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

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

Contents

Introduction

The global cryptographic product landscape, spanning encryption tech, hardware, and software, has evolved significantly, raising regulatory concerns in international trade (Kumar et al., 2020; Primo Braga, 2005; Kennedy, 2000). This analysis explores the regulatory framework within WTO and Regional Trade Agreements (RTAs), touching on matters of business trust, intellectual property rights, and global trade. While WTO lacks specific cryptographic product provisions, the TRIPS Agreement emphasizes protecting manufacturers' IP rights without an exhaustive framework (Huang & Li, 2024). The TBT Agreement permits technical specifications, but they should not unduly restrict trade. RTAs, like the USMCA and Japan – UK EPA, impose restrictions on cryptographic product manufacturers, aiming to balance IP protection and trust. These RTAs, however, may differ in their approaches, presenting challenges for businesses. In summary, the regulatory frameworks seek a balance between IP protection and trust, with careful discretion by WTO members to avoid misuse while adapting to a dynamic cryptographic market. Before the 'information age' emerged, cryptography and information security technology were primarily used for military and intelligence purposes (Rogers, 2021). In the past, these technologies were regarded as tools of warfare. However, in the last thirty years, cryptography has gained increasing significance in ensuring individual privacy in everyday retail and consumer technologies. With the growing concerns over censorship and privacy laws, consumer security is constantly under threat. This makes it essential for individuals to actively protect their data. Moreover, technology has greatly simplified the process of accessing someone's personal information, highlighting the need to understand how to safeguard data and keep it updated with the advancements in data protection technology. Striking this balance has become more manageable with the integration of cryptography technology in today's digital world (Saper, 2013). Cryptography holds paramount significance because it serves as a vital component in ensuring the safety of e-commerce and electronic communication systems (Thabit et al., 2023). It plays a pivotal role in safeguarding sensitive data during both storage and transmission. Furthermore, the significance of information security is on the rise, particularly as information technology products and services become increasingly prominent in the global market. In addition, companies involved in foreign direct investment are placing greater emphasis on high-tech sectors, which carry inherent risks to intellectual property, further underscoring the importance of information security[1].

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

Hence, the growing dependence on cryptographic technology is evident in the context of international trade, as it safeguards numerous online transactions and facilitates swift global payments. Likewise, the evolution of cryptographic technology significantly influences contemporary business practices, as it plays a crucial role in shielding corporate secrets and confidential data from threats like identity theft. Consequently, there is an upsurge in the production of cryptographic products, driven by market demand. At present, certain nations impose limitations on the import and export of cryptographic technology.

In contrast, some, like China, Russia, and Israel, place restrictions on the importation of encrypted data, while others, like North Korea, either restrict or outright ban the use of encryption within their borders[2]. In some countries, the act of sending encryption products abroad necessitates official authorization, regardless of whether these products are domestically manufactured or not. This authorization requirement extends to both initially exported items and those re-exported from the country. The primary objective of this authorization process is to uphold national security and counteract terrorism.

1. Cryptography and Its Technological Products

Cryptography, an ancient art of encoding and decoding, has evolved into a cornerstone of the digital age, ensuring secure communication and data protection. It uses mathematical techniques to render data unintelligible to unauthorized individuals. The goals are confidentiality, integrity, and authenticity. This technology underpins products such as secure messaging apps, VPNs, hardware security modules (HSMs), data encryption software, and blockchain security. Cryptographic tools like digital signatures, Two-Factor Authentication (2FA), and PKI enhance security[3]. Cryptography plays a vital role in protecting data, ensuring the authenticity of digital documents, and fortifying network security through protocols like SSL and TLS. In an interconnected world, it's an indispensable element of data security and privacy.

Cryptography is a technique that uses encryption and decryption to ensure secure communication, even in the presence of malicious third parties. It typically involves the use of a computational algorithm, such as SHA256 as seen in Bitcoin, a publicly shared key, and a privately held key that serves as a digital signature for the user. Encryption involves taking a message or document and scrambling it in a way that only the intended recipients can decipher its contents (Kimani et al., 2020; Zharova & 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

Cryptographic technology can be integrated into both exported and imported information and communication technology (ICT) products within the realm of international trade. A cryptographic product includes a cryptographic module, which means that safeguarded software capable of generating or regenerating keys or certificates can also fall under this category (Riebe et al., 2022). Examples of such products encompass encrypted smartphones and laptops, secure fax machines, VPN devices with encryption capabilities, point-of-sale devices for financial transactions, inventory management systems featuring encryption, input devices equipped with encryption functionality, standard computers preloaded with encryption software, encrypted medical devices, industrial and manufacturing systems like robotics and heavy machinery, facility systems such as fire alarms, as well as specialized encryption components like chips, routers, gateways, and firewalls.

1.1. Cryptographic products and WTO and OECD policy on them

In the digital age, where data privacy and secure communication are paramount, cryptography plays a vital role in international trade. While not explicitly addressing cryptography, World Trade Organization (WTO) Agreements indirectly impact information and communication technology (ICT) products using cryptographic techniques (Sholihah & Afriansyah, 2020). The Agreement on Technical Barriers to Trade (TBT) aims to prevent technical regulations from obstructing international trade. While not mentioning cryptography, it promotes transparent and necessary regulations, ensuring they serve legitimate objectives like security. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) indirectly affects cryptographic products by safeguarding intellectual property rights, including patents, copyrights, and trade secrets related to cryptographic technology. This encourages innovation and trade in ICT products reliant on cryptography.

The OECD is influential in shaping policies regarding cryptographic products. It provides guidelines on data security and privacy, impacting the adoption of cryptographic solutions. It underscores cybersecurity's importance, with cryptography as a vital tool, and influences the development of cryptographic products. The OECD's work also affects cross-border data flows and indirectly impacts the industry through economic policies. In essence, the OECD's influence on cryptographic products' development and utilization has global ramifications for businesses and consumers in the digital era[4]. The OECD has laid down regulations concerning cryptography. While cryptography can be instrumental in enhancing the security of information and communication networks and systems,

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

its improper use can have detrimental effects on e-commerce functionality and privacy protection. In 1997, the OECD introduced the Guidelines for Cryptography Policy. These guidelines outline principles for cryptography policies, one of which is lawful access. It acknowledges that national cryptography policies may grant legal access to unencrypted data or cryptographic keys, provided that these policies adhere to the principles outlined in the other guidelines.

2. WTO Agreements related to Cryptographic Products

2.1. Agreement on Technical Barriers to Trade

The primary goal of the World Trade Organization's Agreement on Technical Barriers to Trade (TBT Agreement) is to ensure that technical regulations, standards, and conformity assessment procedures do not create unnecessary obstacles to international trade. While the TBT Agreement does not contain specific provisions governing technical barriers related to cryptographic products, it allows WTO Members, under Article 2.2, to establish technical specifications for products incorporating cryptographic technology, provided that these specifications are not "more trade-restrictive than necessary to achieve a legitimate objective". (Lin et al., 2021). Additionally, Article 5 grants WTO Members the right to ensure that imported products with cryptographic technology comply with these technical specifications in accordance with the rules outlined in the Agreement. Regarding the issue of addressing certain barriers related to cryptographic products in China, specifically in the context of the Draft revised Encryption Law of the People's Republic of China issued by the Office of State Commercial Cryptography Administration (OSCCA), Canada expressed its concerns (Kang, 1998). Canada sought assurance from China that the implementing regulations would address these concerns by:

Defining the scope of application in a manner that ensures the pursuit of legitimate objectives for cryptographic goods.

Clearly specifying that standards would be established in accordance with the transparency requirements of the TBT Agreement.

Explicitly emphasizing the importance of using international standards whenever possible.

2.2. Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)

The TRIPS Agreement lacks explicit clauses related to cryptographic products. Nonetheless, Article 10(1) of the agreement mandates the safeguarding of source code when it falls under the purview of patent, copyright, or trade secrets protection. Furthermore, the TRIPS Agreement stipulates that computer programs, regardless of whether they are in source or object code, should be treated as literary works protected in accordance with the Berne Convention of 1971.

2.3. GATT and non-discriminatory treatment of cryptographic products

The concept of "non-discriminatory treatment of cryptographic products" emphasizes impartial regulation by governments and regulatory bodies. It aims to ensure fair standards for all cryptographic products, whether domestic or international, recognizing their role in data security. Key principles include equal market access, protection of privacy, and international collaboration. This concept prioritizes fairness, transparency, and product evaluation based on technical merits rather than origin, supporting the evolution of cryptography for secure digital communications and data protection in our interconnected world. The GATT, in Article I, mandates that a member state should not show favoritism among its trading partners, following the "most-favored-nation treatment" principle, and it should also avoid discrimination between its own and foreign products, as articulated in Article III (Baldwin et al., 2000).

Similarly, the GATS requires that foreign services be granted the most-favored-nation treatment according to Article II. However, national treatment, as detailed in Article XVII, is not obligatory unless a Member state has specifically committed to it in their schedules (Muller, 2017). Despite the GATT and the GATS prohibiting discriminatory treatment of goods and services, it remains unclear whether "digital products, including cryptographic products", receive the same protection as non-digital products under the WTO agreements. Furthermore, there have been no clarifications from the Dispute Settlement Body (DSB) regarding the regulation and protection of cryptographic products under the WTO Agreements. With the increasing delivery of products in digital formats, concerns about the equitable treatment of "cryptographic products" are gaining prominence.

Consequently, the concept of non-discrimination is primarily being developed through Regional Trade Agreements (RTAs) to address the deficiencies of the WTO Agreements. However, it's important to note that RTAs typically reference the principles established under the WTO agreements in their application.

3. Regional Agreements related to Cryptographic Products

Regional Trade Agreements (RTAs) have a significant impact on the trade and regulation of cryptographic products within specific regions. They promote economic integration and reduce trade barriers among member states, encouraging standardization of technical protocols, lowering tariffs, and enhancing market access (Rahman & Rahman, 2022). RTAs also influence intellectual property rights and data protection rules for encryption technologies. They foster security cooperation and competition, driving innovation in cryptographic products. However, the exact impact depends on agreement terms,

industries, and local regulations, requiring vigilant monitoring for businesses in the sector to adapt to evolving compliance requirements.

These are bilateral or multilateral trade agreements based on mutual preferences, authorized by the WTO. The GATT, as per Article XXIV:5, permits the establishment of customs unions, free trade areas, or agreements among the territories of participating parties (Dam, 1963). Similarly, under Article V:1 of the GATS, members are allowed to engage in agreements that promote trade liberalization. The following Regional Trade Agreements have particular stipulations for ICT products incorporating encryption.

3.1. The United States – Mexico – Canada Agreement (USMCA)

The United States-Mexico-Canada Agreement (USMCA) has significant implications for cryptographic products in North America. It addresses intellectual property rights, data localization, and digital trade, impacting the development and regulation of cryptographic technologies. USMCA promotes regulatory cooperation and market access, benefiting cryptographic businesses and consumers[5]. Additionally, it emphasizes cybersecurity cooperation, underlining the importance of cryptographic products in ensuring data security and privacy. Companies in the cryptographic sector should monitor how the agreement's provisions affect their operations and compliance in the region.

The North American Free Trade Agreement (NAFTA), which had been operational since January 1994, was succeeded by the United States-Mexico-Canada Agreement (USMCA). The USMCA was a trade accord collectively approved by the three countries on November 30, 2018, and it came into force on July 1, 2020. This agreement is seen as a mutually advantageous outcome for North American workers, farmers, ranchers, and businesses (van der Linden & Shirazi, 2023).

3.2. Japan – UK Comprehensive Economic Partnership Agreement (Japan – UK EPA)

The Japan-UK Comprehensive Economic Partnership Agreement (Japan-UK EPA) primarily focuses on trade and economics but has implications for cryptographic products. It improves market access by reducing trade barriers, addresses intellectual property rights, encourages regulatory cooperation, and influences data privacy and cybersecurity collaboration (Riebe et al., 2022). E-commerce and digital trade considerations also affect the digital market for cryptographic products. Businesses

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

in this sector should stay informed about the agreement's provisions for compliance and market opportunities.

The Japan-UK Economic Partnership Agreement (EPA) is a free trade agreement inked in Tokyo in October 2020. This accord aims to promote trade and investment liberalization, foster a stronger economic relationship between the participating parties, and include elements from the WTO Agreements. Notably, Article 1.9 of the Japan-UK EPA prohibits any actions by the parties that contradict their obligations under the WTO Agreements. The agreement also contains provisions concerning commercial ICT products incorporating cryptography.

National treatment in trade agreements like the Japan-UK EPA and USMCA is crucial for cryptographic products. It ensures equal treatment for domestic and foreign cryptographic items, fostering fair competition and market access. Japan – UK EPA and USMCA both uphold this principle, eliminating discrimination based on product origin (Burri, 2021). This is vital for the sensitive nature of cryptographic technologies, promoting innovation and cybersecurity. Businesses in this sector must closely follow agreement regulations to ensure compliance and equal access to markets.

The agreement does not explicitly detail the national treatment of cryptographic products. Nevertheless, in Articles 2.7 of the Japan – UK EPA and 2.3 of the USMCA agreement, each party is obliged to provide national treatment to the goods of the other party, as outlined in Article III of the GATT (Burri, 2023). Additionally, the agreements include the incorporation of Article III and Article XX of the GATT, making these provisions a part of the agreements. Consequently, the safeguarding of cryptographic products is ensured through these specific Articles.

4. The Issue of the Access to Cryptographic Products

Access to cryptographic products is vital for data security and privacy. These products use complex algorithms to protect information from cyber threats and ensure data integrity. They are essential for safeguarding personal data, national security, and secure online transactions[6]. However, global regulations can impact access, and balancing security with access is a challenge. International cooperation is key for cross-border data protection, and cryptographic products come in various forms. Promoting awareness and proper usage is crucial. Thus, cryptographic product access is essential for data, privacy, and security in an evolving regulatory landscape.

Accessing cryptographic products entails either transferring or gaining access to a private key or other confidential parameters, the specifics of the algorithm, or design details, by a party or a person within that party's jurisdiction (such as manufacturers

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

or suppliers)[7]. The World Trade Organization (WTO) Agreements do not explicitly address the issue of accessing cryptographic products. However, both the United States – Mexico – Canada Agreement (USMCA) and the Japan – UK Economic Partnership Agreement (EPA) impose restrictions on their members, compelling manufacturers and suppliers of cryptographic products to transfer or provide access to proprietary information related to cryptography. The USMCA places stringent limitations on all cryptographic goods, while the Japan – UK EPA restricts access to commercial information and communication technology (ICT) products that utilize cryptography, including software. The rationale behind implementing these restrictions on accessing cryptographic products is to establish trust within the business relationships among the agreement's members and to adhere to the provisions of Article 10(1) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which ensures the protection of intellectual property rights for manufacturers[8]. In contrast, the Organization for Economic Cooperation and Development (OECD) Guidelines for Cryptography Policy offer an alternative approach to accessing cryptographic products. National cryptography policies may allow lawful access to plaintext or cryptographic keys for encrypted data, but such policies must also respect the other principles outlined in the guidelines. Members have the discretion to enact laws regarding access to cryptographic products, but these measures can potentially be misused.

It is important to note that, under Article 2.2 of the Technical Barriers to Trade (TBT) Agreement, WTO Members are permitted to establish technical specifications for products incorporating cryptography technology as long as these specifications do not create trade barriers that are more restrictive than necessary to achieve a legitimate objective. One question that arises is whether permitting lawful access to cryptographic products may constitute a violation of business trust and intellectual property rights.

Conclusion

In conclusion, cryptography, once an ancient art of encoding and decoding, has grown to become an indispensable cornerstone of the digital age. It plays a vital role in securing communication, data protection, and ensuring the confidentiality, integrity, and authenticity of information. From secure messaging apps to blockchain security, the applications of cryptographic technology are diverse and widespread, underpinning the modern digital landscape.The integration of cryptographic technology into international trade, particularly in the realm of information and communication technology (ICT) products, raises complex regulatory challenges. While World Trade Organization (WTO) agreements do not explicitly address cryptography, they indirectly impact cryptographic products by encouraging

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

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

transparent and necessary regulations that serve legitimate objectives like security and intellectual property rights protection. The Agreement on Technical Barriers to Trade (TBT) promotes preventing technical regulations from obstructing international trade, while the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement indirectly safeguards intellectual property rights related to cryptographic technology, thus fostering innovation and trade in ICT products relying on cryptography.

The issue of non-discriminatory treatment of cryptographic products remains a significant concern, and Regional Trade Agreements (RTAs) like the United States – Mexico – Canada Agreement (USMCA) and the Japan – UK Comprehensive Economic Partnership Agreement (Japan – UK EPA) have come to address these concerns by offering a framework for the treatment of cryptographic products. The complex and evolving regulatory framework for cryptographic products underscores the need for international agreements to adapt to the changing landscape of the global cryptographic market. Balancing the protection of innovations with the promotion of trust and cooperation is essential in shaping the future of international trade in cryptographic products. Furthermore, the ongoing debate surrounding the use of export and import restrictions to hinder encryption technology highlights the significance of this issue on a global scale.

Therefore, as the world becomes increasingly interconnected and reliant on cryptographic technology, international agreements, national regulations, and regional trade pacts will continue to play pivotal roles in shaping the trajectory of cryptographic product policies, ensuring both innovation and security in the digital age.

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

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

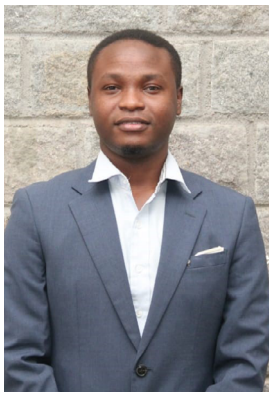
Torrubia, A., Mora, F. J., & Marti, L. (2001). Cryptography Regulations for E-commerce and Digital Rights Management. *Computers & Security*, *20*(8), 724–738. https://doi.org/10.1016/s0167-4048(01)00814-8

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

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

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

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

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

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, Вишвавидьянилайа 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

Магоге 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.