



Научная статья

УДК 34:004: 341.1/8:003.26

EDN: <https://elibrary.ru/zhayee>

DOI: <https://doi.org/10.21202/jdtl.2024.17>

Правовое регулирование международной торговли криптографическими продуктами и технологиями: инструменты ВТО и региональные соглашения

Сайед Кудрат Хашими



Майсурский университет, Майсур, Индия

Джексон Симанго Магоге

Университет Иринга, Иринга, Танзания

Ключевые слова

Всемирная торговая организация,
защита интеллектуальной собственности,
кибербезопасность,
криптография,
международная торговля,
международные соглашения,
недискриминационный режим,
право,
региональные торговые соглашения,
цифровые технологии

Аннотация

Цель: показать сложный правовой ландшафт, меняющийся под воздействием современного цифрового ландшафта, развивающегося в условиях интеграции криптографических технологий в международную торговлю и особенно в сферу продуктов информационно-коммуникационных технологий.

Методы: исследование документов построено прежде всего на совокупности способов толкования актов, позволяющих проанализировать содержание первичных источников права, а именно положений, регулирующих оборот криптографических продуктов, и предложить решения, восполняющие существующие пробелы в этой области. Также для формирования представления о предмете исследования были собраны и обобщены вторичные источники по исследуемой проблематике.

Результаты: выявлены области неопределенности в защите цифровых криптографических продуктов в рамках соглашений ВТО, что ставит под сомнение адекватность существующих мер защиты. Отмечается, что в ряде стран такая ситуация приводит к ограничениям или к полному запрету на импорт и экспорт криптографических технологий и зашифрованных данных по соображениям безопасности. Уделено внимание рассмотрению концепции недискриминационного отношения к криптографическим продуктам, разрабатываемой в первую очередь в рамках региональных торговых соглашений, чтобы устранить недостатки соглашений ВТО. Подчеркивается, что региональные торговые соглашения, несмотря на стимулирования

✉ Контактное лицо

© Хашими С. К., Магоге Дж. С., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

роста сотрудничества и конкуренции в международной торговле, демонстрируют различные подходы к регулированию криптографических продуктов. Отмечается, что это создает проблемы для бизнеса, который должен быть готов к учету особенностей региональных соглашений, местного законодательства и меняющихся правовых требований. Делается вывод о важности баланса между защитой инноваций и содействием доверию и сотрудничеству, развитием криптографических технологий и вопросами безопасности и защиты прав интеллектуальной собственности.

Научная новизна: представлено видение сложного правового ландшафта, окружающего криптографические продукты, показаны различия в подходах к регулированию отношений, связанных с цифровыми и нецифровыми продуктами в рамках соглашений ВТО, и подходы к регулированию криптографических продуктов, применяемые в региональных торговых соглашениях.

Практическая значимость: результаты исследования представляют интерес для государственных органов, политических деятелей, коммерческих структур и частных лиц, участвующих в международной торговле с использованием криптографических технологий, поскольку могут помочь всем заинтересованным сторонам принимать обоснованные решения, ориентироваться в сложностях регулирования указанных отношений и отстаивать справедливое отношение в развивающейся среде цифровой торговли.

Для цитирования

Хашими, С. К., Магоге, Дж. С. (2024). Правовое регулирование международной торговли криптографическими продуктами и технологиями: инструменты ВТО и региональные соглашения. *Journal of Digital Technologies and Law*, 2(2), 328–344. <https://doi.org/10.21202/jdtl.2024.17>

Содержание

Введение

1. Криптография и ее технологические продукты
 - 1.1. Криптографическая продукция и политика в отношении нее ВТО и ОЭСР
2. Соглашения ВТО, касающиеся криптографических продуктов
 - 2.1. Соглашение о технических барьерах в торговле (TBT)
 - 2.2. Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS)
 - 2.3. Соглашение GATT и недискриминационный режим в отношении криптографических продуктов
3. Региональные соглашения, касающиеся криптографических продуктов
 - 3.1. Соглашение между США, Мексикой и Канадой (USMCA)
 - 3.2. Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (Japan – UK EPA)
4. Проблема доступа к криптографическим продуктам

Заключение

Список литературы

Введение

Глобальный ландшафт криптографических продуктов, охватывающих технологии шифрования, аппаратное и программное обеспечение, претерпевает значительные изменения. Это вызывает озабоченность регуляторов в сфере международной торговли (Kumar et al., 2020; Primo Braga, 2005; Kennedy, 2000). В представленном исследовании рассматривается нормативная база в рамках Всемирной торговой организации (далее – ВТО) и региональных торговых соглашений (далее – РТС), затрагиваются вопросы доверия в деловой сфере, прав интеллектуальной собственности и глобальной торговли. В документах ВТО отсутствуют конкретные положения о криптографических продуктах. В Соглашении по торговым аспектам прав интеллектуальной собственности (Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS Agreement, Соглашение ТРИПС) подчеркивается необходимость защиты прав интеллектуальной собственности производителей, но не прописаны исчерпывающие правовые основы такой защиты (Huang & Li, 2024). Соглашение по техническим барьерам в торговле (далее – ТБТ) предусматривает использование технических спецификаций, но они не должны чрезмерно ограничивать торговлю. Такие РТС, как USMCA и Japan – UK EPA, накладывают ограничения на производителей криптографических продуктов, стремясь сбалансировать требования защиты интеллектуальной собственности (далее – ИС) и принципов доверия. Однако эти РТС могут различаться по своим подходам, что создает проблемы для бизнеса. В целом нормативно-правовая база стремится к балансу между защитой ИС и доверием, при этом страны – члены ВТО тщательно следят за тем, чтобы избежать злоупотреблений и адаптироваться к динамичному криптографическому рынку. До наступления «информационной эры» криптография и технологии защиты информации использовались в основном в военных и разведывательных целях (Rogers, 2021). В прошлом эти технологии рассматривались как инструменты ведения войны. Однако за последние тридцать лет криптография приобрела большое значение в обеспечении индивидуальной конфиденциальности в повседневной розничной торговле и потребительских технологиях. В условиях, когда растет обеспокоенность по поводу цензуры и законов о конфиденциальности, безопасность потребителей постоянно находится под угрозой. Они сталкиваются с необходимостью активно защищать свои данные. Кроме того, технологии значительно упростили процесс получения доступа к личной информации, поэтому необходимо понимать, как создать и поддерживать в актуальном состоянии меры по защите данных, соответствующие новейшим достижениям в области технологий защиты информации. Сбалансировать эти тенденции стало возможно благодаря интеграции технологии криптографии в современный цифровой мир (Saper, 2013). Криптография имеет огромное значение, поскольку она служит жизненно важным компонентом в обеспечении безопасности электронной коммерции и электронных коммуникационных систем (Thabit et al., 2023). Она играет ключевую роль в защите конфиденциальных данных как при их хранении, так и при передаче. Значение информационной безопасности постоянно растет по мере того, как продукты и услуги в области информационных технологий занимают все более заметное место на мировом рынке. Кроме того, компании, осуществляющие прямые иностранные инвестиции, делают акцент на высокотехнологичных секторах, которые несут в себе риски для интеллектуальной собственности, что еще больше подчеркивает важность информационной безопасности¹.

¹ Protecting privacy in practice – The current use, development and limits of Privacy Enhancing. (2019, March 20). Policy Commons. <https://clck.ru/3BCb9M>

Таким образом, в контексте международной торговли становится очевидной зависимость от криптографических технологий, поскольку они обеспечивают безопасность многочисленных онлайн-транзакций и способствуют быстрому осуществлению платежей по всему миру. Кроме того, развитие криптографических технологий оказывает значительное влияние на современную деловую практику, поскольку они играют решающую роль в защите корпоративных секретов и конфиденциальной информации от таких угроз, как кража персональных данных. В связи с этим наблюдается рост производства криптографических продуктов, обусловленный рыночным спросом. В настоящее время некоторые страны вводят ограничения на импорт и экспорт криптографических технологий.

Некоторые из них, например Китай, Россия и Израиль, ограничивают импорт зашифрованных данных, а другие, например Северная Корея, ограничивают или полностью запрещают использование шифрования в пределах своих границ². В некоторых странах для отправки шифровальных продуктов за границу требуется официальное разрешение, независимо от того, производятся ли эти продукты внутри страны или нет. Это требование распространяется как на первоначально экспортируемые изделия, так и на те, которые реэкспортируются из страны. Основная цель такого требования – поддержание национальной безопасности и противодействие терроризму.

1. Криптография и ее технологические продукты

Криптография, древнее искусство кодирования и декодирования, стала краеугольным камнем цифровой эпохи, обеспечивая безопасную связь и защиту данных. С помощью математических методов можно сделать данные недоступными для неавторизованных лиц. Целями этого процесса является обеспечение конфиденциальности, целостности и подлинности информации. Эта технология лежит в основе таких продуктов, как приложения для безопасного обмена сообщениями, VPN, аппаратные модули безопасности (HSM), программное обеспечение для шифрования данных и защиты блокчейна. Криптографические инструменты, такие как цифровые подписи, двухфакторная аутентификация (2FA) и PKI, повышают уровень безопасности³. Криптография играет важную роль в защите данных, обеспечении подлинности цифровых документов и укреплении сетевой безопасности с помощью таких протоколов, как SSL и TLS. В условиях взаимосвязанного мира она является неотъемлемым элементом безопасности и конфиденциальности данных.

Криптография – это технология для обеспечения безопасной связи даже в присутствии вредоносных третьих сторон с помощью шифрования и дешифрования. Обычно она предполагает использование вычислительного алгоритма, например SHA256, как в биткойне, открытого ключа и закрытого ключа, который служит цифровой подписью для пользователя. При шифровании сообщения или документа только предполагаемые получатели могут узнать его содержание (Kimani et al., 2020; Zhavorova & Lloyed, 2018; Torrubia et al., 2001).

² Human Rights Watch: Rape common in North Korea. (2018) <https://clck.ru/3BCbAM>

³ Understanding Digital Signatures. (2021, February 1). CISA. <https://clck.ru/3BCbB6>

В рамках международной торговли криптографические технологии могут быть интегрированы как в экспортируемые, так и в импортируемые продукты информационно-коммуникационных технологий (далее – ИКТ). Криптографический продукт включает в себя криптографический модуль; под эту категорию подпадает также защищенное программное обеспечение, способное создавать или воссоздавать ключи или сертификаты (Riebe et al., 2022). Примерами таких продуктов являются зашифрованные смартфоны и ноутбуки, защищенные факс-аппараты, VPN-устройства с возможностью шифрования, устройства для проведения финансовых операций в точках продаж, системы управления складским хозяйством с функцией шифрования; устройства ввода, оснащенные функцией шифрования; стандартные компьютеры, на которые предварительно установлено программное обеспечение для шифрования; медицинские устройства; промышленные и производственные системы, такие как робототехника и тяжелое оборудование; системы для охраны объектов, такие как пожарная сигнализация; а также специализированные компоненты шифрования, например, чипы, маршрутизаторы, шлюзы и брандмауэры.

1.1. Криптографическая продукция и политика в отношении нее ВТО и ОЭСР

В цифровую эпоху, когда конфиденциальность данных и безопасная связь имеют первостепенное значение, криптография играет важную роль в международной торговле. Хотя в соглашениях Всемирной торговой организации криптография прямо не рассматривается, эти документы косвенно влияют на продукты информационно-коммуникационных технологий, использующие криптографические методы (Sholihah & Afriansyah, 2020). Так, Соглашение о технических барьерах в торговле (Agreement on Technical Barriers to Trade, TBT) направлено на предотвращение препятствования международной торговле со стороны технических регламентов. Не упоминая криптографию напрямую, оно постулирует прозрачные и необходимые правила для достижения законных целей, таких как безопасность. Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS) косвенно затрагивает криптографические продукты, защищая права интеллектуальной собственности, в том числе патенты, авторские права и коммерческие тайны, связанные с криптографическими технологиями. Это стимулирует инновации и торговлю продуктами ИКТ, основанными на криптографии.

Организация экономического сотрудничества и развития (далее – ОЭСР) играет важную роль в формировании политики в отношении криптографических продуктов. Эта организация дает рекомендации по безопасности и конфиденциальности данных, что влияет на внедрение криптографических решений. Она подчеркивает важность кибербезопасности, жизненно важным инструментом которой является криптография, и способствует разработке криптографических продуктов. Работа ОЭСР также затрагивает трансграничные потоки данных и косвенно влияет на отрасль через экономическую политику. По сути, влияние ОЭСР на разработку и использование криптографических продуктов имеет глобальное значение для бизнеса и потребителей в цифровую эпоху⁴. В рамках ОЭСР были разработаны правила,

⁴ OECD Guidelines for Cryptography Policy – OECD. (n.d.). Retrieved October 16, 2023. <https://clck.ru/3BCf5o>

касающиеся криптографии. Криптография играет важную роль в повышении безопасности информационно-коммуникационных сетей и систем, однако ее неправильное использование может пагубно сказаться на функциональности электронной коммерции и защите частной жизни. В 1997 г. ОЭСР представила Руководство по политике в области криптографии. В нем изложены принципы политики в области криптографии, одним из которых является законный доступ. В документе отмечено, что национальные нормы в области криптографии могут предоставлять законный доступ к незашифрованным данным или криптографическим ключам при условии, что эти нормы соответствуют принципам, изложенным в других руководствах.

2. Соглашения ВТО, касающиеся криптографических продуктов

2.1. Соглашение о технических барьерах в торговле (ТВТ)

Основная цель Соглашения по техническим барьерам в торговле (TBT Agreement) Всемирной торговой организации заключается в том, чтобы технические регламенты, стандарты и процедуры оценки соответствия не создавали ненужных препятствий для международной торговли. Хотя указанное Соглашение не содержит конкретных положений, регулирующих технические барьеры, связанные с криптографическими продуктами, оно позволяет странам – членам ВТО, согласно ст. 2.2, устанавливать технические спецификации для продуктов, включающих криптографические технологии, при условии, что эти спецификации не являются «более ограничивающими торговлю, чем это необходимо для достижения законной цели» (Lin et al., 2021). Кроме того, ст. 5 предоставляет странам – членам ВТО право обеспечивать соответствие импортируемых продуктов с криптографической технологией этим техническим спецификациям в соответствии с правилами, изложенными в Соглашении. Что касается устранения определенных барьеров, связанных с криптографическими продуктами в Китае, в частности, в контексте пересмотренного законопроекта КНР о шифровании, изданного государственным Управлением по вопросам коммерческой криптографии (OSCCA), Канада выразила свою обеспокоенность (Kang, 1998), запросив у Китая гарантии того, что практические нормы предусматривают:

- 1) определение сферы применения таким образом, чтобы обеспечить достижение законных целей в отношении криптографических товаров;
- 2) четкое указание на то, что стандарты будут установлены в соответствии с принципом прозрачности;
- 3) четкое указание важности использования международных стандартов, когда это возможно.

2.2. Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS)

Соглашение TRIPS не содержит четких положений, касающихся криптографических продуктов. Тем не менее ст. 10(1) Соглашения предписывает защищать исходный код, если он подпадает под защиту патента, авторского права или коммерческой тайны. Кроме того, Соглашение TRIPS предусматривает, что компьютерные программы, независимо от того, представлены ли они в исходном или объектном коде, должны рассматриваться как литературные произведения, охраняемые в соответствии с Бернской конвенцией 1971 г.

2.3. Соглашение ГАТТ и недискриминационный режим в отношении криптографических продуктов

Концепция «недискриминационного отношения к криптографическим продуктам» подчеркивает беспристрастное регулирование со стороны правительств и регулирующих органов. Она направлена на обеспечение справедливых стандартов для всех криптографических продуктов, как отечественных, так и международных, признавая их роль в обеспечении безопасности данных. Ключевые принципы включают равный доступ на рынок, защиту конфиденциальности и международное сотрудничество. Эта концепция ставит во главу угла справедливость, прозрачность и оценку продукта на основе технических достоинств, а не происхождения, тем самым поддерживая развитие криптографии для обеспечения безопасности цифровых коммуникаций и защиты данных в нашем взаимосвязанном мире. Статья I Генерального соглашения по тарифам и торговле (General Agreement on Tariffs and Trade, GATT) предписывает, что государства – члены Соглашения не должны проявлять фаворитизма по отношению к своим торговым партнерам и создавать для них режим наибольшего благоприятствования, а также должны избегать дискриминации между своими и иностранными товарами, как это сформулировано в ст. III (Baldwin et al., 2000).

Аналогичным образом, Генеральное соглашение по торговле услугами (General Agreement on Trade in Services, GATS) требует, чтобы иностранным услугам предоставлялся режим наибольшего благоприятствования в соответствии со ст. II. Однако национальный режим, подробно описанный в ст. XVII, не является обязательным, если только государство-член не взяло на себя особые обязательства по его предоставлению (Muller, 2017). Несмотря на то, что GATT и GATS запрещают дискриминационный режим в отношении товаров и услуг, остается неясным, получают ли «цифровые продукты, включая криптографические», такую же защиту, как и нецифровые продукты в рамках соглашений ВТО. Кроме того, Орган по разрешению споров (Dispute Settlement Body, DSB) не дал никаких разъяснений относительно регулирования и защиты криптографических продуктов в соответствии с соглашениями ВТО. С ростом поставок продукции в цифровых форматах все большее значение приобретают вопросы справедливого отношения к «криптографическим продуктам».

В связи с этим концепция недискриминации разрабатывается в первую очередь в рамках региональных торговых соглашений, чтобы устранить недостатки соглашений ВТО. Однако важно отметить, что РТС обычно ссылаются на принципы, установленные в рамках соглашений ВТО.

3. Региональные соглашения, касающиеся криптографических продуктов

Региональные торговые соглашения оказывают значительное влияние на торговлю и регулирование криптографических продуктов в отдельных регионах. Они способствуют экономической интеграции и снижению торговых барьеров между странами-участницами, поощряя стандартизацию технических протоколов, снижение тарифов и расширение доступности рынков (Rahman & Rahman, 2022). РТС также оказывают влияние на права интеллектуальной собственности и правила защиты данных для технологий шифрования. Они способствуют росту сотрудничества и конкуренции в сфере безопасности, стимулируя инновации в криптографических

продуктах. Однако их конкретное воздействие зависит от условий соглашения, отраслевого и местного законодательства, что требует от предприятий бдительного контроля для адаптации к меняющимся правовым требованиям.

Речь идет о двусторонних или многосторонних торговых соглашениях, основанных на взаимных предпочтениях и санкционированных ВТО. В ст. XXIV:5 ГАТТ предусмотрено создание таможенных союзов, зон свободной торговли или соглашений между регионами участвующих сторон (Dam, 1963). Аналогичным образом, согласно ст. V:1 ГАТС, страны-члены могут заключать соглашения, способствующие либерализации торговли. Ниже рассмотрим региональные торговые соглашения, содержащие особые положения в отношении продуктов ИКТ с использованием технологий шифрования.

3.1. Соглашение между США, Мексикой и Канадой (USMCA)

Соглашение между США, Мексикой и Канадой (USMCA) существенно влияет на рынок криптографических продуктов в Северной Америке. Оно затрагивает вопросы интеллектуальной собственности, локализации данных и цифровой торговли, влияя на развитие и регулирование криптографических технологий. Соглашение способствует сотрудничеству в области регулирования и доступности рынков, что благоприятно сказывается на предприятиях и потребителях в этой сфере⁵. Кроме того, в нем сделан акцент на сотрудничестве в области кибербезопасности, что подчеркивает важность криптографических продуктов для обеспечения безопасности и конфиденциальности данных. Компаниям данного сектора предлагается отслеживать, как положения Соглашения повлияют на их деятельность и соблюдение требований законодательства в регионе.

Указанное Соглашение выступило заменой Североамериканскому соглашению о свободной торговле (The North American Free Trade Agreement, NAFTA), действовавшему с января 1994 г. Оно было одобрено тремя странами 30 ноября 2018 г. и вступило в силу 1 июля 2020 г. Это соглашение рассматривается как взаимовыгодное для сотрудников и владельцев промышленных и сельскохозяйственных предприятий стран Северной Америки (van der Linden & Shirazi, 2023).

3.2. Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (Japan – UK EPA)

Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (The Japan – UK Comprehensive Economic Partnership Agreement, Japan – UK EPA) в первую очередь направлено на сферы торговли и экономики, но имеет последствия для криптографических продуктов. Оно упрощает доступ к рынкам за счет снижения торговых барьеров, решает вопросы интеллектуальной собственности, поощряет сотрудничество в сфере регулирования, а также затрагивает вопросы конфиденциальности данных и сотрудничества в области кибербезопасности (Riebe et al., 2022). Электронная коммерция и цифровая торговля также влияют на цифровой рынок криптографических продуктов. Предприятия этого сектора

⁵ United States – Mexico – Canada Agreement. United States Trade Representative. (n. d.). <https://clck.ru/3BCbhB>

должны знать положения данного Соглашения, чтобы соответствовать требованиям и полноценно использовать рыночные возможности.

Указанное соглашение о свободной торговле было подписано в Токио в октябре 2020 г. Оно направлено на содействие либерализации торговли и инвестиций, укреплению экономических отношений между сторонами-участницами и включает элементы соглашений ВТО. Примечательно, что ст. 1.9 Соглашения запрещает любые действия сторон, противоречащие их обязательствам по соглашениям ВТО. Документ также содержит положения, касающиеся коммерческих продуктов ИКТ, использующих криптографию.

Национальный режим в таких торговых соглашениях, как Japan – UK EPA и USMCA, имеет решающее значение для криптографических продуктов. Он обеспечивает равный режим для отечественных и иностранных криптографических товаров, способствуя честной конкуренции и доступу на рынок. Оба указанных соглашения поддерживают этот принцип, устраняя дискриминацию по признаку происхождения продукции (Burri, 2021). Это крайне важно в связи с чувствительным характером криптографических технологий, а также с необходимостью содействовать инновациям и кибербезопасности. Предприятия этой отрасли должны строго соблюдать нормы соглашений для обеспечения соответствия требованиям законодательства и равного доступа на рынки.

Документы не содержат четкого описания национального режима криптографических продуктов. Однако, согласно ст. 2.7 Japan – UK EPA и 2.3 USMCA, каждая сторона обязана предоставлять национальный режим товарам другой стороны, как указано в ст. III GATT (Burri, 2023). Кроме того, частью соглашений являются ст. III и XX GATT. Таким образом, защита криптографических продуктов обеспечивается положениями этих конкретных статей.

4. Проблема доступа к криптографическим продуктам

Для обеспечения безопасности и конфиденциальности данных жизненно важен доступ к криптографическим продуктам. Эти продукты используют сложные алгоритмы для защиты информации от киберугроз и обеспечения целостности данных. Они необходимы для защиты персональных данных, национальной безопасности и безопасных онлайн-транзакций⁶. Однако глобальное регулирование повлияет на режим такого доступа, и может быть крайне сложно достичь баланса между требованиями безопасности и доступности. Ключевым фактором для трансграничной защиты данных является международное сотрудничество. Поскольку криптографические продукты выпускаются в различных формах, важнейшее значение имеет повышение осведомленности и их правильное использование. Таким образом, доступ к криптографическим продуктам необходим для защиты данных, обеспечения конфиденциальности и безопасности в условиях развивающейся нормативной базы.

Доступ к криптографическим продуктам подразумевает передачу или получение доступа к закрытому ключу или другим конфиденциальным параметрам, особенностям алгоритма или деталям конструкции стороной или лицом, находящимся

⁶ OECD Guidelines for Cryptography Policy – OECD. (n.d.). <https://clck.ru/3BCf5o>

под юрисдикцией этой стороны (например, производителями или поставщиками)⁷. Соглашения Всемирной торговой организации прямо не затрагивают вопрос доступа к криптографическим продуктам. Однако Соглашение между США, Мексикой и Канадой (USMCA) и Соглашение об экономическом партнерстве между Японией и Великобританией (EPA) накладывают ограничения на своих участников, заставляя производителей и поставщиков криптографических продуктов передавать или предоставлять доступ к патентованной информации, связанной с криптографией. USMCA налагает строгие ограничения на все криптографические товары, тогда как EPA ограничивает доступ к коммерческой информации и продуктам информационно-коммуникационных технологий, использующим криптографию, включая программное обеспечение. Обоснованием введения этих ограничений на доступ к криптографическим продуктам является установление доверительных деловых отношений между участниками соглашения и соблюдение положений статьи 10(1) Соглашения по торговым аспектам прав интеллектуальной собственности (TRIPS), которая обеспечивает защиту прав интеллектуальной собственности для производителей⁸. Напротив, Руководство по политике в области криптографии ОЭСР предлагает альтернативный подход к доступу к криптографическим продуктам. Национальное законодательство в области криптографии может разрешать законный доступ к открытому тексту или криптографическим ключам для зашифрованных данных, но при этом должны соблюдаться и другие принципы, изложенные в Руководстве. Страны-участницы могут по своему усмотрению принимать законы, касающиеся доступа к криптографическим продуктам, однако существует опасность злоупотреблений в этой сфере.

Важно отметить, что в соответствии со ст. 2.2 Соглашения о технических барьерах в торговле членам ВТО разрешается устанавливать технические спецификации для продуктов, использующих технологию криптографии, при условии, что эти спецификации не создают торговых барьеров, которые являются более ограничительными, чем это необходимо для достижения законной цели. Возникает вопрос, может ли разрешение законного доступа к криптографическим продуктам представлять собой злоупотребление в области делового доверия и прав интеллектуальной собственности.

Заключение

В заключение следует отметить, что криптография – играет важную роль в обеспечении безопасности связи, защиты данных, конфиденциальности, целостности и подлинности информации. От безопасных приложений для обмена сообщениями до защиты блокчейна – применение криптографических технологий разнообразно и широко распространено, они лежат в основе современного цифрового ландшафта. Интеграция криптографических технологий в международную торговлю, особенно в сферу продуктов информационно-коммуникационных технологий, порождает сложные проблемы регулирования. Хотя соглашения Всемирной торговой организации прямо не касаются криптографии, они косвенно влияют на криптографические продукты, способствуя прозрачному регулированию в целях безопасности и защиты

⁷ Encryption in the Microsoft Cloud. Microsoft. <https://clck.ru/3BCboE>

⁸ WTO. Overview: the TRIPS Agreement. (n. d.). <https://clck.ru/3BCbpN>

прав интеллектуальной собственности. Соглашение по техническим барьерам в торговле призвано предотвратить препятствование международной торговле со стороны технических норм, а Соглашение по торговым аспектам прав интеллектуальной собственности (TRIPS) косвенно защищает права интеллектуальной собственности, связанные с криптографическими технологиями, тем самым способствуя инновациям и торговле продуктами ИКТ, использующими криптографию.

Проблема недискриминационного отношения к криптографическим продуктам по-прежнему вызывает серьезную озабоченность. Решить эту проблему, предлагая рамки для обращения с криптографическими продуктами, призваны региональные торговые соглашения, такие как Соглашение между США, Мексикой и Канадой (USMCA) и Соглашение о всеобъемлющем экономическом партнерстве между Японией и Великобританией (Japan – UK EPA). Сложная и непрерывно развивающаяся нормативная база для криптографических продуктов подчеркивает необходимость международных соглашений для адаптации к меняющемуся ландшафту глобального криптографического рынка. Для формирования будущего международной торговли криптографическими продуктами очень важен баланс между защитой инноваций и содействием доверию и сотрудничеству. Кроме того, продолжающиеся дебаты вокруг использования экспортных и импортных ограничений, препятствующих развитию криптовалютных технологий, подчеркивают важность этого вопроса в глобальном масштабе.

Таким образом, по мере того как мир становится все более взаимосвязанным и зависимым от криптографических технологий, международные соглашения, национальные нормы и региональные торговые соглашения будут продолжать играть ключевую роль в формировании политики в отношении криптографических продуктов, обеспечивая инновации и безопасность в цифровую эпоху.

Список литературы

- Baldwin, R. E., McLaren, J., & Panagariya, A. (2000). Regulatory Protectionism, Developing Nations, and a Two-Tier World Trade System. *Brookings Trade Forum*, 3(2674), 237–293. <https://doi.org/10.1353/btf.2000.0001>
- Burri, M. (2021). Data Flows and Global Trade Law. In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 11–41). Cambridge University Press. <https://doi.org/10.1017/9781108919234.003>
- Burri, M. (2023). A WTO agreement on electronic commerce: an inquiry into its legal substance and viability. *Georgetown Journal of International Affairs*, 53(4), 565–625.
- Dam, K. W. (1963). Regional Economic Arrangements and the GATT: The Legacy of a Misconception. *The University of Chicago Law Review*, 30(4), 615–665. <https://doi.org/10.2307/1598756>
- Huang, Q., & Li, Z. (2024). Trade and peace: The WTO case. *China Economic Review*, 83, 102072. <https://doi.org/10.1016/j.chieco.2023.102072>
- Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 50(4), 1193–1294. <https://doi.org/10.2307/1229286>
- Kennedy, G. (2000). Encryption Policies: codemakers, codebreakers and rulemakers. *Computer Law & Security Review*, 16(4), 240–247. [https://doi.org/10.1016/s0267-3649\(00\)89131-1](https://doi.org/10.1016/s0267-3649(00)89131-1)
- Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J., & Kim, J. (2020). Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how? *Technological Forecasting and Social Change*, 161(161), 120254. <https://doi.org/10.1016/j.techfore.2020.120254>
- Kumar, G., Saha, R., Buchanan, W. J., Geetha, G., Thomas, R., Rai, M. K., Kim, T.-H., & Alazab, M. (2020). Decentralized accessibility of e-commerce products through blockchain technology. *Sustainable Cities and Society*, 62, 102361. <https://doi.org/10.1016/j.scs.2020.102361>
- Lin, C.-F., Peng, S., & Streinz, T. (Eds.). (2021). Reconceptualizing World Trade Organization Law for the Artificial Intelligence Economy. In *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Part II, pp. 95–172). Cambridge University Press.

- Muller, G. (2017). Troubled Relationships under the GATS: Tensions between Market Access (Article XVI), National Treatment (Article XVII), and Domestic Regulation (Article VI). *World Trade Review*, 16(3), 449–474. <https://doi.org/10.1017/S1474745616000471>
- Primo Braga, C. A. (2005). E-commerce regulation: New game, new rules? *The Quarterly Review of Economics and Finance*, 45(2–3), 541–558. <https://doi.org/10.1016/j.qref.2004.12.019>
- Rahman, M. N., & Rahman, N. (2022). Exploring digital trade provisions in Regional Trade Agreements (RTAs) in times of crisis: India and Asia-Pacific countries. *Asia and the Global Economy*, 2(2), 100036. <https://doi.org/10.1016/j.aglobe.2022.100036>
- Riebe, T., Kühn, P., Imperatori, P., & Reuter, C. (2022). U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance. *European Journal for Security Research*, 7(1), 39–65. <https://doi.org/10.1007/s41125-022-00080-0>
- Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age: What Happened? *The Cyber Defense Review*, 6(1), 81–106.
- Saper, N. (2013). International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property*, 11(7), 673.
- Sholihah, R., & Afriansyah, A. (2020). Regulation of Crypto Currency in World Trade Organization. In *Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*. <https://doi.org/10.2991/aebmr.k.200321.006>
- Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography Algorithms for Enhancing IoT Security. *Internet of Things*, 22, 100759. <https://doi.org/10.1016/j.iot.2023.100759>
- Torrubia, A., Mora, F. J., & Marti, L. (2001). Cryptography Regulations for E-commerce and Digital Rights Management. *Computers & Security*, 20(8), 724–738. [https://doi.org/10.1016/s0167-4048\(01\)00814-8](https://doi.org/10.1016/s0167-4048(01)00814-8)
- van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, 9(1), 22. <https://doi.org/10.1186/s40854-022-00432-8>
- Zharova, A., & Lloyd, I. (2018). An examination of the experience of cryptocurrency use in Russia. In search of better practice. *Computer Law & Security Review*, 34(6), 1300–1313. <https://doi.org/10.1016/j.clsr.2018.09.004>

Сведения об авторах



Хашими Сайед Кудрат – PhD в области права, кафедра правоведения, Майсурский университет

Адрес: Индия, г. Майсур, 570005, Вишвавидьянилай Карья Судха, Крофорд Холл

E-mail: sayedqudrathashimy@law.uni-mysore.ac.in

ORCID ID: <https://orcid.org/0000-0001-9835-0575>

Google Scholar ID: https://scholar.google.com/citations?user=_XhWcpEAAAAJ



Мароге Джексон Симанго – ассистент преподавателя, Университет Иринга

Адрес: Танзания, г. Иринга, а/я 200

E-mail: simangojackson@gmail.com

ORCID ID: <https://orcid.org/0000-0001-8096-6929>

Google Scholar ID: <https://scholar.google.com/citations?user=8FERpVoAAAAJ>

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают 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: 10.89.27 / Обязательственное право

Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 16 октября 2023 г.

Дата одобрения после рецензирования – 10 ноября 2023 г.

Дата принятия к опубликованию – 25 июня 2024 г.

Дата онлайн-размещения – 30 июня 2024 г.



Research article

UDC 34:004: 341.1/8:003.26

EDN: <https://elibrary.ru/zhayee>

DOI: <https://doi.org/10.21202/jdtl.2024.17>

Legal Regulation of International Trade in Cryptographic Products and Technologies: WTO Tools and Regional Agreements

Sayed Qudrat Hashimy ✉

University of Mysore, Mysore, India

Jackson Simango Magoge

University of Iringa, Iringa, Tanzania

Keywords

cryptography,
cybersecurity,
digital technologies,
intellectual property rights
protection,
international agreements,
international trade,
law,
non-discriminatory regime,
regional trade agreements,
World Trade Organization

Abstract

Objective: to demonstrate the complex legal landscape which is being changed under the influence of the modern digital landscape developing with the integration of cryptographic technologies into international trade and especially into the field of information and communication technology products.

Methods: the study of the documents is built primarily on a set of ways of interpreting legal acts, which allows analyzing the content of primary legal sources, namely the provisions for cryptographic products circulation, and proposing solutions to fill the gaps in this area. Also, secondary sources were collected and summarized to form an idea of the study subject.

Results: areas of uncertainty in the protection of digital cryptographic products under the WTO agreements have been identified, raising questions about the adequacy of existing protection measures. It is noted that in some countries this situation has led to restrictions or bans on the import and export of cryptographic technologies and encrypted data on security grounds. The authors pay attention to the concept of non-discriminatory treatment of cryptographic products, which is being developed primarily within the framework of regional trade agreements to address the shortcomings of WTO agreements. It is emphasized that regional trade agreements,

✉ Corresponding author

© Hashimy S. Q., Magoge J. S., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

although stimulating cooperation and competition in international trade, demonstrate various approaches to the regulation of cryptographic products. The authors note that this creates challenges for business and it must be prepared to take into account the specificities of regional agreements, local legislation and evolving legal requirements. A conclusion is made that it is important to balance the innovation protection with the promotion of trust and cooperation, between the cryptographic technologies development and the issues of security and intellectual property rights protection.

Scientific novelty: a vision of the complex legal landscape surrounding cryptographic products is presented, showing the differences in approaches to regulating relations around digital and non-digital products under WTO agreements and approaches to regulating cryptographic products applied in regional trade agreements.

Practical significance: the study results are of interest to government agencies, policy makers, commercial entities and individuals involved in international trade in cryptographic technologies, as they can help all stakeholders to make informed decisions, navigate the complexities of regulating these relationships and advocate for fair treatment in the evolving digital trade environment.

For citation

Hashimy, S. Q., & Magoge, J. S. (2024). Legal Regulation of International Trade in Cryptographic Products and Technologies: WTO Tools and Regional Agreements. *Journal of Digital Technologies and Law*, 2(2), 328–344. <https://doi.org/10.21202/jdtl.2024.17>

References

- Baldwin, R. E., McLaren, J., & Panagariya, A. (2000). Regulatory Protectionism, Developing Nations, and a Two-Tier World Trade System. *Brookings Trade Forum*, 3(2674), 237–293. <https://doi.org/10.1353/btf.2000.0001>
- Burri, M. (2021). Data Flows and Global Trade Law. In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 11–41). Cambridge University Press. <https://doi.org/10.1017/9781108919234.003>
- Burri, M. (2023). A WTO agreement on electronic commerce: an inquiry into its legal substance and viability. *Georgetown Journal of International Affairs*, 53(4), 565–625.
- Dam, K. W. (1963). Regional Economic Arrangements and the GATT: The Legacy of a Misconception. *The University of Chicago Law Review*, 30(4), 615–665. <https://doi.org/10.2307/1598756>
- Huang, Q., & Li, Z. (2024). Trade and peace: The WTO case. *China Economic Review*, 83, 102072. <https://doi.org/10.1016/j.chieco.2023.102072>
- Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 50(4), 1193–1294. <https://doi.org/10.2307/1229286>
- Kennedy, G. (2000). Encryption Policies: codemakers, codebreakers and rulemakers. *Computer Law & Security Review*, 16(4), 240–247. [https://doi.org/10.1016/s0267-3649\(00\)89131-1](https://doi.org/10.1016/s0267-3649(00)89131-1)
- Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J., & Kim, J. (2020). Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how? *Technological Forecasting and Social Change*, 161(161), 120254. <https://doi.org/10.1016/j.techfore.2020.120254>
- Kumar, G., Saha, R., Buchanan, W. J., Geetha, G., Thomas, R., Rai, M. K., Kim, T.-H., & Alazab, M. (2020). Decentralized accessibility of e-commerce products through blockchain technology. *Sustainable Cities and Society*, 62, 102361. <https://doi.org/10.1016/j.scs.2020.102361>

- Lin, C.-F., Peng, S., & Streinz, T. (Eds.). (2021). Reconceptualizing World Trade Organization Law for the Artificial Intelligence Economy. In *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Part II, pp. 95–172). Cambridge University Press.
- Muller, G. (2017). Troubled Relationships under the GATS: Tensions between Market Access (Article XVI), National Treatment (Article XVII), and Domestic Regulation (Article VI). *World Trade Review*, 16(3), 449–474. <https://doi.org/10.1017/S1474745616000471>
- Primo Braga, C. A. (2005). E-commerce regulation: New game, new rules? *The Quarterly Review of Economics and Finance*, 45(2–3), 541–558. <https://doi.org/10.1016/j.qref.2004.12.019>
- Rahman, M. N., & Rahman, N. (2022). Exploring digital trade provisions in Regional Trade Agreements (RTAs) in times of crisis: India and Asia-Pacific countries. *Asia and the Global Economy*, 2(2), 100036. <https://doi.org/10.1016/j.aglobe.2022.100036>
- Riebe, T., Kühn, P., Imperatori, P., & Reuter, C. (2022). U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance. *European Journal for Security Research*, 7(1), 39–65. <https://doi.org/10.1007/s41125-022-00080-0>
- Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age: What Happened? *The Cyber Defense Review*, 6(1), 81–106.
- Saper, N. (2013). International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property*, 11(7), 673.
- Sholihah, R., & Afriansyah, A. (2020). Regulation of Crypto Currency in World Trade Organization. In *Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*. <https://doi.org/10.2991/aebmr.k.200321.006>
- Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography Algorithms for Enhancing IoT Security. *Internet of Things*, 22, 100759. <https://doi.org/10.1016/j.iot.2023.100759>
- Torrubia, A., Mora, F. J., & Marti, L. (2001). Cryptography Regulations for E-commerce and Digital Rights Management. *Computers & Security*, 20(8), 724–738. [https://doi.org/10.1016/s0167-4048\(01\)00814-8](https://doi.org/10.1016/s0167-4048(01)00814-8)
- van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, 9(1), 22. <https://doi.org/10.1186/s40854-022-00432-8>
- Zharova, A., & Lloyd, I. (2018). An examination of the experience of cryptocurrency use in Russia. In search of better practice. *Computer Law & Security Review*, 34(6), 1300–1313. <https://doi.org/10.1016/j.clsr.2018.09.004>

Authors information



Sayed Qudrat Hashimy – PhD Scholar (Law), Department of Studies in Law, University of Mysore

Address: Vishwavidyanilaya Karya Soudha, Crawford Hall, Mysuru-570005, India

E-mail: sayedqudrathashimy@law.uni-mysore.ac.in

ORCID ID: <https://orcid.org/0000-0001-9835-0575>

Google Scholar ID: https://scholar.google.com/citations?user=_XhWcpEAAAAJ



Jackson Simango Magoge – Assistant Lecturer, University of Iringa

Address: P.O Box 200, Iringa, Tanzania

E-mail: simangojackson@gmail.com

ORCID ID: <https://orcid.org/0000-0001-8096-6929>

Google Scholar ID: <https://scholar.google.com/citations?user=8FERpVoAAAAJ>

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors 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 – October 16, 2023

Date of approval – November 10, 2024

Date of acceptance – June 25, 2024

Date of online placement – June 30, 2024