

DOI: <https://doi.org/10.15688/lc.jvolsu.2025.2.16>

UDC 343.13

LBC 67.410.2-32



Submitted: 25.05.2025

Accepted: 04.07.2025

CURRENT TRENDS IN INTERNATIONAL COOPERATION IN CRIMINAL CASES AND THEIR LEGAL REGULATION

Oksana S. Kolosovich

Volgograd Academy of the Ministry of the Interior of Russia, Volgograd, Russian Federation

Introduction: digitalization, which is taking place in modern society, opens up new opportunities for law enforcement agencies to combat crime. It is now possible to instantly exchange information regardless of distances and state borders. At the same time, the possibilities of information and communication technologies are only growing, and along with that, the effectiveness of their application in the field under consideration is increasing. Wireless data exchange methods, as well as artificial intelligence technologies, are most actively used in the modern world. **Methods:** the research methodology is based on the application of the dialectical method of cognition, the formal legal method, comparative law, and logical methods of cognition. As a **result** of the study, it is found that information and communication technologies have long acquired a large-scale character in international cooperation in criminal cases and affect the emergence of new ways of interaction between competent authorities of foreign states. The effectiveness and efficiency of law enforcement and judicial authorities in international cooperation, including in matters of taking proof and document management, directly depend on the use of information and communication technologies. Meanwhile, crimes committed using information and communication technologies pose the greatest threat to national security. The state is taking certain steps to change the situation. However, although today artificial intelligence technologies are the main element of digital transformation in police activities, the domestic criminal procedure legislator does not pay sufficient attention to these issues. On the contrary, the Russian Federation is actively working on international platforms to develop universal provisions on international cooperation in countering crimes committed using information and communication technologies. **Conclusion:** the author's solution to the identified problems is proposed.

Key words: information and communication technologies, international cooperation in criminal cases, legal regulation, electronic information, data exchange.

Citation. Kolosovich O.S. Current Trends in International Cooperation in Criminal Cases and Their Legal Regulation. *Legal Concept = Pravovaya paradigma*, 2025, vol. 24, no. 2, pp. 124-130. (in Russian). DOI: <https://doi.org/10.15688/lc.jvolsu.2025.2.16>

УДК 343.13

ББК 67.410.2-32

Дата поступления статьи: 25.05.2025

Дата принятия статьи: 04.07.2025

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПО УГОЛОВНЫМ ДЕЛАМ И ИХ ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Оксана Сергеевна Колосович

Волгоградская академия МВД России, г. Волгоград, Российская Федерация

Введение: цифровизация, происходящая в современном обществе, открывает новые горизонты в деятельности правоохранительных органов по противодействию преступности. Появилась возможность мгновенного обмена информацией независимо от расстояний и государственных границ. При этом потенциал информационно-коммуникационных технологий только растет, а вместе с этим – и эффективность их применения в рассматриваемой сфере. Наиболее активно в современном мире используются беспроводные способы обмена данными, а также технологии искусственного интеллекта. **Методология** исследования базируется на применении диалектического метода познания, формально-юридического метода, сравнительно-правового, логических методов познания. **В результате** исследования установлено, что в международном сотрудничестве по уголовным делам информационно-коммуникационные технологии давно приобрели мас-

штабный характер и влияют на появление новых способов взаимодействия компетентных органов иностранных государств. Эффективность и оперативность правоохранительных и судебных органов в международном сотрудничестве, в том числе в вопросах получения доказательств и осуществления документооборота, напрямую зависят от использования информационно-коммуникационных технологий. Между тем наибольшую угрозу для национальной безопасности представляют преступления, совершенные с использованием информационно-коммуникационных технологий. В целях изменения ситуации государством предпринимаются определенные шаги. Однако несмотря на то что сегодня технологии искусственного интеллекта выступают основным элементом цифровой трансформации в деятельности полиции, отечественный уголовно-процессуальный законодатель этим вопросам не уделяет достаточно внимания. Напротив, на международных площадках Российской Федерацией ведется активная работа по формированию универсальных положений о международном сотрудничестве по противодействию преступлениям, совершенным с использованием информационно-коммуникационных технологий. **Заключение:** предлагается авторское решение обозначенных проблем.

Ключевые слова: информационно-коммуникационные технологии, международное сотрудничество по уголовным делам, правовое регулирование, электронная информация, обмен данными.

Цитирование. Колосович О. С. Современные тенденции международного сотрудничества по уголовным делам и их правовое регулирование // Legal Concept = Правовая парадигма. – 2025. – Т. 24, № 2. – С. 124–130. – DOI: <https://doi.org/10.15688/lc.jvolsu.2025.2.16>

Введение

Информационно-коммуникационные технологии (далее – ИКТ) стали неотъемлемой частью деятельности как правоохранительных и судебных органов, так и криминалитета.

В последние годы наблюдается «практически двукратный ежегодный прирост числа таких преступлений» [1, с. 4], и эта тенденция продолжает набирать обороты. Так, за 2024 г. в Российской Федерации, по сравнению с 2023 г., зафиксирован рост преступлений с использованием ИКТ на 13,1 %, составив 40 % от общего количества зарегистрированных преступлений [5].

При помощи ИКТ оптимизируется деятельность правоохранительных и судебных органов. Не стало исключением расследование трансграничных преступлений, где передача доказательств и обмен данными между правоохранительными органами разных государств являются залогом его эффективности и скорости. К сожалению, отечественные ученые отмечают «забюрократизованность и заформализованность уголовного процесса» в рассматриваемой области [3, с. 492].

Новые формы использования ИКТ в международном сотрудничестве по уголовным делам

Для государств-участников Европейского союза (далее – государств-участников)

правовое регулирование использования ИКТ в рамках международного сотрудничества по уголовным делам занимает центральное место, обуславливая наш интерес к изучению опыта европейского законодателя. Здесь отметим, что им разработан новый механизм направления международных запросов о передаче и хранении электронных доказательств по уголовным делам.

Так, с 18 августа 2026 г. в ЕС начнет действовать «децентрализованная ИТ-система», которая обеспечит «быстрый, безопасный и надежный обмен информацией, позволяющий получателю установить подлинность данных», запрошенных на основании Европейского ордера на предоставление доказательств (ЕРОС) или Европейского ордера на сохранение доказательств (ЕРОС-PR) (в том числе данных, находящихся в облачной инфраструктуре) [9].

В соответствии с законодательством для выдачи Европейского ордера не имеет значения фактическое место нахождения поставщика услуг или объекта, не требуется наличие серверов в юрисдикции ЕС. Устанавливается направление ЕРОС непосредственно поставщику услуг другого государства-участника. В качестве гарантий соблюдения основных прав доказательственная ценность таких материалов будет оцениваться национальным судом. Третьими государствами получение подобных доказательств возможно посредством направления международного

запроса в национальные правоохранительные органы, обслуживающие территорию, на которой зарегистрирован или представлен поставщик услуг.

Новым направлением международного сотрудничества ЕС можно назвать предоставление Евроюсту полномочий по созданию централизованного хранилища для хранения, анализа и обмена электронными доказательствами, собранными европейскими наднациональными органами, другими международными организациями, третьими государствами в отношении определенных категорий преступлений (Регламент 2022/838 [12]). Цель создания депозита доказательств – обеспечение сохранности и юридической силы доказательств, их доступности, допустимости и достоверности в будущем для национальных и международных судов.

Закономерным представляется принятие в ЕС Закона об искусственном интеллекте [13], установившего сферу применения технологий искусственного интеллекта (далее – ИИ), в том числе в правоохранительной деятельности государств-участников. Согласно положениям закона, государствам-участникам надлежит провести ревизию существующего механизма национального правового регулирования международного сотрудничества по уголовным делам для определения его соответствия вводимым правилам. При необходимости механизм должен быть реорганизован посредством изменения международных договоров.

Эффективности международного сотрудничества ЕС способствует четкое законодательное закрепление международными нормами доказательственного значения электронных данных, возможности электронного способа общения и критериев приемлемости электронных документов, условий автоматизированного обмена данными, процессов внедрения и применения данной технологии по уголовным делам, включая ИИ.

ИКТ в международном сотрудничестве по уголовным делам РФ

В Уголовно-процессуальном кодексе Российской Федерации (далее – УПК РФ) предусмотрены возможности использования электронных документов в судебном и досу-

дебном производстве (ст. 474.1, 474.2 УПК РФ), однако международное сотрудничество ими не охвачено.

Вместе с тем уголовно-процессуальным законодателем не решен вопрос о возможных пределах использования ИКТ, доказательственном значении полученной с их помощью информации. Остается открытым вопрос об уголовно-процессуальных гарантиях прав и законных интересов лиц, вовлеченных в эту деятельность.

В свете вышесказанного следует согласиться с высказываниями ученых о необходимости дополнения отечественного уголовно-процессуального законодательства положениями, касающимися сбора «доказательств на электронных носителях информации, включая цифровые следы преступлений, электронные документы, возможность дистанционного участия в уголовном судопроизводстве» [1, с. 5]. Однако этого недостаточно.

Необходима законодательная регламентация более широкого спектра отношений, связанных с использованием в уголовном судопроизводстве ИКТ. В связи с этим своевременны предложения А.Ю. Чуриковой о необходимости установления правил применения ИИ в уголовном судопроизводстве для обработки больших баз данных, включая распознавание лиц; закрепления требований к электронным документам и предоставления возможности их создания и отправки всеми участниками уголовного процесса, а также «практику нормативного регулирования процессов внедрения и применения информационных технологий в уголовном судопроизводстве» [11, с. 16, 18, 28].

Нельзя утверждать, что российский законодатель откровенно игнорирует вопросы использования ИКТ в рамках международного сотрудничества по уголовным делам. Невозможно согласиться и с утверждениями об отсутствии в российском законодательстве положений, которые обязывали бы поставщиков интернет-услуг и услуг связи оперативно обеспечивать сохранность компьютерных данных на определенное время [4, с. 87]. Действительно, в УПК РФ отсутствует специальный раздел или глава, посвященные этому вопросу, положения об электронных доказательствах и иной электронной информации.

Нет и специальных законов, регулирующих использование ИКТ для оказания право-

вой помощи по уголовным делам. На сегодняшний день нормы, регулирующие данную деятельность, содержатся фрагментарно в различных законодательных и подзаконных актах.

К примеру, на основе принципа применения научных и технических достижений, современных технологий и информационных систем осуществляется деятельность полиции (ст. 11 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» [7]).

Передача персональных данных, в том числе иностранным государствам, производится, в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [6], для осуществления правосудия, оперативно-разыскной деятельности, прокурорского надзора, обеспечения безопасности, а также в контексте противодействия терроризму и коррупции; на основании международных договоров РФ персональные данные передаются иностранным государствам (п. 6–7.1 ч. 2 ст. 10, ч. 2 ст. 11 ст. 12 Закона о персональных данных), а в ст. 3 закреплено понятие «трансграничная передача персональных данных».

Кроме того, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [8] в ч. 3.1 ст. 10.1 предусмотрена обязанность «организаторов распространения информации в сети “Интернет”» предоставлять информацию «органам, осуществляющим оперативно-разыскную деятельность и обеспечение безопасности».

Отсутствие на законодательном уровне процедуры использования ИКТ в международном сотрудничестве по уголовным делам частично восполняется ведомственными актами в сфере оперативно-разыскной деятельности, в частности по линии Интерпола, нередко находящимися в ограниченном доступе.

В ходе проведенного интервьюирования 78 % респондентов высказали неудовлетворенность существующей правовой регламентацией международного сотрудничества в УПК РФ, что послужило причиной сотрудничества вне правового поля. В частности, с целью эффективного и быстрого исполнения запроса о правовой помощи сформировалась практика непосредственного взаимодействия с иностранными правоохранительными орга-

нами. По мнению респондентов, вопросы применения ИКТ и их результатов в уголовном судопроизводстве требуют определенности со стороны законодателя (автором было проинтервьюировано 711 сотрудников следственных подразделений и органов дознания МВД России из 42 субъектов РФ).

В то же время на международных площадках Российская Федерация принимает активное участие в создании положений о международном сотрудничестве по предупреждению, выявлению и расследованию преступлений с использованием ИКТ. Так, она выступила инициатором и одним из разработчиков Конвенции Организации Объединенных Наций против киберпреступности; за укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям [10] (далее – Конвенция). Ее уже назвали важнейшим эпохальным документом и «первым международным договором по борьбе с преступностью за последние 20 лет...» [2].

Основными достижениями Конвенции следует назвать: оперативный сбор электронных доказательств и совместное их использование в расследовании широкого круга преступлений, совершенных с использованием ИКТ; установление универсальных правил, предусматривающих упрощенный механизм международного сотрудничества, включая непосредственное взаимодействие компетентных органов сотрудничающих государств; криминализация деяний в исследуемой области национальным законодательством государств-участников; комплексный подход к регулированию различных направлений международного сотрудничества, включая обеспечение безопасности; установление прямого запрета нарушения суверенитета государств в ходе поиска и изъятия информации в информационно-коммуникативных системах; установление процедуры сбора, получения, хранения и передачи электронной информации, включая доказательства и документы, для предварительного расследования или судебного разбирательства; фиксацию права создания органов по проведению совместных рас-

следований; использование терминологии, свойственной отечественному праву; признание неправомерным отказа в помощи в связи с сохранением банковской тайны.

Таким образом, инициатива со стороны Российского государства свидетельствует о признании необходимости совершенствования внутригосударственного механизма международного сотрудничества с применением ИКТ. Подтверждение данного вывода мы находим в положении ст. 59 Конвенции о необходимости приведения национального законодательства в соответствие с указанным международным актом.

На основании изложенного можно прийти к следующим **выводам**:

1. В мире ИКТ занимают центральное место в международном сотрудничестве по уголовным делам. В последние годы в этой области развитие получило правовое регулирование передачи и хранения электронных доказательств.

2. Отечественное законодательство уделяет внимание правовому регулированию использования ИКТ в международном сотрудничестве по уголовным делам. Однако существующие положения не соответствуют современным требованиям: не успевают за быстрым развитием технологий и актуальными потребностями взаимодействия компетентных органов. Положения, касающиеся этой сферы, разрознены и фрагментарны и в основном относятся к оперативно-разыскному праву.

3. На международных площадках Российская Федерация продвигает прогрессивные положения в области использования ИКТ, предлагая упрощенный механизм международного сотрудничества, однако внутреннее уголовно-процессуальное законодательство требует аналогичного внимания.

4. Представляется обоснованным включение в УПК РФ порядка использования в международном сотрудничестве ИКТ (наряду с непосредственным взаимодействием компетентных органов), правового статуса электронной информации, обрабатываемой для использования в уголовном судопроизводстве.

СПИСОК ЛИТЕРАТУРЫ

1. Балашова, А. А. Электронные носители информации и их использование в уголовно-про-

цессуальном доказывании : автореф. дис. ... канд. юрид. наук / Балашова Анна Александровна. – М., 2020. – 31 с.

2. В ООН принята Конвенция по борьбе с киберпреступностью. – URL: <https://cgirc.ru/media/v-onn-prinyata-konventsia-po-borbe-s-kiberprestupnostyu/>

3. Гаврилов, Б. Я. Потребность в новом УПК РФ: современные реалии или фантом / Б. Я. Гаврилов // Юридическая техника. – 2021. – № 15. – С. 491–497.

4. Жданов, Ю. Н. Кибермафия. Мировые тенденции и международное противодействие : монография / Ю. Н. Жданов, С. К. Кузнецов, В. С. Овчинский. – М. : Норма, 2022. – 184 с.

5. Краткая характеристика состояния преступности в Российской Федерации за 2024 год. – URL: <https://мвд.рф/reports/item/60248328/>

6. О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ. – URL: <https://web.archive.org/web/20230324174625>

7. О полиции : федер. закон от 7 февраля 2011 г. № 3-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_110165/

8. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/

9. Регламент Европейского парламента и Совета Европейского союза 2023/1543 от 12 июля 2023 г. о Европейских ордерах на предоставление электронных доказательств и о Европейских ордерах на сохранение электронных доказательств для целей уголовного процесса для исполнения приговоров к лишению свободы, вынесенных в рамках уголовного процесса. – URL: <https://base.garant.ru/408631405/>

10. Решение Генеральной Ассамблеи ООН 78/243. – URL: <https://www.un.org/ru/documents/assembly/A-RES-79-243>

11. Чурикова, А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : автореф. дис. ... д-ра юрид. наук / Чурикова Анна Юрьевна. – Саратов, 2024. – 48 с.

12. Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 Amending Regulation (EU) 2018/1727 as Regards the Preservation, Analysis and Storage at Euro just of Evidence Relating to Genocide, Crimes Against Humanity, War Crimes and Related Criminal Offences. – URL: <https://eur-lex.europa.eu/eli/reg/2022/838/oj>

13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonized Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/

2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance). – URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1729511739137>

REFERENCES

1. Balashova A.A. *Elektronnye nositeli informacii i ih ispolzovanie v ugolovno-processualnom dokazyvanii: avtoref. dis. ... kand. jurid. nauk* [Electronic Media and Their Use in Criminal Procedural Evidence. Cand. jurid. sci. abs. diss.]. Moscow, 2020. 31 p.
2. V OON prinyata Konventsia po borbe s kiberprestupnostyu [The UN Has Adopted the Convention on Combating Cybercrime]. URL: <https://cgitec.ru/media/v-on-prinyata-konventsia-po-borbe-s-kiberprestupnostyu/>
3. Gavrillov B.Ya. Potrebnost v novom UPK RF: sovremennyye realii ili fantom [The Need for a New Criminal Procedure Code of the Russian Federation: Modern Realities or a Phantom]. *Yuridicheskaya tekhnika* [Legal Technology], 2021, no. 15, pp. 491-497.
4. Zhdanov Yu.N., Kuznetsov S.K., Ovchinsky V.S. *Kibermafia. Mirovyye tendentsii i mezhdunarodnoye protivodeystviye: monografiya* [Cyber Mafia. World Trends and International Counteraction. Monograph]. Moscow, Norma Publ., 2022. 184 p.
5. *Kratkaya kharakteristika sostoyaniya prestupnosti v Rossiyskoy Federatsii za 2024 god* [Brief Description of the State of Crime in the Russian Federation in 2024]. URL: <https://мвд.рф/reports/item/60248328/>
6. *O personalnykh dannykh: feder. zakon ot 27 iyulya 2006 g. № 152-FZ* [On Personal Data: Federal Law No. 152-FZ of 27.07.2006]. URL: <https://web.archive.org/web/20230324174625>
7. *O politsii: feder. zakon ot 7 fevralya 2011 g. № 3-FZ* [About the Police: Federal Law No. 3-FZ Dated 07.02.2011]. URL: https://www.consultant.ru/document/cons_doc_LAW_110165
8. *Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: feder. zakon ot 27 iyulya 2006 g. № 149-FZ* [About Information, Information Technologies and Protection Information. Federal Law No. 149-FZ Dated 27.07.2006]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/
9. *Reglament Yevropeyskogo parlamenta i Soveta Yevropeyskogo soyuza 2023/1543 ot 12 iyulya 2023 g. o Yevropeyskikh orderakh na predostavleniye elektronnykh dokazatelstv i o Yevropeyskikh orderakh na sokhraneniye elektronnykh dokazatelstv dlya tseley ugolovnogo protsesssa dlya ispolneniya prigovorov k lisheniyu svobody, vynesennykh v ramkakh ugolovnogo protsesssa* [Regulation of the European Parliament and of the Council of the European Union 2023/1543 of July 12, 2023 on European Warrants for the Provision of Electronic Evidence and on European Warrants for the Preservation of Electronic Evidence for the Purposes of Criminal Proceedings for the Enforcement of Custodial Sentences Imposed in Criminal Proceedings]. URL: <https://base.garant.ru/408631405/>
10. *Resheniye Generalnoy Assamblei OON 78/243* [UN General Assembly Decision 78/243]. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243>
11. Churikova A.Yu. *Ispolzovanie informatsionnykh tekhnologiy i sistem v ugolovnom sudoproizvodstve: vozmozhnosti, riski, pravovoe regulirovanie: avtoref. dis. ... d-ra jurid. nauk* [The Use of Information Technologies and Systems in Criminal Proceedings: Opportunities, Risks, Legal Regulation. Dr. jurid. sci. abs. diss.]. Saratov, 2024. 48 p.
12. *Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 Amending Regulation (EU) 2018/1727 as Regards the Preservation, Analysis and Storage at Eurojust of Evidence Relating to Genocide, Crimes Against Humanity, War Crimes and Related Criminal Offences*. URL: <https://eur-lex.europa.eu/eli/reg/2022/838/oj>
13. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonized Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance)*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689&qid=1729511739137>

Information About the Author

Oksana S. Kolosovich, Candidate of Sciences (Jurisprudence), Associate Professor, Doctoral Student, Scientific Research Department, Volgograd Academy of the Ministry of the Interior of Russia, Istoricheskaya St, 130, 400075 Volgograd, Russian Federation, 1019810198@mail.ru, <https://orcid.org/0009-0004-1016-5391>

Информация об авторе

Оксана Сергеевна Колосович, кандидат юридических наук, доцент, докторант научно-исследовательского отдела, Волгоградская академия МВД России, ул. Историческая, 130, 400075 г. Волгоград, Российская Федерация, 1019810198@mail.ru, <https://orcid.org/0009-0004-1016-5391>