Научная статья
УДК 34:004:347:004.4
EDN: https://elibrary.ru/jqhnur
DOI: https://doi.org/10.21202/jdtl.2025.20

Электронные доказательства как самостоятельный правовой феномен: теоретические основы и европейская практика

Гергана Варбанова

Высшее военно-морское училище имени Николы Вапцарова, Варна, Болгария

Ключевые слова

аутентичность,
вещественные доказательства,
доказательства,
европейское законодательство,
право,
процессуальные действия,
судебное разбирательство,
цифровая информация,
цифровые технологии,
электронные доказательства

Аннотация

Цель: исследование направлено на разработку новой теоретической основы, которая бросает вызов традиционной классификации электронных доказательств как подвида вещественных доказательств и предлагает рассматривать их как качественно новый правовой феномен с собственной независимой правовой природой в контексте применимого европейского законодательства.

Методы: в работе применяется доктринальный метод для юридического анализа применимых европейских нормативных актов, включая Регламент (ЕС) 2023/1543 и Регламент (ЕС) 910/2014 (eIDAS), и их непосредственного применения в национальных правовых системах государств – членов Европейского союза. Для выявления различий между теоретическими взглядами и прецедентным правом используется сравнительно-правовой подход. Проводится технологический анализ цифровой информации и поясняются конкретные примеры, иллюстрирующие проблемы, связанные со сбором и использованием электронных доказательств в рамках европейского законодательства.

Результаты: автор предлагает новое доктринальное понимание электронных доказательств как самостоятельной категории доказательств, отличающейся от традиционных вещественных доказательств цифровой природой и специфическими характеристиками. Внедрение европейских регламентов требует переосмысления правовой природы электронных доказательств как качественно отличного правового явления. Установлено, что отношение к электронным доказательствам как к вещественным создает риск правовой неопределенности, а отсутствие соответствующего правового регулирования препятствует эффективному правоприменению.

Научная новизна: в исследовании впервые предлагается преодолеть устоявшуюся парадигму и выделить электронные доказательства как самостоятельную правовую категорию в системе видов доказательств. Обосновывается уникальная цифровая природа электронных

доказательств и необходимость создания независимой правовой базы в различных национальных законодательствах. Предложено совершенствование научной терминологии с использованием термина «электронные доказательства», соответствующего юридическим определениям в рассматриваемых нормативных правовых актах, вместо устаревшего термина «цифровые доказательства».

Практическая значимость: работа содержит конкретные рекомендации практического характера для использования электронных доказательств в процедурах их идентификации, хранения, представления и анализа в различных судебных разбирательствах в соответствии с применимым наднациональным законодательством. Исследование способствует преодолению устаревших представлений о правовой природе электронных доказательств и их неверного отождествления с вещественными доказательствами, что имеет важное значение для эффективного правоприменения в государствах – членах Европейского союза.

Для цитирования

Варбанова, Г. (2025). Электронные доказательства как самостоятельный правовой феномен: теоретические основы и европейская практика. *Journal of Digital Technologies and Law*, *3*(3), 497–511. https://doi.org/10.21202/jdtl.2025.20

Содержание

Введение

Электронные доказательства имеют особую природу, что отличает их от других видов доказательств, существующих в аналоговом мире. Это подтверждается фактами, которые имели место в прошлом, но относятся и к настоящему. Особенность электронных доказательств заключается в том, что они сохраняются неизменными в течение длительного периода времени, однако для них характерна и динамика, т. е. их содержание может отличаться от состояния в момент существования факта, который они удостоверяют. Часто содержание электронных доказательств изменяют, чтобы скрыть информацию или намеренно исказить ее, и отследить эти изменения нелегко. Электронные доказательства содержат цифровую информацию, закодированную в виде двоичных данных (последовательности единиц и нулей), и это бросает вызов юридической теории и практике, поскольку юридическая наука оказывается неразрывно связанной с техническими особенностями электронных доказательств

как нового правового феномена. Цифровую информацию нельзя рассматривать как материальный объект, ее нельзя воспринимать непосредственно, она не является объектом физического мира. Все это создает серьезные проблемы для юридической теории и практики.

В статье представлена новая теоретическая база, позволяющая пересмотреть традиционную классификацию электронных доказательств как подмножества вещественных доказательств. Автор предлагает изменить парадигму понимания правовой природы электронных доказательств и рассматривает их как новое правовое явление, имеющее свою собственную независимую правовую природу и требующее наднационального регулирования. Исследование фокусируется на применимом европейском законодательстве, включая Регламент (ЕС) 2023/1543, Регламент (ЕС) 910/2014 (eIDAS), и на тех проблемах, которые ставит перед нами указанная новая теория правовой природы электронных доказательств.

В работе использован доктринальный метод правового анализа применимых нормативных актов ЕС и практики их применения в национальных правовых системах государств Евросоюза. Для прояснения различий между теоретическими положениями и прецедентным правом, возникающих при применении наднациональных правовых норм, применяется сравнительный подход. Автор анализирует технологические аспекты, связанные с природой цифровой информации, и приводит конкретные примеры, иллюстрирующие проблемы, связанные со сбором и использованием электронных доказательств в контексте европейского законодательства.

В статье предпринята попытка предложить пути преодоления старой парадигмы и выделить электронные доказательства в качестве самостоятельной правовой категории в системе видов доказательств, а также отграничить их от вещественных доказательств. Приводятся аргументы в пользу уникальной цифровой природы электронных доказательств и необходимости создания независимой правовой базы в рамках национальных законодательств. Автор предлагает усовершенствовать научную терминологию, а именно использовать термин «электронные доказательства», который соответствует юридическим определениям, приведенным в рассматриваемых нормативных актах, и отказаться от использования устаревшего термина «цифровые доказательства».

1. Классическая теория вещественных доказательств

Данная теория определяет вещественные доказательства как материальные объекты, которые воспроизводят факты, имеющие отношение к делу, или позволяют делать доказательные выводы об этих фактах. Они относятся к событиям, которые произошли в прошлом, но имеют значение в настоящем и связаны с процессом доказывания. Например, Mubarik (2019) рассматривает в качестве вещественных доказательств любые предметы, материалы, отпечатки пальцев и различные вещества (в том числе телесные), собранные на месте преступления, которые имеют отношение к расследованию и могут способствовать прояснению обстоятельств дела. Чтобы доказательство можно было квалифицировать как вещественное, оно должно иметь материальную природу и восприниматься с помощью органов чувств человека. Некоторые теоретики утверждают, что физический носитель несет цифровую информацию (например, диск, USB-носитель, жесткий диск), а значит, может рассматриваться как вещественное доказательство (Pastukhov, 2015; Dmitrieva & Pastukhov, 2023).

Этот традиционный подход имеет недостатки и подвергается серьезной критике, поскольку электронные доказательства, рассматриваемые в качестве цифровой информации, не всегда имеют материальную природу и могут существовать исключительно в цифровой среде, не будучи объективированными на физическом носителе – например, в виде записи на облачном сервере. Электронные доказательства часто не существуют в аналоговой форме и не являются частью материального мира в классическом смысле этого слова.

2. Европейское законодательство, применимое к электронным доказательствам

Стремясь определить и унифицировать понимание специфической правовой природы электронных доказательств, Европейский союз принял Регламент (ЕС) 2023/1543, который имеет прямое применение и содержит юридическое определение понятия «электронные доказательства». Такое законодательное решение не случайно, оно направлено на преодоление различий в толковании понятий в национальных законодательствах государств-членов и на достижение единого понимания правовой природы электронных доказательств.

Регламент определяет «электронные доказательства» как данные абонента, данные о трафике или данные о контенте, хранящиеся поставщиком услуг или от имени поставщика услуг в электронной форме. Этот законодательный подход отличается нейтральностью и не содержит исчерпывающего перечня всех видов цифровой информации, которые могут быть квалифицированы как электронные доказательства. Регламент выделяет лишь электронные доказательства как особый вид цифровой информации, которая хранится или передается поставщиками услуг в контексте предоставления ими цифровых услуг и для целей уголовного судопроизводства. Файлы или другие цифровые данные, хранящиеся пользователями локально, не подпадают под действие Регламента (ЕС) 2023/1543. Такие данные могут подпадать под определение «электронных документов» в соответствии с Регламентом (ЕС) 910/2014 (eIDAS), если они содержат информацию, имеющую юридическое значение для различных гражданских, коммерческих, административных или иных общественных отношений.

Регламент (ЕС) 910/2014 (eIDAS) определяет «электронный документ» как любой контент, хранящийся в электронной форме, в частности, в виде текста, звукозаписи, изображения или аудиовидеозаписи. В контексте eIDAS электронный документ – это носитель цифровой информации, относящейся к гражданским, административным, коммерческим или иным общественным отношениям. Достаточным условием является содержание в электронном документе информации, имеющей юридическое значение, независимо от того, был ли документ создан случайно или намеренно для целей конкретного правоотношения. Статья 46 Регламента (ЕС) 910/2014 предусматривает, что электронный документ имеет такую же доказательственную ценность, как и другие виды доказательств. Цитируемая норма императивно гласит, что недопустимо отрицать доказательственную ценность электронного документа только потому, что он представлен в электронной форме. Это, в свою очередь, обеспечивает правовую определенность в трансграничных спорах, включая арбитраж (Ferreira & Gromova, 2024). На практике Регламент обязывает государства-члены признавать действительность электронных документов в качестве

допустимых доказательств в различных судебных разбирательствах (Nekrošius, 2021; Daniel & Daniel, 2012)[1].

В контексте нашего исследования следует сравнить понятия «электронное доказательство» по смыслу Регламента (ЕС) 2023/1543 и «электронный документ» по смыслу Регламента (ЕС) 910/2014. Электронные доказательства в соответствии с Регламентом (ЕС) 2023/1543 охватывают широкий спектр цифровой информации – данные об абонентах, трафике и контенте, которые могут включать структурированные или неструктурированные данные, метаданные или содержание сообщений – и отличаются от электронных документов. Сфера действия Регламента (ЕС) 2023/1543 ограничена конкретными делами в уголовном судопроизводстве – хранением и предоставлением электронных доказательств, и только в отношении цифровой информации, хранящейся поставщиками услуг или от их имени.

С другой стороны, понятие «электронный документ» по смыслу Регламента (ЕС) 910/2014 (eIDAS) имеет более узкое технологическое применение, поскольку оно, по сути, относится к цифровому контенту, воспринимаемому как «документ», но его юридическая применимость значительно шире. «Электронный документ» не ограничивается сферой уголовного судопроизводства или данными, хранящимися у конкретных поставщиков услуг, но применим ко всем отраслям права: гражданскому, коммерческому, административному и уголовному (Kirkov, 2022; Berube et al., 2025; Shin et al., 2025). Поэтому можно сделать вывод, что электронные доказательства в соответствии с Регламентом 2023/1543 представляют собой специализированный тип цифровой информации, предназначенной для целей уголовного судопроизводства, и имеют более узкую сферу регулирования. Напротив, электронные документы в соответствии с Регламентом 910/2014 имеют более широкую сферу применения и значение, поскольку их допустимость в качестве доказательств зависит не от конкретного контекста уголовного судопроизводства, не от места хранения или источника данных, а от соблюдения принципов, установленных законодательством ЕС для процессов электронной идентификации, аутентификации и доверительных услуг, включая типы электронных подписей, используемых в электронных документах.

Примечательно сходство определений «данных контента» в Регламенте (ЕС) 2023/1543 и «электронных документов» в eIDAS. Разница заключается в контексте и целях: «данные контента» в соответствии с Регламентом 2023/1543 ориентированы на цифровую информацию, которая передается и хранится поставщиками цифровых услуг и которая должна храниться и, соответственно, предоставляться для нужд уголовного правосудия, в то время как определение «электронного документа» в eIDAS относится к признанию юридической ценности и использованию электронных документов во всех сферах общественной жизни.

Определение электронных доказательств по смыслу Регламента (ЕС) 2023/1543 не является исчерпывающим, а лишь описывает некоторые виды цифровой информации, которые могут рассматриваться как электронные доказательства. Этот подход идентичен определению понятия «электронный документ» в Регламенте (ЕС) 910/2014 – любой контент, хранящийся в электронной форме, в частности текст, звукозапись, изображение или аудиовизуальная запись. В обоих случаях перечень не является исчерпывающим, ведь технологии развиваются. При регулировании

[1] Varbanova, G. (2020). Legal regime of electronic documents. Varna: Dangrafik Publishing.

общественных отношений в сфере информационных технологий законодательный подход должен быть гибким, учитывая динамику технологического развития. Технологическое развитие подразумевает появление новых типов электронных доказательств и электронных документов, которые нельзя исключить из сферы действия Регламента (ЕС) 2023/1543 или eIDAS просто потому, что они не определены в явном виде как электронные доказательства или электронные документы соответственно.

3. Определение и правовая природа электронных доказательств

Электронные доказательства – это один из ключевых инструментов в процессе доказывания, который требует особого подхода к их сбору, анализу и правовой оценке. Такой подход должен учитывать интенсивное развитие технологий, а также специфические особенности электронных доказательств в контексте процесса нормотворчества (Begishev et al., 2020).

До принятия Регламента (ЕС) 2023/1543 теоретические исследования определяли электронные доказательства как любую информацию, хранящуюся или передаваемую в цифровой форме, которая может быть использована в качестве доказательства. Традиционно некоторые авторы считают электронные доказательства вещественными, поскольку содержащаяся в них информация объективирована на конкретном материальном носителе. Согласно этому подходу, доказательственную ценность определяют физические характеристики носителя, а не сама информация (электронные доказательства), записанная на нем. Несмотря на кажущуюся правдоподобность, эта концепция является ошибочной, поскольку не учитывает и не отражает специфическую природу электронных доказательств как цифровой информации, которая обладает своими уникальными характеристиками (Wu et al., 2025)[2].

В более поздних исследованиях также высказывается представление о том, что электронные документы являются особой категорией квазивещественных доказательств. По мнению ряда авторов (Bufetova, 2023; Guo, 2022), электронный документ в качестве вещественного доказательства – это документ, который существует в электронном виде, содержит информацию, относящуюся к делу, и записан на электронном носителе, позволяющем воспроизводить и использовать эту информацию в процессе доказывания. Это определение показывает, что электронный документ принадлежит к особому виду квазивещественных доказательств, в котором важна информация, содержащаяся на материальном носителе, а не его материальные характеристики.

Такая неопределенность возникает из-за непонимания того, как создается, изменяется, хранится и удаляется цифровая информация. Цифровая информация может храниться на различных носителях: жестком диске, USB-устройстве, в облаке, на сервере – или передаваться по электронным каналам, но информация не идентична самому носителю. Файл может быть сохранен на компьютере или другом техническом носителе, скопирован, передан или удален, но компьютер или носитель, на котором записан файл, не является вещественным доказательством, тем более что

[2] Varbanova, G. (2024). The significance of electronic evidence in the context of cybersecurity and national security. Print Master Publishing.

информация может быть записана на облачном сервере и доступна через компьютер или другое устройство.

Из определений электронных доказательств и электронных документов видно, что они не имеют материальной (осязаемой) природы, а представляют собой цифровую запись, поэтому их можно определить как разновидность нематериальных доказательств (Vuchkov, 2023; Horsman, 2021). Для того чтобы иметь возможность определить электронные доказательства как новое правовое явление, необходимо прояснить их цифровую природу и способ создания, передачи, хранения, записи и удаления цифровой информации.

Цифровая информация – это данные в двоичном коде, последовательность нулей и единиц, обрабатываемая информационными системами (компьютером, интеллектуальным устройством и т. д.). Таким образом, текст, изображения, звук или видео, записанные на техническом носителе, представляют собой цифровую информацию в двоичном коде, которая может быть воспринята органами чувств человека с помощью обычных средств через использование общепринятых стандартов преобразования и воспроизведения информации, с помощью которых нули и единицы могут восприниматься в виде текста, изображений или аудиофайлов.

Чтобы собранные электронные доказательства был приняты в суде, необходимо обеспечить полную целостность и идентичность информационных данных, с тем чтобы гарантировать их подлинность, целостность содержания и неизменность данных. Только при соблюдении этих требований электронные доказательства могут быть приняты в качестве действительных и надежных доказательств в судебном разбирательстве.

4. Аутентичность, целостность и доказательное значение электронных документов

Для современного мира характерно постоянное увеличение числа правоотношений, которые возникают, развиваются и прекращаются в электронной среде. Каждый день исключительно в электронном виде заключается множество контрактов, потребители пользуются онлайн-сервисами, совершают электронные платежи, и даже судебные разбирательства теперь проводятся с помощью видеоконференций и других инструментов электронного мира. Практически все сферы общественной и экономической жизни тесно связаны с использованием электронных средств коммуникации, обработки и хранения информации.

Киберпространство стало зоной коммерции, которая выходит за рамки физических границ, но в то же время представляет собой центр притяжения для совершения многочисленных новых и ранее неизвестных компьютерных преступлений.

Электронные доказательства – будь то электронные документы, записи актов коммуникации, лог-файлы, метаданные или другие формы цифровой информации – являются неотъемлемой частью правовых отношений в электронной среде и имеют существенное значение для раскрытия преступлений, совершаемых в киберпространстве. Для доказывания фактов, независимо от того, идет ли речь о гражданских или коммерческих правоотношениях или о преступлениях, совершенных в киберпространстве, требуется гарантировать подлинность, целостность и неизменность электронных доказательств. Это достигается путем применения соответствующих технических и организационных мер.

Ключевой проблемой при представлении, анализе и принятии электронных доказательств в ходе судебных разбирательств (гражданских, уголовных или административных) являются подлинность, целостность и доказательная ценность электронных доказательств и электронных документов. В современном цифровом мире электронные доказательства становятся наиболее часто используемыми доказательствами. Для того чтобы быть принятыми в качестве действительных и надежных средств доказывания, электронные доказательства и электронные документы должны удовлетворять нескольким критериям, включая обеспечение целостности цифровых данных, чтобы гарантировать их подлинность, целостность и неизменность.

Электронный документ считается аутентичным, когда установлены автор, место и время его создания, а его содержание действительно исходит от указанного автора и не изменялось с момента его создания (Surovtseva, 2020). В этом смысле подлинность и неизменность электронного документа могут быть обеспечены за счет использования сертификационных услуг в соответствии с Регламентом (ЕС) 910/2014 (eIDAS) – например, квалифицированной электронной подписи, квалифицированной электронной печати или квалифицированного электронного штампа времени, которые удостоверяют как личность автора, так и время создания и целостность электронного документа. Целостность электронного документа или цифровой информации также может быть гарантирована за счет использования технологии блокчейн- и смарт-контрактов, которые обеспечивают возможность хранения данных в децентрализованной, неизменяемой и прозрачной среде (Miao et al., 2021). Записи в реестре блокчейна гарантируют, что содержание электронного документа не подвергалось изменениям с момента его создания. Данная технология обеспечивает надежное хранение электронного документа, защиту от его последующего изменения или удаления, а также удостоверяет хронологию записей в децентрализованном реестре, что гарантирует подлинность и отслеживаемость электронных доказательств (Al-E'mari et al., 2024; Stoykova, 2023).

Системы искусственного интеллекта также могут использоваться в процессе доказывания, и в частности на этапе проверки подлинности электронных документов, посредством автоматизированного анализа содержимого, обнаружения аномалий, сравнения версий и оценки рисков, что повышает безопасность работы с электронными доказательствами. Интеграция систем искусственного интеллекта, блокчейн-технологий и служб квалифицированной сертификации создает многоуровневый механизм защиты целостности и подлинности электронных документов и электронных доказательств, особенно в контексте судебных разбирательств и электронного правосудия.

Заключение

В данном исследовании предлагается изменить традиционную парадигму понимания правовой природы электронных доказательств в контексте европейского законодательства. Проанализированы Регламент (ЕС) 2023/1543 и Регламент (ЕС) 910/2014 (eIDAS); метод сравнительно-правового анализа позволяет сделать вывод о том, что электронные доказательства нельзя приравнивать к традиционной категории вещественных доказательств, поскольку они имеют особую, цифровую природу и уникальные технические характеристики. Электронные доказательства – это новый правовой феномен, который должен получить самостоятельное правовое регулирование

в отношении процессуальных действий, связанных с их сбором, хранением, анализом и принятием в качестве адекватного средства доказывания в судебном процессе. Рассмотрение электронных доказательств в качестве одного из видов вещественных доказательств не только неверно, но и создает реальный риск правовой неопределенности и трудностей в эффективном правоприменении в отдельных государствах – членах ЕС. Настоящее исследование способствует развитию теоретического понимания электронных доказательств в соответствии с применимым европейским законодательством, а также намечает возможности для будущих исследований по интеграции новых технологий, таких как блокчейн и искусственный интеллект, в процесс доказывания и верификации подлинности электронных доказательств.

В работе предлагается преодолеть старую парадигму и выделить электронные доказательства как самостоятельную правовую категорию в системе видов доказательств, а также установить их отличия от вещественных доказательств. Автор приводит ряд аргументов в пользу уникальной цифровой природы электронных доказательств и необходимости создания независимой правовой базы в различных национальных законодательствах. Предлагается усовершенствовать научную терминологию, используя термин «электронные доказательства», который соответствует юридическим определениям, приведенным в рассматриваемых нормативных актах, и отказаться от использования устаревшего термина «цифровые доказательства».

Автор приводит конкретные рекомендации, имеющие практическое значение в процессе использования электронных доказательств, а именно идентификации, хранения, представления и анализа электронных доказательств в различных судебных разбирательствах в соответствии с применимым наднациональным законодательством. В то же время в данном исследовании предлагается преодолеть устаревшие представления о правовой природе электронных доказательств и их неверное отождествление с вещественными доказательствами.

Список литературы

Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital forensics meets blockchain: Enhancing evidence authenticity and traceability. *2024 2nd International conference on cyber resilience (ICCR)* (pp. 01–06). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532961

Begishev, I. R., Khisamova, Z. I., & Nikitin, S. G. (2020). The organization of hacking community: Criminological and criminal law aspects. *Russian Journal of Criminology*, *14*(1), 96–105. https://doi.org/10.17150/2500-4255.2020.14(1).96-105

Bérubé, M., Beaulieu, L., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306

Bufetova, M. Sh. (2023). The electronic document as a type of physical evidence in Russian criminal proceedings. *Siberian Legal Readings*, *3*, 47–55. https://doi.org/10.17150/2411-6122.2023.3.47-55

Daniel, Larry. E., & Daniel, Lars. E. (2012). *Discovery of digital evidence in civil cases. In Digital Forensics for Legal Professionals* (Ch. 16, pp. 113–121). Elsevier eBooks. https://doi.org/10.1016/b978-1-59749-643-8.00016-x

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Ferreira, D., & Gromova, E. (2024). Digital evidence in disputes involving states. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4

Guo, Z. (2022). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kirkov, A. (2022). Forensic activity experts in Bulgaria. Organization and problems. In *Collection of materials international scientific and practical seminar on the topic: "Digitalization of activities Courts: Current and Prospective Tasks"* (AI No. 276, 15.06.2015, pp. 5–9).

Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y. (2021). Blockchain-based Electronic Evidence Storage and Efficiency Optimization. In *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)* (pp. 109–113). IEEE. https://doi.org/10.1109/AIBT53261.2021.00025

Mubarik, N. (2019). Importance and role of physical evidence in forensic science. *Academic Journal of Forensic Sciences*, *2*(1), 18–22.

Nekrošius, V. (2021). Use of information technologies in Lithuanian civil procedure. *Procedia Computer Science*, *192*, 2662–2667. https://doi.org/10.1016/j.procs.2021.09.036

Pastukhov, P. S. (2015). Elektronnoe important evidence in a criminal case sudoproizvodstve. *Vestnik Tomsk state-owned University*, *396*, 149–153.

Shin, D., Ha, J., & Euom, I. (2025). Data-Driven Digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. *Computer Modeling in Engineering & Sciences*, *143*(3), 3795–3838. https://doi.org/10.32604/cmes.2025.066727

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Surovtseva, N. (2020). Authenticity and identity of electronic records. *Herald of an archivist*, *2*, 467–477. https://doi.org/10.28995/2073-0101-2020-2-467-477

Vuchkov, V. (2023). Electronic evidence in criminal cases and its sources – necessary considerations. Law *Journal of New Bulgarian University*, *19*(2), 12–19. https://doi.org/10.33919/ljnbu.23.2.1

Wu, D., Zuo, X., & Guo, Y. (2025). The application of electronic evidence in forensic imaging analysis. *Journal of Radiation Research and Applied Sciences*, *18*(3), 101708. https://doi.org/10.1016/j.jrras.2025.101708

Информация об авторе

Варбанова Гергана – PhD, ассистент кафедры права в области национальной безопасности и информационных технологий, Высшее военно-морское училище имени Николы Вапцарова
Адрес: Болгария, г. Варна, ул. Василя Друмева, д. 73
E-mail: g.varbanova@naval-acad.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=60021317100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HKP-1334-2023
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=02-0uFYAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 19 июня 2025 г.
Дата одобрения после рецензирования – 28 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:347:004.4
EDN: https://elibrary.ru/jqhnur
DOI: https://doi.org/10.21202/jdtl.2025.20

Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice

Gergana Varbanova
Nikola Vaptsarov Naval Academy, Varna, Bulgaria

Keywords

authenticity,
digital information,
digital technologies,
electronic evidence,
European legislation,
evidence,
judicial procedure,
law,
material evidence,
procedure

Abstract

Objective: to develop a new theoretical framework that challenges the traditional classification of electronic evidence as a subtype of material evidence and suggests considering it as a qualitatively new legal phenomenon with its own independent legal nature in the context of applicable European legislation.

Methods: the work uses the doctrinal method for the legal analysis of applicable European legislation, including Regulation (EU) 2023/1543 and Regulation (EU) 910/2014 (eIDAS), as well as their direct application in the national legal systems of the European Union member states. A comparative legal approach was used to identify differences between theoretical views and case law. A technological analysis of digital information was performed; specific examples were explained to illustrate the problems associated with the collection and use of electronic evidence within the European legislation framework.

Results: the author proposes a new doctrinal understanding of electronic evidence as an independent category that differs from traditional material evidence in its digital nature and specific characteristics. The introduction of European regulations requires rethinking the legal nature of electronic evidence as a qualitatively different legal phenomenon. It was established that treating electronic evidence as material one creates a risk of legal uncertainty, while the lack of appropriate legal regulation hinders effective law enforcement.

Scientific novelty: for the first time, the research proposes to overcome the established paradigm and identify electronic evidence as an independent

legal category in the system of evidence types. The article substantiates the unique digital nature of electronic evidence and the need to create an independent legal framework in various national legislations. It is proposed to improve scientific terminology using the term "electronic evidence", which corresponds to the legal definitions in the legislation under study, instead of the outdated term "digital evidence".

Practical significance: the work contains specific practical recommendations for the use of electronic evidence in the procedures for its identification, storage, presentation and analysis in various court proceedings in accordance with applicable supranational legislation. The research helps to overcome outdated ideas about the legal nature of electronic evidence and their incorrect identification with material evidence. This is important for effective law enforcement in the European Union member states.

For citation

Varbanova, G. (2025). Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice. *Journal of Digital Technologies and Law, 3*(3), 497–511. https://doi.org/10.21202/jdtl.2025.20

References

Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital forensics meets blockchain: Enhancing evidence authenticity and traceability. *2024 2nd International conference on cyber resilience (ICCR)* (pp. 01–06). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532961

Begishev, I. R., Khisamova, Z. I., & Nikitin, S. G. (2020). The organization of hacking community: Criminological and criminal law aspects. *Russian Journal of Criminology*, *14*(1), 96–105. (In Russ.). https://doi.org/10.17150/2500-4255.2020.14(1).96-105

Bérubé, M., Beaulieu, L., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306

Bufetova, M. Sh. (2023). The electronic document as a type of physical evidence in Russian criminal proceedings. *Siberian Legal Readings*, *3*, 47–55. https://doi.org/10.17150/2411-6122.2023.3.47-55

Daniel, Larry. E., & Daniel, Lars. E. (2012). *Discovery of digital evidence in civil cases. In Digital Forensics for Legal Professionals* (Ch. 16, pp. 113–121). Elsevier eBooks. https://doi.org/10.1016/b978-1-59749-643-8.00016-x

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Ferreira, D., & Gromova, E. (2024). Digital evidence in disputes involving states. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4

Guo, Z. (2022). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kirkov, A. (2022). Forensic activity experts in Bulgaria. Organization and problems. In *Collection of materials international scientific and practical seminar on the topic: "Digitalization of activities Courts: Current and Prospective Tasks"* (AI No. 276, 15.06.2015, pp. 5–9).

Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y. (2021). Blockchain-based Electronic Evidence Storage and Efficiency Optimization. In *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)* (pp. 109–113). IEEE. https://doi.org/10.1109/AIBT53261.2021.00025

Mubarik, N. (2019). Importance and role of physical evidence in forensic science. *Academic Journal of Forensic Sciences*, *2*(1), 18–22.

Nekrošius, V. (2021). Use of information technologies in Lithuanian civil procedure. *Procedia Computer Science*, *192*, 2662–2667. https://doi.org/10.1016/j.procs.2021.09.036

Pastukhov, P. S. (2015). Elektronnoe important evidence in a criminal case sudoproizvodstve. *Vestnik Tomsk state-owned University*, *396*, 149–153.

Shin, D., Ha, J., & Euom, I. (2025). Data-Driven Digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. *Computer Modeling in Engineering & Sciences*, *143*(3), 3795–3838. https://doi.org/10.32604/cmes.2025.066727

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Surovtseva, N. (2020). Authenticity and identity of electronic records. *Herald of an archivist*, *2*, 467–477. https://doi.org/10.28995/2073-0101-2020-2-467-477

Vuchkov, V. (2023). Electronic evidence in criminal cases and its sources – necessary considerations. Law *Journal of New Bulgarian University*, *19*(2), 12–19. https://doi.org/10.33919/ljnbu.23.2.1

Wu, D., Zuo, X., & Guo, Y. (2025). The application of electronic evidence in forensic imaging analysis. *Journal of Radiation Research and Applied Sciences*, *18*(3), 101708. https://doi.org/10.1016/j.jrras.2025.101708

Author information

Gergana Varbanova – PhD, Assistant Professor, Department of National Security and Information Technology Law, Nikola Vaptsarov Naval Academy
Address: 73 Vasil Drumev Street, Varna, Bulgaria
E-mail: g.varbanova@naval-acad.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=60021317100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HKP-1334-2023
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=02-0uFYAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 99, 2025
Date of approval – June 28, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025