, чему способствовали Гражданский процессуальный кодекс Российской Федерации и Арбитражный процессуальный кодекс Российской Федерации, предусматривающие возможность использования в качестве письменных доказательств документов и материалов, выраженных в форме цифровой записи.

В отличие от гражданского процесса вопросы исследования цифровых устройств в ходе уголовного судопроизводства не так часто привлекают внимание российских юристов, что не вполне понятно, если принять во внимание важность данной отрасли права для общества в целом. Напротив, криминалистическим аспектам деятельности по получению цифровых данных уделяется важное внимание [4, с. 14], что приводит к дисбалансу в юридической доктрине — ситуации, когда существует множество криминалистических рекомендаций, серьезный правовой анализ которых не проводится.

Те же немногочисленные правовые исследования, которые имеются, часто носят описательный характер (к примеру, в них излагается содержание статей 85, 182, 183 Уголовно-процессуального кодекса Российской Федерации, касающихся работы с электронными носителями информации с небольшими пояснениями [5; 6]) либо уделяют внимание техническим аспектам деятельности тех или иных устройств, в то время как вопрос об актуальности электронных доказательств как новой правовой категории остается нераскрытым.

Таким образом, можно заключить, что электронные доказательства остаются для отечественного доказательственного права скорее неким проектом на будущее, чем состоявшейся доктринальной категорией.

В этой связи полезно обратиться к юридической науке Соединенных Штатов Америки, для которой указанный термин давно стал широко признанным среди правоведов.

Так, под электронным доказательством американские юристы понимают сведения, которые обрабатываются, хранятся или передаются любым искусственным устройством, компьютером или компьютерной системой, и которые представляют то или иное обстоятельство, имеющее значение для дела, как более или менее вероятное [7, р. 27].

При этом основными характеристиками цифровых сведений, имеющими значение для защиты прав граждан Соединенных Штатов Америки на тайну личной жизни, являются следующие их особенности.

1) Значительный объем памяти [8, р. 26]. Дело в том, что цифровое устройство, принадлежащее гражданину, может нести такой огромный массив информации о его жизни, который раньше мог бы поместиться только в отдельном помещении. Более того, сохраненная на компьютере информация может быть представлена не только текстовыми файлами, но и в качестве видео-, аудиозаписей.

2) Существенная простота копирования данных [7, р. 32]. При этом качество копирования находится на таком высоком уровне, что единственное различие между оригиналом документа и его копией может заключаться лишь во времени создания файлов.

3) Неочевидность и относительность содержания. Неочевидность содержания прежде всего обусловлена тем, что любые данные, записанные в память компьютера, отчасти являются скрытыми метаданными, которые могут содержать информацию о времени создания файла, его авторе, последних изменениях, попытках получить к нему доступ и многие другие сведения [9, с. 128]. Большинство обычных пользователей не знает о существовании этих данных, так как для их обзора необходимо обладать определенными навыками или использовать специальное программное обеспечение, в то время как для специалистов исследование такой информации не представляет какой-либо сложности. Относительность содержания электронных доказательств предполагает, что даже тот объем информации, который доступен для обзора обычным пользователям, не всегда одинаков, так как варьируется в зависимости от программного обеспечения конкретного компьютера и его настроек [7, р. 30].

4) Наконец, последняя особенность цифровых данных заключается в том, что они могут как храниться в памяти самого устройства, так и быть получены через информационно-телекоммуникационную сеть Интернет или иную коммуникационную систему [10, р. 42]. Следовательно, получая доступ к компьютеру, представитель правоохранительных органов одновременно получает доступ к источникам информации, которая может храниться удаленно.

Необходимо подчеркнуть, что указанные свойства цифровых устройств, отмеченные современными американскими учеными, действительно претендуют на роль отличительных особенностей электронных доказательств именно как юридического явления, так как имеют важное значение для реализации и защиты прав граждан на тайну личной жизни.

Так, значительный объем хранимых в памяти сведений позволяет электронному устройству стать наиболее ценным объектом охраны персональных данных, что имеет особое значение для уголовно-процессуального права как системы норм, существенная часть которых является гарантиями против чрезмерного вмешательства полиции

в жизнь граждан. До появления цифровых технологий самым информативным источником данных о ком-либо считалось жилище, правовая защита которого признана обществом настолько значимой, что оно выработало выверенную и сбалансированную систему гарантий, препятствующих кому-либо, в том числе органам публичного преследования, произвольно вторгаться в дом гражданина. Современные электронные устройства хранят настолько значительное число сведений, что они, если бы были переведены в аналоговую форму, с легкостью заполнили обычное по размерам жилое помещение. Однако в силу недавнего появления в обществе цифровых носителей их значимость для защиты тайны личной жизни пока не была в достаточной мере осознана. В результате важнейшее хранилище личной информации осталось без адекватной правовой конструкции, обеспечивающей ее защиту от чрезмерного интереса правоохранительных органов.

Легкость копирования информации также имеет важные правовые следствия, связанные прежде всего с обеспечением права пользования имуществом. Если для физического объекта нахождение в одном месте исключает существование в другом, то для информации данное утверждение неверно: практически любые объемы данных могут копироваться и передаваться без каких-либо серьезных усилий на значительные расстояния. Указанная особенность цифровой информации привела многих юристов к мысли о том, что исследование электронных доказательств возможно без их изъятия у владельца путем создания специальной копии для правоохранительных органов, либо, напротив, уже изъятая информация может быть скопирована и передана ее владельцу, пока оригинал проверяется правоохранительными органами. По последнему из указанных путей и пошел отечественный законодатель, закрепив в части 2<sup>1</sup> статьи 85, части 9<sup>1</sup> статьи 182, части 3<sup>1</sup> статьи 183 Уголовно-процессуального кодекса Российской Федерации возможность копирования содержания электронных носителей информации. Американские правоведы больше склоняются к первому из указанных вариантов [11, р. 133].

Неочевидность и относительность содержания компьютерной информации имеет юридическое значение постольку, поскольку существенным образом ограничивает граждан в возможности предвидеть, какой объем информации будет получен правоохранительными органами относительно их действий и личности в целом. Обычный человек, не обладающий специальными познаниями в информатике, как правило, не может точно сказать, как именно и куда записывается в память компьютера его активность в виртуальной среде, а главное, в каком объеме его деятельность фиксируется. Немногие, к примеру, знают, что вся стертая с компьютера информация на самом деле доступна для восстановления еще продолжительное время. Любой файл, который удален пользователем, остается на диске и помечается как готовый к записи новой информации. Пока новые сведения не записаны, старые могут быть восстановлены и всесторонне изучены. При таком положении становится понятным, что доступ к электронному устройству лица, вовлеченного в орбиту интересов правоохранительных органов, должен быть существенным ограничен различными процессуальными средствами, поскольку компьютер, помимо средства коммуникации, еще и прекрасное средство фиксации виртуальной активности гражданина.

Последняя особенность цифровых устройств – возможность получать информацию удаленно – также имеет важное значение для права, так как, получая доступ к содержанию того или иного компьютера, сотрудники правоохранительных органов могут проверить, к примеру, электронную почту владельца цифрового устройства,

то есть исследовать данные, находящиеся в другом месте, в том числе за границами государства. Данная специфическая черта отличает цифровые устройства от обычных объектов материального мира, в том числе различных контейнеров, поскольку последние могут предоставить сведения лишь о том, что содержат в себе [10, р. 43]. В настоящее время, среди американских правоведов идут дискуссии об определении критериев и пределов доступа к информации, хранящейся удаленно. В частности, предлагается ограничить число поисковых действий, которое сотрудник полиции имеет право совершить, исследуя электронное доказательство, запретить изучать данные, размещенные в сети Интернет, предоставить право на изучение телефона только при предварительном получении судебного ордера либо допустить исследование телефона без санкции органа правосудия только для установления того, не представляет ли он непосредственной опасности для полицейского, как, к примеру, орудие, с помощью которого можно физически противодействовать задержанию [10, р. 58].

Таким образом, разработка понятия электронного доказательства является перспективным направлением юридических исследований, позволяющим учесть новые общественные реалии, связанные с развитием компьютерных технологий, обеспечить адекватный механизм защиты прав граждан на тайну личной жизни в эпоху информационной революции. В этой связи представляется, что слабая проработанность концепции электронного доказательства в российском праве должна быть устранена путем изучения зарубежного опыта по указанной проблематике, его переосмысления и выработки новых теоретических воззрений в рамках российской юридической науки.

Вместе с тем следует отметить, что именно введение в уголовно-процессуальную доктрину (а впоследствии, возможно, в законодательство) понятия электронного доказательства позволит объединить все проблемные вопросы исследования цифровых устройств вокруг одного абстрактного термина. Такое объединение предоставит возможность правоведом рассматривать возникающие на практике трудности собирания, проверки и оценки электронных доказательств не отдельно, разрозненно друг от друга, но в их взаимосвязи и взаимообусловленности. Объединив обозначенные трудности в систему, преобразовав их из совокупности критических замечаний в одну концептуальную проблематику, юридическое сообщество получит возможность разрешить их комплексно, посредством конструирования особой процессуальной формы получения нового вида сведений – цифровой информации. Именно такой подход позволил бы установить баланс между интересами отдельного человека, связанными с обеспечением тайны личной жизни, и задачей эффективного расследования преступлений.

#### **Библиографический список**

1. Шейфер С.А. Доказательства и доказывание по уголовным делам. М., 2012. 238 с.
2. Доля Е.А. Формирование доказательств на основе результатов оперативно-розыскной деятельности. М., 2013. 373 с.
3. Лисиченко В.К. Криминалистическое исследование документов (правовые и методологические проблемы): дис. ... д-ра юрид. наук. Киев, 1973. 427 с.
4. Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях. СПб., 1997. 88 с.
5. Вехов В.Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22–24.

6. Зуев С.В. Электронное копирование информации – регламентация в УПК // *Законность*. 2013. № 8. С. 22–23.
7. *Electronic evidence: third edition* / ed by S. Mason. Croydon, 2012. 934 p.
8. Kessler G.C. *Judge' Awareness, Understanding, and Application of Digital Evidence*. Miami, 2010. 182 p.
9. Леготин Е.Ю. Организация метаданных в хранилище данных // *Научный поиск. Технические науки: материалы третьей науч. конф. аспирантов и докторантов*. Челябинск: Издательство Южно-Уральского государственного университета, 2011. Т. 2. С. 128–132.
10. Adam M.G. The iphone meets the fourth amendment // *UCLA Law Review*. 2008. Vol. 27. P. 27–58.
11. Kerr O.S. Search warrants in an era of digital evidence // *Mississippi Law Journal*. 2005. December. P. 85–145.

## References

1. Sheyfer S.A. Evidences and proving in criminal cases. M., 2012, 238 p. [in Russian].
2. Dolya E.A. Formation of evidence on the basis of results of operational and search activity. M., 2013, 373 p. [in Russian].
3. Lisichenko V.K. *Kriminalisticheskoe issledovanie dokumentov (pravovye i metodologicheskie problemy): dis. ... d-ra iurid. nauk* [Forensic processing of documents (legal and methodological problems): Doctor's of Law thesis]. Kiev, 1973, 427 p. [in Russian].
4. Kushnirenko S.P., Panfilova E.I. Criminally-remedial methods of seizure of computer information with regard to economic crimes. SPb., 1997, 88 p. [in Russian].
5. Vehov V.B. Work with digital evidences in conditions of changed criminal procedure legislation. *Rossiiskii sledovatel'* [Russian investigator], 2013, no. 10, pp. 22–24 [in Russian].
6. Zuev S.V. Digital copying of information – Criminal Procedure Code regulation. *Zakonnost'* [Legitimacy], 2013, no. 8, pp. 22–23 [in Russian].
7. *Electronic evidence: third edition*. S. Mason (Ed.). Croydon, 2012, 934 p. [in English].
8. Kessler G.C. *Judge' Awareness, Understanding, and Application of Digital Evidence*. Miami, 2010, 182 p. [in English].
9. Legotin E.U. Organization of metadata in data storage. *Nauchnyi poisk. Tekhnicheskie nauki: materialy tret'ei nauch. konf. aspirantov i doktorantov* [Scientific inquiry. Engineering sciences: materials of the third scientific conference of postgraduate students and doctoral students]. Chelyabinsk, Izdatel'stvo Iuzhno-Ural'skogo gosudarstvennogo universiteta, 2011, Vol. 2, pp. 128–132 [in Russian].
10. Adam M.G. The iphone meets the fourth amendment. *UCLA Law Review*, 2008, Vol. 27, pp. 27–58 [in English].
11. Kerr O.S. Search warrants in an era of digital evidence. *Mississippi Law Journal*, 2005, December, pp. 85–145 [in English].

*R.I. Okonenko\****RUSSIAN AND AMERICAN EVIDENCE LAW IN THE INFORMATION AGE:  
CRIMINAL PROCEDURAL LAW ASPECT**

In the article modern tendencies in Russian and American evidence law that are determined by appearance of informational technologies are viewed. Special attention is paid to the digital evidence conception as promising direction for legal research. Peculiar characteristics of digital devices (such as great volume of memory, data copying simplicity, unobviousness and content relativity, remote access to information) are defined by the author for making new models of personal criminal procedural activity, that enhance level of legal protection against public agencies unreasonable intrusion into private life. Also author briefly describes state of Russian legal science in order to define its incompliance with social realia, speed of technological progress and conclude that additional research in sphere of privacy is required for making law-enforcement activity more effective.

**Key words:** digital evidence, digital evidence, protection of personal data, privacy, electronic data storage device, information technologies, computer information, remote access, legal doctrine, types of evidences, evidence law, criminal procedure, USA law.

---

\* *Okonenko Roman Ivanovich* (tabularasa-86@mail.ru), assistant judge, Moscow City Court, 8, Bogorodsky Val, Moscow, 107076, Russian Federation.