

DOI: <http://dx.doi.org/10.21686/2411-118X-2025-4-141-145>

Допустимость электронных доказательств, полученных в результате поисково-познавательной деятельности в сети Интернет

А. В. Константинов

кандидат юридических наук, доцент, доцент кафедры
уголовного права, уголовного процесса и правоохранительной деятельности РУТ (МИИТ).
Адрес: ФГАОУ ВО «Российский университет транспорта»,
127994, Москва, ул. Образцова, д. 9, строение 9.
E-mail: alexk_pochta@mail.ru

Е. В. Поликарпова

старший преподаватель кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России им. В. Я. Кикотя.
Адрес: ФГКОУ ВО «Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя»,
117437, Москва, Академика Волгина ул., д. 12.
E-mail: policewoman1980@rambler.ru

Admissibility of Electronic Evidence Obtained as a Result of Research and Learning Activities on the Internet

A. V. Konstantinov

PhD, Associate Professor, Associate Professor of the Department
of Criminal Law, Criminal Procedure and Law Enforcement Activities of RUT (MIIT).
Address: Federal State Institution of Higher Education «Russian University of Transport»,
9 Obratsova Street, Building 9, Moscow, 127994, Russian Federation.
E-mail: alexk_pochta@mail.ru

E. V. Polikarpova

Senior Lecturer of the Department of Combating Crimes
in the Field of Information and Telecommunication Technologies
of Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot.
Address: Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot,
12 Academic Volgin Str., Moscow, 117437, Russian Federation.
E-mail: policewoman1980@rambler.ru

Поступила 13.11.2025 Принята к печати 30.11.2025

Аннотация

Статья посвящена исследованию проблемы использования информации, полученной в ходе поисково-познавательной деятельности в сети Интернет (OSINT), в качестве допустимых доказательств в судопроизводстве. Анализируются правовые, технические и процессуальные аспекты, рассматриваются российские и зарубежные подходы. Особое внимание уделяется критериям законности сбора информации, включая требования к «технической чистоте» методов и этическую оценку процесса поиска. Рассматривается проблема достоверной фиксации динамичного цифрового контента. Поднимается вопрос недостаточности простых скриншотов, обосновывается необходимость использования криптографических средств подтверждения времени создания и целостности данных (в частности, протоколов типа RFC 3161). Проведен сравнительно-правовой анализ подходов к регулированию сбора открытых данных в различных правовых системах: доктрина «open fields» в США, регламентация защиты данных в Европейском союзе (GDPR) и смешанный подход в Индии. На основе анализа российской практики выявлены ключевые недостатки текущего регулирования, приводящие к необходимости частого назначения судебных экспертиз для верификации электронных доказательств. В заключение формулируется вывод о необходимости комплексного

совершенствования законодательства России и внедрения технических стандартов для интеграции OSINT-инструментария в доказательный процесс.

Ключевые слова: электронные доказательства, допустимость доказательств, сеть Интернет, поисково-познавательная деятельность, цифровые доказательства, открытые источники информации.

Abstract

The article is devoted to the study of the problem of using information obtained in the course of search and cognitive activity on the Internet (OSINT) as admissible evidence in court proceedings. The author analyzes legal, technical and procedural aspects, examines both Russian and foreign approaches. Particular attention is paid to the criteria for the legality of information collection, including requirements for the "technical purity" of methods and the ethical assessment of the search process. The author considers the problem of reliable fixation of dynamic digital content. The issue of the insufficiency of simple screenshots is raised and the need to use cryptographic means of confirming time and data integrity (in particular, protocols such as RFC 3161) is justified. A comparative legal analysis of approaches to regulating the collection of open data in various legal systems has been carried out: the "open fields" doctrine in the United States, the Data protection Regulation in the European Union (GDPR) and a mixed approach in India. Based on the analysis of Russian practice, key shortcomings of current regulation have been identified, leading to the frequent need to appoint forensic examinations to verify electronic evidence. In conclusion, the conclusion is formulated about the need for comprehensive improvement of the legislation of the Russian Federation and the introduction of technical standards for the integration of OSINT tools into the evidence-based process.

Keywords: electronic evidence, admissibility of evidence, the Internet, search and learning activities, digital evidence, open sources of information.

Современная цифровая трансформация обусловила кардинальные изменения в характере доказывания по уголовным, гражданским и административным делам. Особую роль при этом играют электронные доказательства – информация, зафиксированная в цифровой форме и полученная в результате взаимодействия с информационными и телекоммуникационными сетями, в первую очередь с сетью Интернет. В условиях массового распространения цифровых платформ, соцсетей, блокчейн-технологий и облачных сервисов возрастает объем потенциально значимой доказательственной информации, доступной в открытых источниках. Однако именно легкость доступа к таким данным порождает серьезные вызовы в плане обеспечения их допустимости в судебном процессе.

Под поисково-познавательной деятельностью в сети Интернет понимается целенаправленный процесс сбора, анализа и интерпретации информации из открытых источников, осуществляемый правоохранительными органами и частными лицами в целях установления обстоятельств, имеющих юридическое значение. Ключевой проблемой, определяющей допустимость получения сведений таким образом, является соответствие их требованиям, установленным процессуальным законодательством, и способность противостоять возражениям относительно подлинности, целостности и происхождения информации.

Отсутствие в российском праве четко регламентированного правового статуса электронных доказательств, полученных вне рамок следственных действий, а также противоречивость судебной практики в их оценке подчеркивают актуальность данной проблематики. Электронные доказательства и так называемые электронные образы документов затрагиваются, например, в Постановлении Пленума Верховного Суда Российской Федерации от 26 декабря 2017 г. № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов»¹. Между тем зарубежные юрисдикции, особенно англосаксонские, накопили значительный опыт регулирования подобных вопросов, что позволяет выявить тенденции и выработать сбалансированную модель допустимости подобных доказательств.

В российском законодательстве понятие «электронное доказательство» не закреплено в явной форме; вместо этого, согласно статье 74 Уголовно-процессуального кодекса Российской

¹ Постановление Пленума Верховного Суда Российской Федерации от 26 декабря 2017 г. № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов». – URL: <https://www.vsr.ru/files/26294/>

Федерации (далее – УПК РФ) и статье 55 Гражданского процессуального кодекса Российской Федерации (далее – ГПК РФ), используется термин «иные документы» и «предметы, содержащие информацию в электронной форме». Это порождает проблемы при квалификации доказательств, полученных в сети Интернет, и создает правовую неопределенность, особенно в случаях, когда доказательства получены не следователем, а частным лицом или даже противной стороной в судебном разбирательстве.

В отличие от российской модели, в США действует Федеральное правило доказывания № 902 (FRE 902)¹, которое предусматривает категории самодостовверяющихся доказательств, включая электронные записи, подтвержденные цифровыми сертификатами или иными средствами целостности. Аналогичный подход реализован в Канаде (Canada Evidence Act, Part II)² и Австралии (Evidence Act 1995)³. Такие нормы позволяют признавать допустимыми электронные доказательства без необходимости вызова дополнительных свидетелей, если посредством специальных технических механизмов подтверждена подлинность этих данных.

Значительный вклад в теоретическое осмысление природы электронных доказательств внесли такие исследователи, как Э. Кейси, чьи работы подчеркивают необходимость дифференциации между данными и доказательствами: данные становятся доказательствами лишь после их интерпретации в контексте расследуемого события и проверки на соответствие критериям допустимости [5]. В российской науке аналогичная мысль высказывается рядом ученых, которые указывают на то, что «электронное доказательство не существует в вакууме — оно обретает юридическое значение лишь при наличии процессуальной формы и подтверждения источника» [2; 4].

Таким образом, электронное доказательство не может быть признано допустимым исходя лишь из его содержания; его юридическая сила зависит от соблюдения процессуальных и техни-

ческих требований при сборе, фиксации и представлении в суд.

Допустимость доказательства в российском процессуальном праве определяется его соответствием требованиям, предусмотренным статьей 75 УПК РФ (недопустимыми являются доказательства, полученные с нарушением требований закона). При этом критерий «нарушения закона» в контексте поисково-познавательной деятельности в интернете трактуется весьма неоднозначно. С одной стороны, сбор открытой информации, не ограниченной авторскими или иными правами, формально не нарушает закон. С другой — при отсутствии надлежащей фиксации, верификации и документирования процесса сбора возникает риск признания доказательства недопустимым.

В зарубежной практике используется более гибкий подход, основанный на концепции “chain of custody” (цепочка хранения) и “authenticity” (подлинность). Так, в решении по делу Лоррейн против «Маркел Америкэн Иншуренс Ко.» суд США сформулировал пять критериев допустимости электронных доказательств:

- подлинность;
- отсутствие нарушения правила “hearsay” (не допускаются свидетельские показания «со слов»);
- соответствие требованиям оригинала/копии;
- отсутствие нарушения правила о недопустимости косвенных доказательств;
- баланс между доказательственной ценностью и риском несущественных или предвзятых выводов⁴.

Особую сложность представляет ситуация, когда электронные доказательства получены вне рамок деятельности правоохранительных органов. Российская судебная практика в таких случаях склонна исключать подобные материалы из числа допустимых, ссылаясь на нарушение процессуального порядка.

Технические аспекты допустимости электронных доказательств, полученных в ходе OSINT-деятельности, также требуют отдельного рассмотрения. Согласно рекомендациям ENFSI (European Network of Forensic Science Institutes), при сборе открытой информации необходимо фиксировать:

¹ Federal Rules of Evidence, Rule 902 (as amended Dec. 1, 2017). — URL: https://www.uscourts.gov/sites/default/files/evidence-rules-procedure-dec2017_0.pdf

² Canada Evidence Act, Part II. — URL: <https://lois-laws.justice.gc.ca/eng/acts/C-5/index.html>

³ Evidence Act 1995. — URL: <https://www.legislation.gov.au/C2004A04858/2016-05-01/text>

⁴ Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007). — URL: <https://www.courtlistener.com>

- точное время и дату сбора;
- URL-адрес или уникальный идентификатор источника;
- метаданные (если доступны);
- среду, в которой производился сбор (браузер, операционная система, используемое ПО);
- хеш-сумму полученной информации для подтверждения целостности.

Отсутствие хотя бы одного из этих элементов может поставить под сомнение надежность доказательства.

Этическое измерение также играет важную роль. Поисково-познавательная деятельность не должна превращаться в слежку, хакерскую атаку или нарушение права на частную жизнь. Принцип соразмерности, закрепленный в статье 8 Европейской конвенции о правах человека [5], требует, чтобы сбор информации из открытых источников не затрагивал сферу интимной жизни, если это не обусловлено необходимостью расследования преступления.

Поисково-познавательная деятельность в сети Интернет представляет собой систематизированный процесс сбора, анализа и интерпретации информации из источников, доступ к которым не ограничен технически или юридически. К таким источникам относятся: веб-сайты, социальные сети, открытые базы данных, новостные агрегаторы, архивы (например, Wayback Machine), а также публичные записи (например, реестры юридических лиц или судебных актов).

Важно провести грань между поисково-познавательной деятельностью и следственными действиями. Согласно статье 164 УПК РФ, получение доказательств возможно лишь в рамках предусмотренных законом процессуальных действий: осмотра, обыска, выемки, допроса и т. д. Однако поисково-познавательная деятельность не является следственным действием, поскольку не предполагает вмешательства в сферу прав и свобод граждан. Тем не менее, если в результате такой деятельности выявляется информация, имеющая значение для дела, она может быть использована как повод для производства следственных действий.

Таким образом, поисково-познавательная деятельность в рамках открытых источников допустима, если:

- источник информации публичен;
- доступ к нему не ограничен;

- сбор информации не сопровождается техническим вмешательством (например, взломом, обходом капчи, подделкой user-agent);
- информация не используется в нарушение этических норм.

Для обеспечения допустимости электронных доказательств, полученных в ходе поисково-познавательной деятельности, необходимо строго соблюдать методологию их фиксации. Однако простой скриншот без метаданных и подтверждения целостности в большинстве случаев признается недостаточным доказательством.

Особое внимание следует уделить проблеме временной привязки. В условиях, когда информация в сети Интернет может быть изменена или удалена в любой момент, доказательство должно содержать точное указание времени его получения. В этом контексте перспективным представляется использование протоколов, таких как RFC 3161 (Time-Stamp Protocol)¹, позволяющих получать юридически значимые временные метки от доверенных третьих лиц.

В Китае и других странах с авторитарной моделью правления акцент делается на контроле над информацией, и любая поисково-познавательная деятельность вне официальных каналов может быть расценена как угроза национальной безопасности. В Индии наблюдается смешанный подход: Верховный суд в деле «К.С. Путтасвами против Союза Индии» от 24 августа 2017 г. (Justice K.S. Puttaswamy v. Union of India)² признал право на приватность фундаментальным, но при этом допустил использование открытых данных в целях расследования преступлений.

В Европейском союзе действует сбалансированный подход, учитывающий и интересы правосудия, и право на приватность. Статья 6 Регламента Европейского парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г.³ о защите физических лиц при обработке персо-

¹ RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol, TSP). – URL: <https://standards.globalspec.com/std/1512539/ietf-rfc-3161>

² Дело «К. С. Путтасвами против Союза Индии» от 24 августа 2017 г., Writ Petition (Civil) No. 494 of 2012. – URL: <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/02/Puttaswamy-v.-Union-of-India-II-RU.pdf>

³ Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных. – URL: <https://eur-lex.europa.eu/>

нальных данных и о свободном обращении таких данных (Регламент GDPR) допускает обработку персональных данных, если они «публично доступны», однако требует соблюдения принципа цели и соразмерности.

Сравнительный анализ показывает, что в англосаксонских системах права электронные доказательства, полученные из открытых источников, имеют более высокий шанс быть признанными допустимыми при условии соблюдения процедурных норм. В США действует доктрина открытых пространств ("open fields"), согласно которой информация, доступная без нарушения границ частной собственности (в том числе в цифровом пространстве), может свободно использоваться в качестве доказательства.

Российская модель находится в промежуточном состоянии: с одной стороны, признается возможность использования открытой информа-

ции, с другой – отсутствует четкий правовой механизм ее реализации. В условиях сомнений в подлинности электронных доказательств, полученных в ходе поисково-познавательной деятельности в сети Интернет, ключевую роль играет назначение судебной экспертизы.

Электронные доказательства, полученные в результате поисково-познавательной деятельности в сети Интернет, обладают высокой потенциальной доказательственной силой, однако их допустимость в российском процессе остается проблематичной из-за отсутствия четкого правового регулирования, технических стандартов фиксации и методологической базы. Только при условии комплексного подхода, объединяющего юридические, технические и этические аспекты, возможно обеспечение баланса между эффективностью правосудия и защитой прав граждан в условиях цифровой эпохи.

Список литературы

1. Андреева Ю. И. Электронные доказательства в уголовном процессе // Закон и право. – 2025. – № 8. – С 147–152.
2. Основы теории электронных доказательств : монография / под редакцией С. В. Зуева. – Москва : Юрлитинформ, 2019.
3. Рамалданов Х. Х. Особенности изъятия электронных носителей информации в уголовном процессе // Экономика. Право. Общество. – 2025. – № 2. – С. 71–75.
4. Смирнов А. В. Электронные доказательства, электронное доказывание, искусственный интеллект: что далее? // Уголовное судопроизводство. – 2024. – № 1. – С. 24–31.
5. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. – Waltham, MA : Academic Press, 2011.