УДК 343.1:341.96 **DOI: 10.34670/AR.2026.18.55.037**

Новое законодательство ЕС о цифровых доказательствах: преобразование процедур трансграничного доступа и вызовы судебных гарантий

Реховский Александр Федорович

Кандидат юридических наук,
доцент,
Владивостокский государственный университет,
690014, Российская Федерация, Владивосток, ул. Гоголя, 41;
e-mail: A.Rekhovskiy@vvsu.ru

Аннотация

В статье анализируются инновационные положения Регламента (ЕС) 2023/1543 и Директивы (ЕС) 2023/1544, введшие в правовую систему ЕС механизмы Европейского приказа о производстве (European Production Order, EPO) и Европейского приказа о сохранении (European Preservation Order, EPrO). Исследование сосредоточено на парадигматическом сдвиге от взаимной правовой помощи к модели прямого признания и приватизации доступа к электронным доказательствам через сервис-провайдеров. Выявляются системные проблемы единообразия стандартов допустимости, судебного контроля, защиты фундаментальных прав обвиняемого, а также влияние технологических инноваций (ИИ, deepfakes) на надежность цифровых улик. Рассматривается практика имплементации в государствах-членах ЕС. Формулируются рекомендации по введению европейских минимальных стандартов криптографической верификации и chain of custody для цифровых доказательств.

Для цитирования в научных исследованиях

Реховский А.Ф. Новое законодательство ЕС о цифровых доказательствах: преобразование процедур трансграничного доступа и вызовы судебных гарантий // Вопросы российского и международного права. 2025. Том 15. № 12А. С. 369-375. DOI: 10.34670/AR.2026.18.55.037

Ключевые слова

Цифровые доказательства, e-evidence, Европейский приказ о производстве, допустимость доказательств, цепь хранения, справедливый суд, Европейский союз, уголовный процесс, трансграничное сотрудничество.

Введение

Цифровизация преступной деятельности и расширение объема электронных данных в расследованиях уголовных дел выдвинули на авансцену проблему ускорения и унификации процедур получения цифровых доказательств в трансграничном контексте. В 2023 году Европейский союз принял революционный правовой пакет - Регламент (ЕС) 2023/1543 и Директиву (ЕС) 2023/1544, - кардинально преобразовав способ взаимодействия национальных судов и правоохранительных органов государств-членов с поставщиками электронных услуг при получении цифровых доказательств. До принятия данного пакета процедура основывалась на громоздких механизмах взаимной правовой помощи (Mutual Legal Assistance Treaties, MLAT) и Европейских приказов об истребовании (European Investigation Orders, EIO), что замедляло расследования и создавало лакуны для скрывания следов преступной деятельности [Tosza, Ligeti, 2024; Regulation (EU) 2023/1543, 2023; Council Directive 2014/41/EU, 2014].

Основная часть

Исторический контекст этих трансформаций глубоко связан с вызовами современного киберпространства и трансграничной преступности. К началу 2024 года примерно 85% расследований в странах ЕС включали компонент цифровых доказательств, однако согласованных европейских стандартов их верификации и допустимости отсутствовало. Несмотря на благие намерения, e-evidence пакет создает парадоксальную ситуацию: ускорение [Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial, 2025] доступа к доказательствам идет в ущерб судебному контролю и гарантиям справедливого разбирательства.

Данная статья посвящена критическому анализу этого законодательного сдвига и выявлению системных проблем, требующих решения при имплементации на национальном уровне.

1. Архитектура нового механизма: Европейский приказ о производстве и сохранении.

1.1. Сущность и процедура EPO/EPrO. Регламент 2023/1543 вводит два основных инструмента, функционально расширяющих компетенцию национальных судов и следователей в получении электронных данных: Европейский приказ о производстве (EPO) представляет собой судебный акт национального суда, направленный сервис-провайдеру на территории другого государства-члена ЕС, с требованием передать или обеспечить доступ к удаленно хранимым электронным данным. Выдача EPO требует наличия обоснованного подозрения в совершении преступления, а также мотивировки необходимости и пропорциональности такого вмешательства в фундаментальные права (право на приватность, защиту персональных данных согласно GDPR).

Европейский приказ о сохранении (EPrO) действует на ранней стадии расследования и направлен на предотвращение удаления или модификации данных до выдачи полного EPO. Срок действия EPrO ограничен, что позволяет правоохранительным органам «заморозить» цифровые доказательства до выдачи надлежащего судебного приказа. Это особенно важно в контексте преступлений, связанных с терроризмом, организованной преступностью или детской порнографией, где скорость критична [Regulation (EU) 2023/1543, 2023; Directive 95/46/EC, 1995].

1.2. Роль юридических представителей провайдеров [5]. Директива 2023/1544 вводит обязательство для всех поставщиков цифровых услуг, действующих на территории ЕС, назначить

юридического представителя (legal representative) для взаимодействия с национальными органами по поводу исполнения EPO/EPrO. Это создает новую инфраструктуру: коммерческие компании (Google, Meta, Microsoft и др.) становятся де-факто посредниками правосудия, что фундаментально меняет природу доказательственной деятельности в уголовном процессе [Directive (EU) 2023/1544, 2023; Regulation (EU) 2023/1543, 2023].

Таймлайн внедрения: регламент вступит в силу 18 августа 2026 года, предоставляя переходный период для адаптации национальных судебных систем и коммерческих провайдеров.

2. Парадигматический сдвиг: от взаимной помощи к приватизации доступа. Принципиально новой чертой e-evidence пакета является переход от модели взаимной правовой помощи к модели прямого признания (direct recognition). В старой системе каждый запрос тщательно проверялся с позиции согласованности с национальным процессуальным правом исполняющего государства, что обеспечивало юридические гарантии, но замедляло процесс. Новая система предполагает, что суд государства, выдавшего EPO, действовал надлежащим образом, и данные автоматически признаются в исполняющем государстве без полной переоценки законности [Mutual recognition principle in EU law and its application to e-evidence]. Однако это создает трещину в системе судебного контроля.

На примере дела EncroChat (CJEU C-670/22), рассмотренного Судом по правам человека ЕС 30 апреля 2024 года, видно, что суды все еще требуют проверки материальных условий получения доказательств согласно нормам исполняющего государства, если были использованы нетрадиционные методы (например, взлом зашифрованных систем или промежуточные оперативные расследования). Если ответчик не может эффективно оспорить подлинность, законность или надежность доказательства, оно должно быть исключено из судебного разбирательства в соответствии с правом на справедливый суд (ECHR Article 6) [Case C-670/22 (EncroChat), 2024; ECHR Article 6].

3. Критические проблемы допустимости и надежности цифровых улик.

3.1. Лакуна в европейских стандартах верификации. Хотя Регламент 2023/1543 определяет процедурные рамки взаимодействия с провайдерами, он остается молчалив в отношении минимальных европейских стандартов для оценки подлинности, целостности и достоверности электронных доказательств (chain of custody).

Это создает риск асимметрии в судебной практике разных государств-членов: если немецкий суд придерживается строгих криптографических стандартов верификации, то польский или испанский суд может руководствоваться менее строгими критериями [Wąsek-Wiaderek, Michałowicz, 2024].

На практике это означает, что одни и те же цифровые доказательства могут быть признаны допустимыми в одной стране и недопустимыми в другой, что подрывает единство европейского судебного пространства [Слоўик, 2023].

3.2. Риски ИИ и глубокой подделки (deepfakes) [A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response, 2023]. Согласно исследованиям 2024–2025 годов, поставщики услуг используют ИИ-системы для фильтрации, категоризации и анализа содержимого (например, для выявления CSAM, терроризма, преступного контента). Регламент не требует раскрытия этих алгоритмических методов, что создает риск скрытого вмешательства в уголовное расследование. Одновременно появились новые технологические угрозы: deepfakes (глубокие подделки видео и аудио), созданные с помощью нейронных сетей, способны имитировать голос и действия реальных лиц с высокой степенью достоверности.

Если такие «доказательства» попадут в судебный процесс без надлежащей верификации и криптографической аутентификации, это может привести к судебным ошибкам [Spajić, Jovašević, 2025].

3.3. Процедурные гарантии обвиняемого. Согласно GDPR Article 22 и ECHR Article 6, обвиняемый имеет право: знать методы анализа его данных; оспорить результаты автоматизированной обработки; требовать человеческого пересмотра автоматизированных решений [GDPR Article 22; ECHR Article 6]; иметь равные средства защиты (equality of arms) при опровержении цифровых доказательств.

Регламент 2023/1543 не полностью учитывает эти гарантии, предоставляя поставщикам услуг значительную свободу в описании методов сбора и передачи данных.

4. Национальная имплементация: вызовы и проблемы согласованности.

4.1. Пример Польши и проблема эквивалентности [Wąsek-Wiaderek, Michałowicz, 2024]. Анализ национального законодательства, в частности Польши, выявляет системные проблемы имплементации. Польское уголовное процессуальное право содержит специфические требования к наделению полномочиями национальных органов по запросам данных от провайдеров.

Однако Регламент 2023/1543 прямого применения требует, чтобы польский суд выдавал EPO иностранным провайдерам на тех же условиях, что и национальным. Это требует не просто рецепции, а радикального пересмотра польского процессуального кодекса [Kodeks postępowania karnego].

4.2. Молчание регламента о критериях допустимости. Несмотря на то, что Регламент имеет прямое применение во всех государствах-членах, он оставляет на их усмотрение финальную оценку допустимости полученных через EPO/EPrO доказательств согласно внутреннему уголовному процессу [Регламент (ЕС) 2023/1543, 2023]. Это создает парадокс: единая процедура получения, но разнородные стандарты оценки допустимости.

4.3. Феномен «отравленного плода» (fruits of the poisoned tree). Если в исполняющем государстве способ получения данных был незаконен согласно его национальному праву, полученные доказательства должны быть исключены не только в исполняющем, но и в запрашивающем государстве [Kiourkova, 2024].

Однако механизм информирования об этом и процедура проверки недостаточно регламентированы, что создает риск прохождения недопустимых доказательств через судебный процесс.

5. Стандарты для оценки цифровых доказательств в национальных судах. На основе анализа судебной практики, международных норм и директив DFRWS EU рекомендуются следующие минимальные европейские стандарты для оценки допустимости цифровых доказательств:

Таблица 1 – Стандарты для оценки цифровых доказательств в национальных судах

Критерий	Требование	Инструменты реализации
Подлинность	Документированное доказательство, что данные получены от истинного источника	Сертификат от провайдера, цифровые подписи, криптографические отпечатки
Интегритет	Целостность данных при передаче и хранении	Хеш-суммы файлов, криптографические печати, регистры доступа
Цепь хранения	Полная документированная история доступа, модификации, передачи	Журналы аудита, временные метки, подписание каждого этапа
Аутентификация источника	Убедительное доказательство принадлежности данных подозреваемому лицу	Биометрические данные, IP-адреса, метаданные файлов
Прозрачность методов	Раскрытие алгоритмических и аналитических методов	Технические описания, испытание на воспроизводимость
Оспоримость	Право ответчика вызывать экспертов для переанализа	Судебная экспертиза, возможность независимой проверки

6. Сравнение с российским уголовным процессом. Российский уголовный процесс, регламентируемый УПК РФ, предусматривает систему доказательств, включающую и электронные данные [Таблица 1 - Стандарты для оценки цифровых доказательств в национальных судах]. Однако у российского подхода есть существенные отличия от европейского:

1. Централизованный контроль: УПК РФ предоставляет следователю широкие полномочия в получении доказательств, при этом судебный контроль происходит на более поздних стадиях [Федеральный закон № 60-ФЗ, 2011; Уголовный кодекс РФ].

2. Механизм международного запроса: Россия использует инструменты взаимной правовой помощи (каналы МВД, МИД), а не прямого обращения судов к коммерческим провайдерам [Таблица 1 - Стандарты для оценки цифровых доказательств в национальных судах].

3. Защита информации: российское законодательство о защите персональных данных и государственной тайне более строго ограничивает доступ иностранных органов к цифровым данным [Федеральный закон № 152-ФЗ, 2006; Закон РФ № 5485-1, 1993].

Опыт ЕС демонстрирует, что переход на модель прямого доступа требует пересмотра баланса между эффективностью расследований и судебными гарантиями, что может быть полезно при развитии российского законодательства в области цифровой криминалистики.

7. Заключение и рекомендации. Регламент (ЕС) 2023/1543 и Директива (ЕС) 2023/1544 представляют собой смелый шаг к технологической модернизации уголовного процесса в ЕС, но сопровождаются системными вызовами для судебных гарантий и фундаментальных прав обвиняемых [Tosza, Ligeti, 2024; Wąsek-Wiaderek, Michałowicz, 2024].

Заключение

К числу критических проблем относятся: 1) Отсутствие европейских минимальных стандартов для верификации, аутентификации и chain of custody цифровых доказательств; 2) Недостаточное раскрытие алгоритмических методов анализа данных, используемых провайдерами; 3) Риски, связанные с ИИ и deepfakes, требующие внедрения криптографических механизмов проверки оригинальности; 4) Асимметрия национальных стандартов допустимости, подрывающая единство европейского судебного пространства; 5) Недостаточная процедурализация гарантий для обвиняемого при оспаривании цифровых доказательств.

Рекомендации: 1) Разработать на уровне ЕС единые европейские стандарты криптографической верификации и chain of custody для цифровых доказательств с учетом рекомендаций DFRWS EU. 2) Обязать провайдеров полностью раскрывать методы извлечения, анализа и сохранения данных, включая использование ИИ-компонентов. 3) Создать реестр сертифицированных судебных экспертов по цифровой криминалистике в ЕС для независимого пересмотра методологии. 4) Расширить гарантии обвиняемого право знать и оспаривать методы анализа его данных согласно ECHR Article 6 и GDPR Article 22. 5) Гармонизировать национальные процессуальные нормы относительно допустимости цифровых доказательств через принятие общеевропейской рамки. На фоне растущей цифровизации преступной деятельности дальнейшее развитие законодательства об электронных доказательствах как в ЕС, так и в России, должно идти по пути баланса: с одной стороны, обеспечивая оперативность и эффективность расследований, с другой - гарантируя фундаментальные права и справедливое судебное разбирательство.

Библиография

1. Case C-670/22 (EncroChat), ECLI:EU:C:2024:336 // Judgment of 30.04.2024.

2. Council Directive 2014/41/EU regarding the European Investigation Order in criminal matters // Official Journal of the European Union. L 130. 1.05.2014.
3. Directive 95/46/EC (General Data Protection Regulation) and its general principles of necessity and proportionality.
4. Directive (EU) 2023/1544 on ensuring a single point of contact for legal service providers in the EU.
5. ECHR Article 6 «Right to a fair trial».
6. Federal′nyi zakon ot 27.07.2006 № 152-FZ «O zashchite personal′nykh dannykh».
7. Federal′nyi zakon ot 4.04.2011 № 60-FZ «Ob alternativnoi procedure uregulirovaniia sporov s uchastiem posrednika».
8. GDPR Article 22 «Right not to be subject to a decision based solely on automated processing»; ECHR Article 6.
9. Kodeks postępowania karnego (КПК Польши), глава об доказательствах.
10. Mutual recognition principle in EU law and its application to e-evidence.
11. Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial // European Criminal Law Review. 2025. Vol. 15, Issue 2. P. 245–280.
12. Regulation (EU) 2023/1543 on European Production Orders and Preservation Orders for electronic evidence in criminal matters // Official Journal of the European Union. L 192. 30.07.2023.
13. Reglament (ES) 2023/1543, Stat′ia 1 (primenenie).
14. Sloŭik, A. Verifikatsiia v zaprashivaiushchem gosudarstve dokazatel′stv, poluchennykh na osnove Evropeiskogo prikaza ob istrebovanii // Roczniki Nauk Prawnych. 2023. Vol. 33, No. 3. P. 67–87.
15. Tosza, S., Ligeti, K. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of «judicial» cooperation // European Criminal Law Review. 2024. Vol. 14, Issue 2. P. 123–157.
16. Ugolovno-protsessual′nyi kodeks Rossiiskoi Federatsii ot 18.12.2001 № 174-FZ.
17. Ugolovnyi kodeks RF, st. 1 o primenenii mezhdunarodnogo prava.
18. ąsek-Wiaderek, M., Michałowicz, M. The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change // Studia Iuridica Lublinensia. 2024. Vol. 33, No. 5. P. 421–445.
19. Zakon RF ot 21.07.1993 № 5485-1 «O gosudarstvennoi taine».
20. A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response // arXiv. 2023. eprint 2312.10667.
21. Kiourkova, D. The Problem of Obtaining Evidence from EU Countries While Achieving the «Crime Does Not Pay» Goal // Bialystok Legal Studies. 2024. Vol. 29, No. 6. P. 119–136.
22. Spajić, J., Jovašević, D. Algorithmic Evidence in Criminal Trials: Admissibility, Explainability, and Fair-Trial Guarantees // International Journal of Criminal Justice. 2025. Vol. 12, Issue 1. P. 89–115.

New EU Legislation on Digital Evidence: Transforming Cross-Border Access Procedures and the Challenges to Judicial Guarantees

Aleksandr F. Rekhovskii

PhD in Law,
Associate Professor,
Vladivostok State University,
690014, 41, Gogolya str., Vladivostok, Russian Federation;
e-mail: A.Rekhovskiy@vvsu.ru

Abstract

The article analyzes the innovative provisions of Regulation (EU) 2023/1543 and Directive (EU) 2023/1544, which introduced into the EU legal system the mechanisms of the European Production Order (EPO) and the European Preservation Order (EPrO). The research focuses on the paradigmatic shift from mutual legal assistance to a model of direct recognition and privatization of access to electronic evidence through service providers. Systemic problems of uniformity in admissibility standards, judicial oversight, protection of the accused's fundamental rights, as well as the impact of technological innovations (AI, deepfakes) on the reliability of digital evidence are identified. The

practice of implementation in EU member states is considered. Recommendations are formulated for the introduction of European minimum standards for cryptographic verification and chain of custody for digital evidence.

For citation

Rekhovskii A.F. (2025) Novoye zakonodatel'stvo YeS o tsifrovykh dokazatel'stvakh: preobrazovaniye protsedur transgranichnogo dostupa i vyzovy sudebnykh garantiy [New EU Legislation on Digital Evidence: Transforming Cross-Border Access Procedures and the Challenges to Judicial Guarantees]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (12A), pp. 369-375. DOI: 10.34670/AR.2026.18.55.037

Keywords

Digital evidence, e-evidence, European Production Order, admissibility of evidence, chain of custody, fair trial, European Union, criminal procedure, cross-border cooperation.

References

1. Case C-670/22 (EncroChat), ECLI:EU:C:2024:336 // Judgment of 30.04.2024.
2. Council Directive 2014/41/EU regarding the European Investigation Order in criminal matters // Official Journal of the European Union. L 130. 1.05.2014.
3. Directive 95/46/EC (General Data Protection Regulation) and its general principles of necessity and proportionality.
4. Directive (EU) 2023/1544 on ensuring a single point of contact for legal service providers in the EU.
5. ECHR Article 6 «Right to a fair trial».
6. Federal′nyi zakon ot 27.07.2006 № 152-FZ «O zashchite personal′nykh dannykh».
7. Federal′nyi zakon ot 4.04.2011 № 60-FZ «Ob alternativnoi procedure uregulirovaniia sporov s uchastiem posrednika».
8. GDPR Article 22 «Right not to be subject to a decision based solely on automated processing»; ECHR Article 6.
9. Kodeks postępowania karnego (КПК Польши), глава об доказательствах.
10. Mutual recognition principle in EU law and its application to e-evidence.
11. Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial // European Criminal Law Review. 2025. Vol. 15, Issue 2. P. 245–280.
12. Regulation (EU) 2023/1543 on European Production Orders and Preservation Orders for electronic evidence in criminal matters // Official Journal of the European Union. L 192. 30.07.2023.
13. Reglament (ES) 2023/1543, Stat′ia 1 (primenenie).
14. Sloǔik, A. Verifikatsiia v zaprashivaiushchem gosudarstve dokazatel′stv, poluchennykh na osnove Evropeiskogo prikaza ob istrebovanii // Roczniki Nauk Prawnych. 2023. Vol. 33, No. 3. P. 67–87.
15. Tosza, S., Ligeti, K. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of «judicial» cooperation // European Criminal Law Review. 2024. Vol. 14, Issue 2. P. 123–157.
16. Ugolovno-protsessual′nyi kodeks Rossiiskoi Federatsii ot 18.12.2001 № 174-FZ.
17. Ugolovnyi kodeks RF, st. 1 o primenenii mezhdunarodnogo prava.
18. Wąsek-Wiaderek, M., Michałowicz, M. The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change // Studia Iuridica Lublinensia. 2024. Vol. 33, No. 5. P. 421–445.
19. Zakon RF ot 21.07.1993 № 5485-1 «O gosudarstvennoitaine».
20. A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response // arXiv. 2023. eprint 2312.10667.
21. Kiourkova, D. The Problem of Obtaining Evidence from EU Countries While Achieving the «Crime Does Not Pay» Goal // Bialystok Legal Studies. 2024. Vol. 29, No. 6. P. 119–136.
22. Spajić, J., Jovašević, D. Algorithmic Evidence in Criminal Trials: Admissibility, Explainability, and Fair-Trial Guarantees // International Journal of Criminal Justice. 2025. Vol. 12, Issue 1. P. 89–115.