

Дата поступления рукописи в редакцию: 22.06.2026 г.
Дата принятия рукописи в печать: 11.07.2026 г.

DOI: 10.24412/2782-3849-2026-7-521-524

КВАЧ Сергей Сергеевич,

кандидат юридических наук, доцент, доцент кафедры Е5 «Техносферная безопасность и вычислительная механика» БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова,

e-mail: kvachss@yandex.ru

БЕРНДТ Анастасия Анатольевна,

кандидат юридических наук, доцент высшей школы права Югорского государственного университета,

e-mail: aa_berndt@ugrasu.ru

КИБЕРСУВЕРЕНИТЕТ И ТРАНСГРАНИЧНАЯ ПРАВОВАЯ ПОМОЩЬ: ПОИСК БАЛАНСА МЕЖДУ ЗАЩИТОЙ ДАННЫХ И ЭФФЕКТИВНОСТЬЮ ПРАВОСУДИЯ

Аннотация. Статья исследует конфликт между принципом киберсуверенитета (реализуемого через Федеральный закон № 149-ФЗ «Об информации», Федеральный закон № 152-ФЗ «О персональных данных» и Доктрину информационной безопасности РФ) и потребностью правосудия в оперативном доступе к электронным доказательствам. Авторы выявляют критические барьеры: законодательство о локализации данных (ст. 18 Федерального закона № 152-ФЗ), создающее коллизии с иностранными запросами; юрисдикционную неопределенность облачных сервисов; технологические ограничения, связанные с шифрованием и анонимизацией; неэффективность Гаагских конвенций (1965, 1970 гг.) для динамичных цифровых доказательств. Для преодоления дисбаланса предложены конкретные механизмы: ратификация Второго Дополнительного протокола к Будапештской конвенции (2022 г.) или разработка его аналога для ускоренного взаимодействия с провайдерами; внедрение в ГПК РФ и АПК РФ модели «уведомление и проверка» через институт «Трансграничного электронного запроса суда» с правом вето Минюста РФ; создание Единой цифровой платформы трансграничной правовой помощи для электронного документооборота, базы провайдеров и отслеживания запросов. Особо выделен дифференцированный подход: с «дружественными» юрисдикциями (ЕАЭС, СНГ, БРИКС) рекомендованы многосторонние соглашения о прямых запросах, а с «проблемными» странами — традиционные процедуры с усилением принципа взаимности и контролем защиты данных российских граждан. Авторы делают вывод, что баланс достижим через синтез гибких процедур, технологической инфраструктуры и международной гармонизации, где киберсуверенитет служит основой доверительного сотрудничества, а не барьером для эффективного правосудия.

Ключевые слова: киберсуверенитет; трансграничная правовая помощь; электронные доказательства; локализация данных; Гаагские конвенции; Будапештская конвенция; цифровая платформа.

KVACH Sergey Sergeevich,

Candidate of Law, Associate Professor

BERNDT Anastasia Anatolyevna,

Candidate of Law, Associate Professor

CYBER SOVEREIGNTY AND CROSS-BORDER LEGAL ASSISTANCE: FINDING A BALANCE BETWEEN DATA PROTECTION AND THE EFFECTIVENESS OF JUSTICE

Annotation. The article explores the conflict between the principle of cyber sovereignty (implemented through Federal Law No. 149-FZ “On Information”, Federal Law No. 152-FZ “On Personal Data” and the Doctrine of Information Security of the Russian Federation) and the need for justice in prompt access to electronic evidence. The authors identify critical barriers: legislation on

data localization (Art. 18 of Federal Law No. 152-FZ), which creates conflicts with foreign requests; the jurisdictional uncertainty of cloud services; technological limitations related to encryption and anonymization; and the inefficiency of the Hague Conventions (1965, 1970) for dynamic digital evidence. Specific mechanisms have been proposed to overcome the imbalance: the ratification of the Second Additional Protocol to the Budapest Convention (2022) or the development of its equivalent for accelerated interaction with providers; the introduction of the "notification and verification" model in the Civil Procedure Code of the Russian Federation and the Arbitration Procedure Code of the Russian Federation through the institute of "Cross-border Electronic Court Request" with the right of veto of the Ministry of Justice of the Russian Federation; and the creation of a unified digital platform for cross-border legal assistance for e-document management, a provider database, and query tracking. A differentiated approach is highlighted: with "friendly" jurisdictions (EAEU, CIS, BRICS), multilateral agreements on direct requests are recommended, while with "problematic" countries, traditional procedures are recommended, with a strengthened principle of reciprocity and control over the protection of Russian citizens' data. The authors conclude that a balance can be achieved through a synthesis of flexible procedures, technological infrastructure, and international harmonization, where cyber sovereignty serves as the basis for trusting cooperation rather than a barrier to effective justice.

Key words: cyber sovereignty; cross-border legal assistance; electronic evidence; data localization; Hague Conventions; Budapest Convention; digital platform.

Цифровая трансформация глобального правового пространства обостряет фундаментальное противоречие между принципом киберсуверенитета – правом государства регулировать информационные потоки и обеспечивать безопасность данных на своей территории (ФЗ-149 «Об информации», ФЗ-152 «О персональных данных», Доктрина информационной безопасности РФ) – и требованием эффективности правосудия в трансграничных спорах и уголовных делах. Традиционные механизмы правовой помощи (Гаагские конвенции 1965 и 1970 гг.), основанные на сложных дипломатических или центрально-органовских процедурах, зачастую неприменимы к динамичным электронным доказательствам (логи серверов, переписка в мессенджерах, облачные данные), которые могут быть изменены или удалены до исполнения запроса.

В условиях санкций, затруднённого авиасообщения, визовых проблем «непредоставление в срок документа, необходимого для совершения нотариального действия, или его полное отсутствие является достаточно значительной проблемой» [1, с.95].

Национальное законодательство о локализации и трансграничной передаче данных (ст. 18 ФЗ-152), создают прямой конфликт с запросами иностранных судов на предоставление таких данных, хранящихся в российских дата-центрах. Аналогичные нормы существуют в странах ЕС, Китае, и некоторых других странах, что приводит к риску взаимного блокирования запросов. Применение оговорки о публичном порядке (ст. 1193 ГК РФ, ст. 412 ГПК РФ) для отказа в исполнении запроса на доступ к данным, «противоречащего основам правопорядка

РФ», становится частым явлением, особенно в условиях геополитической напряженности [1, с.96].

Юрисдикционная неопределенность «облачных» данных также накладывает определённые противоречия. Физическое расположение серверов крупных провайдеров (Microsoft Azure, Yandex Cloud и др.) часто неизвестно или распределено по разным странам. Запрос к провайдеру, зарегистрированному в США, о данных, физически находящихся в РФ, ставит вопрос о применимом праве и возможности прямого доступа в обход государственных органов [2, с. 190].

Существуют также и технологические ограничения. Так, шифрование данных и анонимизирующие технологии (например VPN) делают традиционные методы сбора доказательств неэффективными. Запросы к государствам о правовой помощи для дешифрования часто технически невыполнимы или требуют раскрытия уязвимостей, что противоречит интересам национальной безопасности.

Таким образом, можем констатировать серьёзные проблемы, ограниченность и недостаточность традиционных механизмов правовой помощи.

Процедуры вручения документов и получения доказательств через Центральные административные органы (ЦАП) слишком медленные для электронных доказательств. Конвенции [3] не учитывают специфику прямого взаимодействия с IT-провайдерами и не решают вопросов юрисдикции над облачными данными.

Большинство двусторонних договоров РФ о правовой помощи не содержат специальных

норм об электронных доказательствах. Процедуры остаются громоздкими, а понятие «публичный порядок» трактуется расширительно в цифровом контексте.

В РФ (в отличие от США или ЕС), законодательство не предусматривает возможности для иностранных правоохранительных органов напрямую запрашивать данные у российских IT-компаний, даже если они касаются расследования преступлений против граждан РФ.

Внеждународном праве разрабатываются документы, регламентирующие затронутые вопросы, например, Будапештская конвенция о киберпреступности (СЕД №185) [4] и Второй Дополнительный протокол (2022) [5].

Каковы же возможные пути достижения баланса в указанной сфере для Российской Федерации?

Во-первых, представляется возможным ратификация и имплементация Второго Дополнительного протокола к Будапештской конвенции (если политически возможно) или разработка аналога. По результатам ратификации внесение изменений в процессуальное законодательство, а также в Федеральные законы «О связи», «Об информации».

Во-вторых, создание национального механизма по модели «уведомление и проверка» для гражданского и арбитражного процесса, для чего внести изменения в ГПК РФ (гл. 45.1) и АПК РФ (гл. 31.1) связанные с созданием института «Трансграничного электронного запроса суда».

В-третьих, развитие цифровой инфраструктуры, в первую очередь создание Единой цифровой платформы трансграничной правовой помощи на базе Минюста РФ. Функциями указанного Центра будут являться: администрирование безопасного канала для направления/приема запросов по Гаагским конвенциям и новым процедурам; электронный документооборот (е-запросы, е-апостиль); база данных иностранных провайдеров с контактами для прямых запросов; система отслеживания статуса запросов.

В-четвёртых, интеграция с международными системами. Изучение возможности подключения к e-CODEX (ЕС), а также создание и развитие аналогичных платформ в рамках BRICS+.

Важнейшим вопросом станет международно-правовое регулирование дешифрования. В первую очередь, необходимо продвижение в рамках ООН, БРИКС, ШОС инициативы по разработке Конвенции о трансграничном доступе к электронным доказательствам, включающей:

Принцип «Легального доступа по

решению суда» как основание для требования к провайдерам дешифровать и передать данные.

Механизм независимой экспертной оценки запросов на дешифрование и передачу данных для проверки обоснованности и соразмерности.

Гарантии защиты коммерческой тайны и «системной безопасности» провайдеров.

Представляется необходимым в первую очередь заключение многосторонних соглашений с «дружественными» юрисдикциями (ЕАЭС, СНГ, БРИКС) об ускоренной правовой помощи по электронным доказательствам, максимально приближенных к модели прямых запросов с контролем министерства юстиции. Не стоит забывать о принципе взаимности, который подразумевает возможность предоставления электронных доказательств и без договора, так «в большинстве стран взаимная правовая помощь осуществляется только на основе договора, хотя в ряде стран помощь может оказываться на основе принципов взаимности или международной вежливости, или в соответствии с требованиями внутреннего законодательства» [6, с.79].

С «проблемными» юрисдикциями – недружественными странами, предлагается использование традиционных Гаагских процедур с усилением принципа взаимности и контролем адекватной защиты данных российских граждан при исполнении их запросов в РФ.

Киберсуверенитет и эффективное правосудие в трансграничном цифровом пространстве не являются антагонистами по своей сути. Их конфликт – следствие устаревших правовых форм и отсутствия адекватных технологических решений. Достижение баланса между киберсуверенитетом и эффективностью правосудия в эпоху цифровой трансформации требует отказа от ригидных подходов в пользу гибкой, многоуровневой системы трансграничной правовой помощи, основанной на процедурных гарантиях и технологической совместимости.

Предложенные пути – имплементация передовых международных механизмов, создание национальной цифровой платформы, развитие специализированных норм в процессуальных кодексах РФ и активная работа над новыми международными стандартами – направлены на решение конкретных проблем:

Преодоление медлительности традиционных процедур через ускоренные каналы взаимодействия с провайдерами при сохранении государственного контроля.

Снятие юрисдикционных конфликтов через четкие правила определения применимого права и механизмы уведомления и блокирования.

Обеспечение исполнения запросов к

данным в условиях шифрования через судебные контролируемые процедуры дешифрования.

Соблюдение требований локализации данных за счет контроля за иностранными запросами к данным на территории России.

Дифференциация сотрудничества с учетом политико-правового контекста.

Список литературы:

[1] Парамузова О.Г., Гамова И.В. Правовые проблемы нотариального производства в современном мире // Евразийская интеграция: экономика, право, политика. 2023. №4 (46). С. 92-101.

[2] Андриянов, Д. В. Lex petrolea, глобализация и будущее международного частного права / Д. В. Андриянов // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2021. – № 3(79). – С. 190-195. – DOI 10.17803/2311-5998.2021.79.3.190-195.

[3] Гагская конвенция о получении за границей доказательств по гражданским или торговым делам ссыла в список литературы от 18 марта 1970 года // Международные конвенции о взаимодействии судов и судебно-правовом сотрудничестве по гражданским и коммерческим делам. М.: ЮРИТ-Вестник, 2000. С. 18-28.

[4] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // СПС «Гарант» (дата обращения: 15.03.2025)/

[5] Второй Дополнительный протокол к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств (СДСЕ № 224) // Сайт Совета Европы URL: <https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=224> (дата обращения: 15.03.2025)

[6] Миронова А.В. Оказание международной правовой помощи в получении электронных доказательств // Вестник Московского университета МВД России. 2020. №3. С. 78-80.

References:

[1] Paramuzova O. G., Gamova I.V. Legal problems of notarial production in the modern world// Eurasian integration: economics, law, politics. 2023. №4 (46). S. 92-101.

[2] Andriyanov, D.V. Lex petrolea, globalization and the future of private international law/D.V. Andriyanov//Bulletin of the University named after O.E. Kutafin (MSLA). – 2021. – № 3(79). – S. 190-195. – DOI 10.17803/2311-5998.2021.79.3.190-195.

[3] The Hague Convention on Obtaining Evidence Abroad in Civil or Commercial Cases reference to the list of references of March 18, 1970// International Conventions on the Interaction of Courts and Judicial Legal Cooperation in Civil and Commercial Cases. M.: JURIT-Vestnik, 2000. S. 18-28.

[4] Convention on Crime in the Field of Computer Information ETS N 185 (Budapest, November 23, 2001)//ATP "Guarantor" (accessed: 15.03.2025) /

[5] Second Additional Protocol to the Convention on Cybercrime on Enhancing Cooperation and Disclosure of Electronic Evidence (CSCE No. 224)//Council of Europe website URL: <https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=224> (Accessed: 15.03.2025)

[6] A.V. Mironova. Provision of international legal assistance in obtaining electronic evidence// Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. №3. S. 78-80.



ЮРКОМПАНИ
www.law-books.ru

Юридическое издательство «ЮРКОМПАНИ»
издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.