ISSN 2949-2483

Volume 2 Number 2

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2024

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 2, No. 2
2024
DOI: 10.21202/2949-2483.2024.2
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483
Published since 2023, frequency – 4 issues a year. DOI: 10.21202/2949-2483

Address: 42 Moskovskaya Str., 420111 Kazan, Russian Federation
Tel.: +7 (843) 231-92-90
Fax: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Website: https://www.lawjournal.digital
Telegram: https://t.me/JournalDTL_world
VKontakte: https://vk.com/JournalDTL
Yandex.Dzen: https://dzen.ru/JournalDTL
Odnoklassniki: https://ok.ru/JournalDTL

Founder and publisher of the Journal

Kazan Innovative University named after V. G. Timiryasov. Address: 42 Moskovskaya Str., 420111 Kazan, Republic of Tatarstan, Russian Federation. Tel.: +7 (843) 231-92-90. Fax: +7 (843) 292-61-59. E-mail: info@ieml.ru. Website: https://ieml.ru

Certificate on registering a mass medium: EL no. FS 77-84090 of 21.10.2022, issued by Roskomnadzor.
Territory of distribution: Russian Federation, foreign countries.

Date of signing the issue for publication: 2024, June 25. Hosted on the website https://www.lawjournal.digital: 2024, June 30.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 2, No. 2
2024
DOI: 10.21202/2949-2483.2024.2
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Editorial
UDC 34:004
EDN: https://elibrary.ru/bpdcht
DOI: https://doi.org/10.21202/jdtl.2024.13

Contemporary Foreign Legal thought on the New Phenomena of Digital Transformation

Ildar R. Begishev
Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia

Anna K. Zharova
National Research University «Higher School of Economics», Moscow, Russia

Elizaveta A. Gromova
South Ural State University (national research university), Chelyabinsk, Russia

Maksim V. Zaloilo
Institute of Legislation and Comparative Law under the Government of the Russia, Moscow, Russia

Irina A. Filipova
National Research Lobachevsky State University of Nizhny Novgorod, Nizhniy Novgorod, Russia

Albina A. Shutova
Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia

Just recently it seemed ephemeral that legal scholars and practitioners around the world would be directly involved in digitalization processes. It seemed hard to imagine that in a short period of time, the rapid leap in technology development would begin to change virtually all areas (including legal activities), making digitalization so comprehensive that it would be perceived as commonplace. One could not suppose that the increasing importance of digital competencies on the labor market would be natural; however, they have become essential for effective use and work with digital technologies. Today, we have to revise the competence-based approach to educating and training qualified lawyers and improving their qualifications, taking into account the digital economy trends that form a new regulatory environment for relations. Such concepts as “digital rights”, “digital maturity”, “technological sovereignty” and many others are deeply embedded into the legal lexicon. Lawyers, together with experts from other branches of knowledge, act in the coordinates of digital transformation, the criteria of which

are yet to be defined, given that law is the main factor in the pace of technologization and digitalization of social relations.

In their work, lawyers are inevitably confronted with new phenomena generated by digitalization. The attitude to the latter has divided the legal world, with a certain degree of conventionality, into two groups. Some perceive it as a good thing that ensures scientific and technological progress and entails new opportunities for humanity, society and state. Others are wary of it, foreseeing the emergence of previously unknown risks, challenges, and threats to humanity, including existential ones. But no matter how we regard digitalization and its phenomena, we can say for sure that it has become a global megatrend setting new research paradigms. It unites those scholars and practitioners from different parts of the world who seek to share their experience and vision of solutions to the emerging problems, both applied and theoretical, caused by digitalization, and to contribute to the development of legal practice, science, and technology. This can be seen from the content of the Journal of Digital Technologies and Law, which has expanded the geography of the authors whose research were presented in the first issue of 2024.

Having set the bar high in 2023, the Journal continues to develop international cooperation not only by working with its ambassadors, who are renowned experts in the field of law and technology and represent the Journal in different countries of the world, but also by publishing new and noteworthy research from different countries. In this sense, the current issue focuses on reflecting the various strands of foreign legal thought influenced by digitalization. The first issue of 2024 presents the works of scholars from Australia, China, Egypt, France, India, Mali, Morocco, Nigeria, Philippines, Portugal, Spain, Tanzania, and Uganda.

This issue of Journal of Digital Technologies and Law contains scientific research of foreign legal science, which reflects on country, regional and international aspects of the convergence of law and technology, the possibilities and effectiveness of combining the internal (national) law of states and the international legal instruments. It also touches upon transformation of classical concepts, doctrines, and legal institutions in the modern conditions of digitalization. It reveals the legal and technological components of new phenomena generated by digital transformation, such as cyberspace, cyber sovereignty, sharenting, lootboxes and others, as well as the consequences of the digital transformation of law, legal problems and prospects of digitalization.

The issue opens with the article “Demarcation of cyberspace: political and legal effects of applying the concept of sovereign states’ interests” (**Yassin Abdalla Abdelkarim (Egypt)**). The study analyzes various aspects of adapting the traditional legal concept of sovereignty to current realities. It emphasizes the need to rethink this concept in cyberspace, taking into account the security requirements and the need for a disciplinary determinant of cyber sovereignty. The author shows the application of traditional and modern legal concepts of sovereignty in the new digital environment and reveals the functional significance of the concept of state cyber interests for demarcating cyberspace and defining the boundaries of national sovereignty.

Problems of sovereignty, cybersecurity risks, approaches to regulation and improving the efficiency of data management in different jurisdictions were shown in the article "Legal issues of cross-border data transfer in the era of digital government" (**Gulbakyt Bolatbekkyzy (China)**). The paper suggests that the issues of sovereignty and information localization are among the most complex in the field of transboundary data transfer and in forming transboundary trust space. The latter is recognized as an important stimulus for the development of national digital ecosystems and data exchange formats (G2G, G2C, G2B, B2B, and B2C). At the same time, it is important to strike a balance between data availability, on the one hand, and data security, on the other.

It should be noted that global data flows have already become a factor determining the sustainable development of modern international trade. The obstacles arising on this path, which hinder cross-border data transfer, often entail delays and higher prices for goods and services. The study "Using smart contracts in international commerce and prospects of further evolution of Incoterms" (**Prince FaterAudu (Nigeria), Shabih Fatima (India)**) is devoted to analyzing the prospects of international trade contracts in the light of technological innovations in trade law. It analyzes the international commercial terms governing transactions between importers and exporters and concludes that their synchronization with smart contracts can have a positive impact on the prospects for international trade and especially on export-import contracts.

In the context of international trade, the security of online transactions and cross-border payments becomes increasingly important. New technologies such as smart contracts and blockchain were supposed to increase the security of communication and cross-border information exchange. Cryptographic technologies can also solve this problem by information encoding and decoding. However, the integration of the latter into international trade, namely in the area of information and communication technology products, has raised complex regulatory issues. The issue pays special attention to the specifics of legal regulation of international trade in cryptographic products and technologies according to the World Trade Organization and regional trading agreements (**Sayed Qudrat Hashimy (India), Jackson Simango Magoge (Tanzania)**). The paper reveals the complex legal landscape being reshaped by the digital imperative to integrate cryptographic technologies into international trade.

Online transactions are becoming widespread not only at the international, cross-border level, but also in massive multiplayer online games, where virtual goods are purchased in in-game stores. The development of business models in this sphere has followed the path of such microtransactions: one may purchase the whole game or individual items in it. A new revenue model appeared, based on selling in-game (virtual) items. This phenomenon, called lootboxes, has rapidly gained momentum and globalized, which has become a legal problem in some jurisdictions. In this regard, a comparative study of legal regulation of lootboxes in different countries is of interest (**Seppy Pour (Australia)**).

Another article in this issue demonstrates the effectiveness of electronic payments as a means of transaction, but also highlights a number of legal problems that may hinder their seamless use (**Ismaila Ozovehe Haruna (Nigeria), Paul Atagamen Aidonoji (Uganda), Onivehu Julius Beida (Nigeria)**). A wide range of issues related to the work of electronic payment systems is revealed by the example of an African state with most promising prospects – Nigeria. Nigerian authorities have already taken certain steps to address the problems identified, but the authors note the insufficiency of these measures to effectively regulate the electronic payment system in the country.

Another new phenomenon considered to be a result of digitalization is sharenting. To be more precise, it is related to the spread of social networks and the Internet activity of children and their parents. It consists in posting information about minors (especially their photos and videos) on social networks, jeopardizing the fundamental rights of minors, their privacy, and generating social and legal conflicts. This issue contains a study devoted to these problems (**Francisco José Aranda Serna (Spain)**). Having analyzed the key provisions of Spanish, French and US legislations, the author determines the social and legal nature of sharenting and its legal consequences.

The article "Measures to prevent the violation of the rights of content creators in digital environment: case study of Nigeria" (**Adetutu Deborah Aina-Pelemo, Ithamar Bassey, Glorious Okeoghene Akpojaro (Nigeria)**) is devoted to determining the level of protection of the rights of content creators in social networks and to developing measures to prevent offenses in this area. By the example of the Nigerian experience, the authors examine the rights and protections provided to digital content creators under intellectual property law.

The digital format can also be used in the interests of standardization, as well as to simplify the formulation of many documents. One of the articles in this issue (**Dominique T. Molintas (Philippines-Australia)**) attempts to synthesize the main provisions of public-private partnership agreements into a general matrix that can serve as a tool for drafting such agreements, taking into account the specifics of legislation and other circumstances.

In recent years, artificial intelligence has been in the center of attention both in science and practice. This topic is also reflected in this issue (**Hamza Jabir (Morocco), Kamal Lagtati (Morocco), Denis Pohe-Tokpa (France)**). Using analytical and comparative methods, the authors identify the challenges and analyze the possibilities of ethical and legal regulation of artificial intelligence based on the experience of digital transformations in Morocco.

The issue concludes with a brief analytical excursion into anthroposociogenesis, presenting the evolution of humanity, various social institutions, and an understanding of the existential role of laws aimed at ensuring that societies live together in the context of technological innovation (**DjénébaTraoré, Mali – Cabo Verde**)).

The presented studies show that digital transformation is associated with the problem of uneven development of digital technologies in different countries. This problem is not new, it is recognized in research in different ways, as the problem of the digital divide, digital gap, digital inequality. At the same time, its relevance remains and is in the focus of attention of foreign doctrine.

We hope that this issue of the Journal of Digital Technologies and Law will be of interest to a wide range of readers and the articles will serve as an example for those potential authors who are ready and willing to demonstrate their promising scientific results and developments in the field of innovation and law on the pages of our journal.

In this year, the Journal of Digital Technologies and Law was approved for indexing in **HeinOnline**, the world's largest database of legal research and legal periodicals. This further emphasizes that our journal meets the accepted publishing standards. We make efforts to ensure transparency and reproducibility of research results.

The demand for scientific search and new results in this field is confirmed by the high interest in the Journal of Digital Technologies and Law and the articles published in it, which cover the problems of digital technologies and law (Fig. 1).

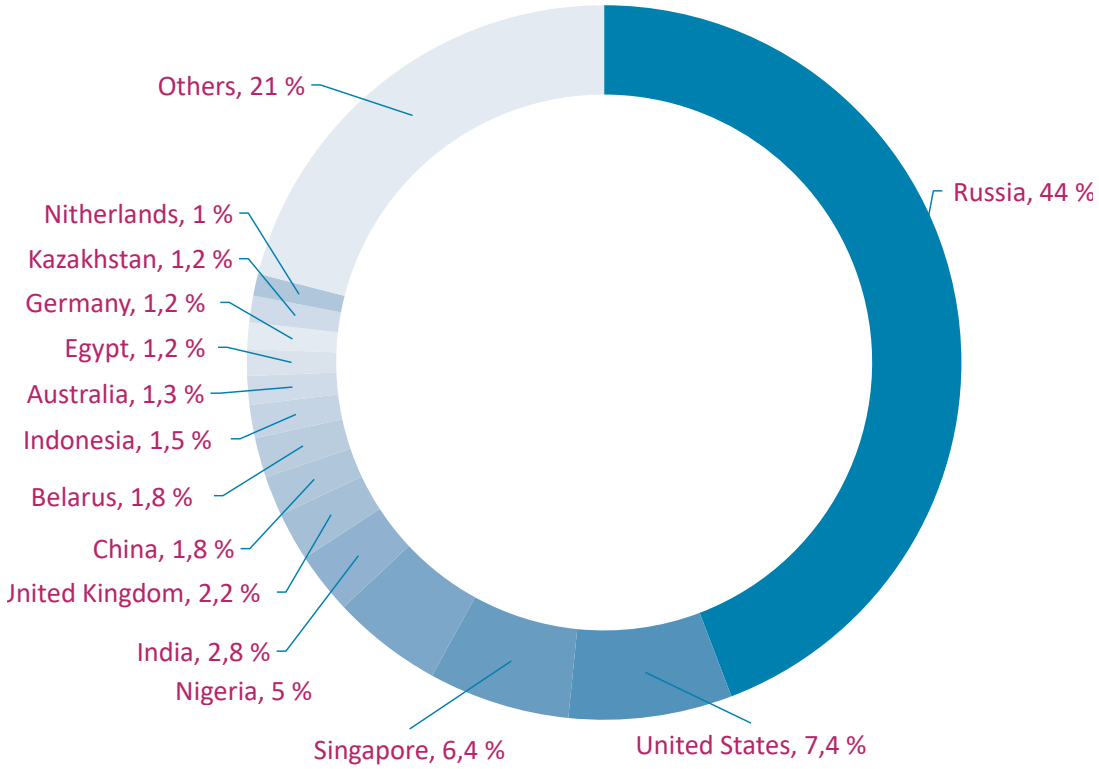


Fig. 1. Traffic statistics of the Journal of Digital Technologies and Law website (as of June 30, 2024)

In order to further shape an international dialog, we are open for cooperation with leading and young researchers both from Russia and from abroad, as well as experts and practicing lawyers, to publish their ideas on improving the existing and developing new approaches to the problems of legal regulation and protection of social relations in the sphere of digital technologies.

We would like to thank the authors, reviewers, editorial staff, journal ambassadors, editorial board members and readers for their cooperation and growing interest in our periodical.

Research article
UDC 34:004:342.3:004.9
EDN: https://elibrary.ru/sywsrk
DOI: https://doi.org/10.21202/jdtl.2024.14

Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests

Yassin Abdalla Abdelkarim
Luxor Elementary Court, Sohag, Egypt

Keywords

border,
cyber interest,
cyber security,
cyber sovereignty,
cyberspace,
digital technologies,
law,
national interest,
sovereignty,
state

Abstract

Objective: to substantiate the existence of national cyber sovereignty as a legal concept; by introducing the concept of state cyber interests as an innovative determinant, to review the traditional concepts of national sovereignty and state borders in the context of the dynamic nature of cyberspace and the need to develop a hybrid mechanism for cyber borders protection, based simultaneously on law and technology.

Methods: the doctrinal method was used to identify the basic discrepancies in the views of leading scientists in different fields on fundamental theoretical-methodological, conceptual and categorical issues, including the justification of a single algorithm for establishing borders in cyberspace. The doctrinal method is supplemented by the analysis of judicial practice of different countries, which allows considering the courts extending their jurisdiction to disputes related to cyberspace.

Results: the study presents the application of traditional and modern legal concepts of sovereignty in the new digital environment, resulting in a combination of legal and technological approaches. The author reveals functional significance of the concept of state cyber interests for demarcating cyberspace and defining the boundaries of national sovereignty. The adaptability of this concept to the technically uncertain nature of cyberspace is shown. The conclusion is made about the main directions in forming the concept of cyber interests in cyberspace and its political and legal implications, based, among other things, on the practice of courts of different countries in resolving cyber disputes.

Scientific novelty: the concept of state cyber interests is considered as an innovative method of defining cyber borders. It leads to the transformation of the traditional sovereignty concept and the close national interest concept in relation to cyberspace in the context of fulfilling security requirements and intensifying national defense against cyber threats.

Practical significance: the obtained results eliminate existing contradictions in the definition of sovereignty and its spatial limits under the modern technology development; contribute to the elaboration of a disciplinary standard of cyber sovereignty based on a reliable demarcator necessary for the definition of state sovereignty and borders in cyberspace; adapt traditional legal concepts of sovereignty and national interests to the global modern cyber challenges; contribute to the transformation of traditional legal concepts of sovereignty and national interests in cyberspace.

For citation

Abdelkarim, Y. A. (2024). Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests. *Journal of Digital Technologies and Law, 2*(2), 262–285. https://doi.org/10.21202/jdtl.2024.14

Contents

Introduction

The inauguration of the Internet has opened an ultimate unbounded sphere of interactions which extends universally. Nowadays, cyberspace connects each corner of Earth. This permits cosmopolitan multi-directional streams of data among nations that transfer a diversity of information, constituting international human cyber interactions.

The borderless theme of cyberspace challenged traditional legal norms of sovereignty and borders, which are indispensable to imposing state control over national territory to deter extraterritorial harm caused by countless foreign illegal cyber activities. Thus, security requirements implied reconceptualizing those notions in cyberspace to activate a national shield against cyber threats. As a response, scholars competed to elaborate on these concepts in cyberspace. They sought to imagine a clear portrait of them and develop firm standards to determine their manifestation in cyberspace. Nevertheless, the absence of a unified methodology created contradicting portraits of sovereignty and borders in cyberspace according to the scope of each scholar. Consequently, they differed in presenting the required determinant.

Henceforth, the research allocates this practical gap and tries to bridge it by introducing a new determinant of sovereignty and borders concepts in cyberspace. This determinant is the concept of state cyber interest. The research points out that national interests in cyberspace are the chief motivation for state intervention. State interests are the true presentation of nationalism in cyberspace; they drive states to act to safeguard their sovereign interests.

To achieve the research objective, it reviews relevant literature on sovereignty and borders in cyberspace to prove their integral coherence and their tight link to the idea of nationalism. Then, it sheds light on the absence of a disciplined demarcation standard in cyberspace, which is the practical gap in knowledge that the research seeks to bridge. Afterwards, it explains the concept of state interest and previews its implications and how domestic courts utilise it to settle cyber disputes. At last, the research proves the functionality of the state cyber interest concept to assign borders in cyberspace through legal reasoning and providing a practical framework.

1. Sovereignty and Borders in Cyberspace: Integral Coherence

As a legal political notion, sovereignty has been a controversial concept that jurists and politicians have elaborated on since the 16th century. It is a crucial organizer of inter-state relations and the entire global motion of human interactions. Prominent Western scholars like Bodin[1] and Hobbes[2] portrayed sovereignty as the king's ultimate authority

[1] Jean Bodin (1530–1596), a French politician and Philosopher.

[2] Thomas Hobbes (1588–1679), English philosopher, scientist, and historian.

to make decisions within a nation[3] According to their view, sovereignty is a political determinant of state power over a bordered territory; a limitation of national power that imposes a de facto obligation of mutual respect of national sovereignty among states. This political notion evolved into a social contract according to Rousseau[4]. Afterwards, philosophers and jurists developed sovereignty theories. Regardless of the various explanations of sovereignty, it remains a core determinant of state authority over its territory according to the Westphalian doctrine, sovereignty refers to the supreme power of a state within a territory (McLean & McMillan, 2009). This concept is the traditional definition of sovereignty in legal and political sciences that suits the nature of inter-state interactions in the real world. Thus, states adopt traditional demarcation methods to draw the national borders among them that regulate their powers and interactions.

Nevertheless, the emergence of cyberspace as a modern sphere of human relationships and interactions implied stretching the traditional notions into its cyber activities. This fact demanded that jurists and scholars rethink their attitudes toward the existing notions and theories to fit cyberspace. Therefore, the concept of sovereignty began to crystallize in cyberspace to organize state power and track illegal activities. Because of the glaring differences between cyberspace and the real world, academics and legislators exert tremendous endeavours to reshape sovereignty under the dynamic nature of cyberspace. The reshaping process proved the uselessness of the traditional border demarcation methods due to the distinguishing nature of cyberspace. The latter implies the development of a specific appropriate tool to draw cyber borders that determine states sovereignty.

In this section, the study explores the evolution of the literature on the concepts of cyber sovereignty and cyber borders to grasp the scholarly efforts of reshaping sovereignty. Then it reviews the social and political perspectives of cyber sovereignty to determine its impacts on national politics and domestic social policies, shedding light, in particular, on the legislative aspect. Last, the study analyzes the demarcation process in the real world and cyberspace to disclose the vacuum in determining state sovereignty in cyberspace.

1.1. Evolution of Borders and Sovereignty in Cyberspace

In 1983, the official open worldwide communication sphere “the Internet” was introduced to humanity (University System of Georgia Online Library) thanks to the invention of the Transfer Control Protocol/Internetwork Protocol (TCP/IP). Since then, massive amounts of data have been transferred globally among Internet users, who

[3] Sovereignty. (2024, Mar. 12). Encyclopedia Britannica. https://clck.ru/3A7Ttf

[4] Jean-Jacques Rousseau (1712–1778), a French Philosopher.

were individuals, entities, and governments. The development in data exchange drove scholars to analyze the newly invented sphere of interactions to conclude its features.

Choucri and Clark pointed out that the absence of sovereignty in cyberspace is not imagined (Choucri & Clark, 2013); traditional sovereignty extends to cyberspace but in a form that suits the borderless nature of this sphere. They mean that sovereignty should be contextualised according to the technical nature of cyberspace. This solution manifests an attempt to integrate a legal notion into a technical context to overcome the legal vagueness of cyberspace.

Scholars continued to develop a clear understanding of cyber sovereignty by creating a discipline determinant of this concept. Therefore, they focused on explaining and clarifying how borders are manifested in cyberspace. Borders are the logical corollary for sovereignty because they constitute its boundaries. Sovereignty and borders are twin concepts; to determine sovereignty borders should be disciplined and allocated. This logic stretches to cyberspace as the accurate interpretation of sovereignty requires developing a disciplined determinant of borders in cyberspace.

Henceforth, scholars sought to innovate a technical determinant of national borders in cyberspace. These borders share the same features and functions as traditional borders since they enable states to impose their sovereignty in cyberspace. Accordingly, Osborn defined cyber borders as the "Functional Equivalent of the Border, where the data arrives at the first practical point of inspection — a network router, computer server, PC, or other networked devices" (Osborn, 2017). His definition is based on the explanations of data exchange models provided in his research. As a consequence, state authorities, e.g., customs officials, can observe data flow in cyberspace to track illegal merchandise or to impose taxes on other legally traded cyber materials. The prominence of Osborn's definition is caused by his bias toward a purely technical approach in explaining a legal notion, that suits the nature of cyberspace. He considered that state cyber sovereignty extends to the first point where data flow interacts with state interests. Likewise, Fang prioritized the technical aspect when defining cyber sovereignty by stating "Cyberspace sovereignty of a state is based on the ICT (Information and communications technology) systems under the state's own jurisdiction; the boundaries thereof consist of a collection of the state's own network device ports directly connected to the network devices of other states; cyberspace sovereignty is exercised for protection of various operations of data by cyber roles" (Fang, 2018). He drew the state cyber territory according to its national network of devices. Therefore, the network map is the state territory in cyberspace. Furthermore, he mentioned that cyber sovereignty grants the state the same powers over its territory granted by traditional sovereignty, e.g., self-defence and independence (Fang, 2018). Fang's definition is a successful mixture of law and technology because it established state territory in cyberspace on the technical map of national network devices and mentioned state rights granted by this legal concept.

In this regard, the Egyptian Public Prosecution adopted a functional approach concerning the admittance of cyber borders. An official statement noted that the state has virtual borders in cyberspace; they manifest the fourth political state boundaries[5]. Thus, surveilling this sphere of interactions constitutes a state interest of utmost importance. Despite the statement devoid of a definition of cyber borders, it admitted their existence and functions.

The Internet occupation of modern-day life intensifies human relations and interactions in cyberspace. The ongoing developments of cyberspace communication techniques challenge states power to impose order on the Internet. These developments motivated modern scholars to sharpen their lens on the legal issues that arise from cyber interactions. Among these issues, the questions of state sovereignty and its national authority over cyber territory have occupied a considerable position in scholars' debate. In addition, jurisprudence developed several tools to assign political borders in cyberspace.

Cyber sovereignty should not be limited to the physical perspective of network devices (Omar et al., 2022). The absence of traditional borders in cyberspace implied conceptualizing sovereignty to adapt to the technical unbounded nature of cyberspace. Therefore, Omar et al. introduced the term "Universal Information Sovereignty" to express the state authority to conduct cyber security operations to defend its national interests in virtual reality (Omar et al., 2022). They argued that determining the limits of state cyber sovereignty is a political process rather than legal because each state has its own evaluation of data flow and its effects on national interests (Omar et al., 2022). They shed light on the practical aspect of cyber sovereignty by figuring out its direct nexus to cyber security. Sovereignty is the legitimization of cyber security operations. Thus, it is an ultimate manifestation of state interests in cyberspace.

Zekos noted that the global nature of the Internet transferred the practice of sovereignty from states to market forces because this nature replaces the traditional interpretation of state sovereignty with a globalized market power that accords the capitalist control of cyberspace (Zekos, 2022). Due to the ongoing economic benefits of globalized cyberspace, states suffer hardships regarding securing their traditional sovereignty (Zekos, 2022). Therefore, cyber globalization created the concept of cyber sovereignty; it is an adaptation of the traditional legal notion of sovereignty in cyberspace (Zekos, 2022). Cyber sovereignty, hence, suits the boundlessness of the cyber sphere, where traditional territorial boundaries disappear entirely. Nonetheless, he claimed that state sovereignty, in its legal concept, has a strong nexus to its territory as this notion permits the state to impose its authority within the national borders (Zekos, 2022). Accordingly, he

[5] The Egyptian Public Prosecution. (2020). Official Statement on Hanin Hossam's Case. https://clck.ru/39rfJM

stipulates the existence of a recognized state territory in cyberspace to establish its sovereignty over it. With the absence of traditional territorial boundaries, he suggested applying advanced geographical digital tracking of data flow on the Internet to ensure state sovereignty (Zekos, 2022). Furthermore, he concluded that states should adopt the effect factor to recognize their territory in cyberspace (Zekos, 2022); each activity that generates effects within the traditional territory extends state sovereignty over it. Under this interpretation, domestic courts managed to establish personal jurisdiction over cyber disputes. The nexus between the cyber society and the state justifies stretching national sovereignty to cyberspace, disregarding the distinguishing cyber dimensional expression (Zekos, 2022). Consequently, states can impose their sovereignty over electronic transactions and interactions that affect their interests. This elaboration proves the existence of cyber sovereignty as a legal notion.

According to Simmons and Hulvey, imposing cyber borders implies paving the road for domestic laws to organize and control data flows between national cyber spatial and universal cyberspace (Simmons & Hulvey, 2023). Henceforth, cyber borders reflect the governments' endeavours to control national cyberspace against foreign interference (Simmons & Hulvey, 2023). Thus, borders and sovereignty are two sides of a single coin in cyberspace, which is national security.

Respecting cyber sovereignty is a chief principle concerning cyber operations. It is an extension of traditional sovereignty which constitutes a threshold of peaceful global cyber cohabitation (Japaridze, 2023). Cyber sovereignty provides states with the authority to surveil and track illegal activities on the Internet and to take the appropriate countermeasures to maintain their national integrity in the virtual world (Japaridze, 2023). Thus, cyber sovereignty contributes to protecting individuals against cyber threats. However, the extremist interpretation of cyber sovereignty might Balkanize cyberspace to tiny distant islands (Japaridze, 2023), which contradicts the original purpose of this global sphere. Hence, sovereignty, as a determinant of state authority, is indispensable in cyberspace to organize global interactions.

It is worth mentioning that Zein defined cyber sovereignty as "the submission of cyberspace to state interests and values" (Zein, 2022). This definition implies the state ultimate authority to control and surveil cyberspace and reflects the obvious nexus between sovereignty in cyberspace and state authority. It also includes the exerted efforts to demarcate cyberspace. She argued that cyberspace is a de facto "universal common" similar to international high seas and human cultural heritage (Zein, 2022). Therefore, it is challenging to impose certain state sovereignty over it. Nevertheless, states might crystalize their national cyber sovereignty by imposing technical measures to limit data flow, observe suspicious activities, and exploit the vagueness of cyberspace against other states (Zein, 2022). Furthermore, the legal consequences of traditional sovereignty

extend to cyber sovereignty because states should consider mutual respect for national sovereignty while operating in cyberspace, avoiding unlawful interference in the internal affairs of other countries, and maintaining the integrity of territorial cyber sovereignty against illegal cyber attacks that target critical infrastructure (Zein, 2022). It should be noted that Zein highlighted that cyber sovereignty has a strong nexus to state security and well-being. The political perspective overwhelms her elaboration on stretching sovereignty, in its traditional legal interpretation, to the newly innovated cyberspace. In this context, Zhuk argued that sovereignty in cyberspace is purely virtual and implies imposing state control over its digital infrastructure located within the national virtual territory (Zhuk, 2023). It is an exclusive feature of online communities that has no ties with traditional physical territory.

To sum up, since sovereignty legitimizes state actions to defend national interests, scholars spared no effort to elaborate on how this concept is manifested in cyberspace. While old scholars debated its existence, modern literature discloses the global admittance of cyber sovereignty. This acceptance is evident in the scholarly endeavours to interpret this notion within the technical context of cyberspace. It is crucial to note that scholars managed to highlight the functional aspects of cyber sovereignty when explaining it; their definitions reflected that sovereignty is the method that legitimizes state practices in cyberspace to present its national interests. Furthermore, the absence of a clear determinant of sovereignty might trigger a global cyber conflict because of inter-state authority overlapping. This consequence threatens the stability required by the flourishment of universal interactions in cyberspace. Therefore, the development of a discipline determinant of cyber sovereignty is a must to evade dire consequences.

1.2. Cyber Sovereignty Tight Nexus to Nationalism

Nationalism has become the chief determinant of state perceptions of spaces since its evolution in the 18th century. States managed to control their spaces on the basis of national interests. Koulos argued that countries, to exercise their powers within a specific territory, initiate a nationalization process of it (Koulos, 2022). According to Cox, nationalism is "the sum of those beliefs, idioms, and practices, oriented to a territorially delineated nation and embodied in the political demands of a self-identified people, which may or may not be realized in a nationalist movement and state 'of their own'" (Cox, 2021). From this definition, it could be understood that nationalism had been limited to traditional territorial spaces for a while. Nonetheless, the emergence of the Internet eliminated the traditional boundaries between nations and permitted transnational interactions. Therefore, nationalism evolved to conquer cyberspace as states inaugurated plans for the nationalization of cyberspace. In this aspect, the research explores the strong links

between sovereignty and nationalism in cyberspace as a threshold to prove the need to demarcate states cyber sovereignty and find a determinant of states cyber borders. Moreover, it sheds light on certain states regulations of cyber security to reveal the national attitudes toward cyberspace demarcation.

The sense of nationalism does not suppress its application to the real world; on the Internet, several interactions are motivated by nationalism. The unlimited universal nature of cyberspace created several fields of digital rivalry. The controlling factor of this rivalry is nationalism. Therefore, despite its ambiguous nature, states sought to incorporate cyberspace into their national concepts (Koulos, 2023). Put differently, national regimes would try subordinating cyberspace to their political ambitions. For instance, the URL terminus usually refers to the state where the domain owner is located, e.g., .fr for France, .us for the United States, and .eg for Egypt. Koulos brought this instance as preliminary evidence of cyberspace nationalization. The global theme of cyberspace evolved a cosmopolitan understanding of nationalism because of the reshaping of values (Cox, 2021). Globalization aroused national political ambitions for domination in cyberspace. Henceforth, Cox indicated that a borderless sphere ignites fevered inter-state competition under the flag of nationalism (Cox, 2021). Furthermore, borders in cyberspace are shaped to protect sovereignty over national soil. Nonetheless, states utilize appropriate techniques to impose national cyber borders. These mechanisms suit the specific technical vague nature of cyberspace, distinguishing them from the traditional border demarcation methods. The intensive globalization of cyberspace drives states to concentrate on its territorialization to safeguard their national interests against political tensions[6]. Nationalism is the main justification for their policies.

Since cyberspace is a rich well of data, superpowers seek to impose their control on it under the notion of cyber sovereignty[7]. Therefore, states utilize specific technologies to strengthen their grasp on the national cyber territory. They impose national sovereignty in cyberspace through data observance and capture mechanisms to maintain cyber superiority as a part of an overall economic and security plan (St-Hilaire, 2020). States might use their political pressure on Internet giants to exploit their technical capabilities within political conflicts[8].

6 Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. https://clck.ru/3A7YMR

7 Ibid.

8 Blenkinsop, Ph. (2022, March 3). EU bars 7 Russian banks from SWIFT, but spares those in energy. Reuters. https://clck.ru/3A7Yt8

Furthermore, Cyberspace has become a major inter-state confrontation field because of the variety of contradicting interests the flowing data represents (Manshu & Chuanying, 2021). These cyber conflicts might trigger political situations with dire consequences if not settled. In practice, it is witnessed that states like China and Russia invested enormous deals of technology to establish their patriotic sovereignty in cyberspace to enhance their cyber security against the domination of Western countries. Even though their policies might Balkanize cyberspace, which contradicts free data flow, these states prioritize national interests (St-Hilaire, 2020). Nationalism is the glaring engine of these policies, evidencing its strong nexus to cyber sovereignty. A prominent example of the nexus between cyber sovereignty and nationalism manifests in Hillary Clinton's promise to eliminate the digital Iron Curtain deployed by China to control data flow on the Internet (St-Hilaire, 2020). It is an inter-state cyber competition for domination motivated by nationalism to guarantee national cyber supremacy. Moreover, the US Cyber Command was established to function as a task force protecting the national US interests in cyberspace against foreign threats[9]. Afterwards, the Chinese President declared, in 2014, the national vigorous endeavour to gain supremacy in cyberspace (Segal, 2014). Nationalist competitions to dominate cyberspace manifests a techno arms race between superpowers to hold strongly this wealthy data resource.

To conclude, wealthy cyberspace ignited states enthusiasm to dominate this sphere of interactions. They are motivated by nationalist ideals of supremacy to guarantee national outperformance in cyberspace. This fact implies states endeavour to impose borders in cyberspace to safeguard national interests and defend sovereignty. Through these endeavours, the concept of nationalism is represented in cyberspace, which proves its strong tie with cyber sovereignty. Indeed, defending national cyber borders prerequisite to developing a mechanism to assign these borders in cyberspace.

1.3. Cyberspace Demarcation: The Need for a Determinant

The previous review reveals that jurisprudence admitted that assigning borders in cyberspace is indispensable to determining the limits of national sovereignty for evading potential confrontations. The existence of cyber borders is the core of cyber sovereignty which grants their demarcation a distinguished importance. In the real world, the demarcation of inter-state borders does not constitute an obstacle because states utilize the traditional tools adopted and affirmed by international law. Furthermore, nationalist motivations imply assigning obvious state borders to enable national defence in cyberspace. Nevertheless, because of the technically ambiguous nature of cyberspace, the process of assigning national borders becomes prominently complicated.

[9] Command (2010), Our Mission and Vision. https://clck.ru/3A7XsQ

It is affirmed that the state territory is the spatial of its exclusive authority, which is bounded by admitted and clear boundaries that constitute the state political borders (Ahmed, 2021). Traditionally, borders indicate the extent to which a state can impose its authority. Thus, demarcating obvious borders between states and territories is crucial for stability and peace; it prevents unlawful interference among nations. Since a state without a territory is not imagined, a territory without borders cannot exist because the integrity and acceptance of a territory depends on assigning its obvious and stable borders. Traditional borders are maintained by techniques under authorization legal chains that surveil the physical movement of persons and goods, e.g., entry and departure visas, customs administration, and frontier and coast guard units (Simmons and Hulvey 2023).

Likewise, cyberspace demarcation occupies a prominent order in protecting state interest policies. States have a legal right to impose their sovereignty against cyberattacks targeting national infrastructure. Furthermore, cyber sovereignty is a chief concern regarding criminal justice because of the obligation of the national judicial authorities to respect other state sovereignty while gathering evidence on the Internet (Sallavaci, 2020). Cross-border judicial proceedings should be organized by multilateral, or bilateral, treaties to avoid violating cyber sovereignty. Therefore, contemporary scholars admit that cyber sovereignty is required for criminal justice. This fact requires innovating an appropriate mechanism to assign borders in cyberspace. Nevertheless, the rapid dynamic environment of cyberspace as a consequence of the tremendous universal data flows complicates assigning clear political borders (Abdelrahman & Mekhiemer, 2022). Restricting the national territory in cyberspace to a limited space is a complicated idea because of the lack of a disciplined determinant, contrary to traditional borders. Traditional interstate borders have become unrealistic because of the global theme of cyberspace (Ahmed, 2021).

To border the national cyber territory, states use their traditional territorial metaphors to respond to foreign cyber threats (Simmons and Hulvey, 2023). This approach is motivated by the states spatial thinking of cyberspace. They consider cyberspace a territory to dominate where they practice sovereign control. Techniques like data localization, website blocking, and judicial cooperation requests are symbols of combining technologies and law to demarcate cyberspace. Osborn's definition of cyber borders reflected this attitude. However, depending on a technical pillar to impose a firm border in cyberspace might prove deficient because of the rapid developments of Internet technologies that might confront slow legislation amending process. Thus, it becomes urgent to develop a stable determinant of cyber borders. This research introduces the concept of state interest as a determinant of cyber borders.

2. Utilizing the State Interest Concept to Demarcate Cyberspace

2.1. Demonstrating the Concept

The concept of human interest refers to the needs which persons seek to satisfy for their well-being. These needs are not purely singular but they have social specifications resulting from their contributions to social relations. Moreover, they are not absolute because of production capabilities restrictions (Wang, 2022). Through their pillars, interests manifest the social transformation of human needs and the tight tie binding humans together in a specific field of interactions. They are determinants of human relations that unify them in certain situations and diverse them in other situations. Because of the diversity of interest factors, they can create contradicted positions among social groups, i.e., states (Wang, 2022). Interests are the starting points for creating political, economic, and social ties within a community (Wang, 2022). Cox (2021) argued that interests have become the main pillar of social sciences concentration because of their contribution to the concept of collective emotions in a community (Cox, 2021). Thus, interests are the effective expression of the collective motivation of a group that drives national authorities to react for protection.

Concerning states, interests as a social phenomenon refer to national requirements that satisfy domestic needs against the interests of other states. Since states might differ in their interest identification standards, conflict of interests occurs. Therefore, interests determine the way that states behave to guarantee their needs. Applying this meaning in cyberspace implies that each state would conduct itself to satisfy its national needs on the Internet; states cyber behaviour will be conducted according to their interests.

States interests are common interests because they are formed by the needs of a united group (Wang, 2022). In cyberspace, the concept of state interest, as a common interest, has main characteristics; publicity, realization through the chain of product supply, unity, fundamental values inclusion, and independence (Wang, 2022). These are the chief determinants of state interest as a concept.

2.2. The Political and Legal Implications of State Cyber Interest Concept

Fang argued that national sovereignty in cyberspace is a political state interest (Fang, 2018) and when a state imposes its authority over its cyber territory it defends national cyber interests. Put differently, assigning political borders in cyberspace and tightening national sovereignty within them reflects a utilization of the state interest concept to determine and maintain cyber borders. Another example of subordinating state cyber diplomacy to state interest is the contradiction between the US and China.

While the US fights for unlimited cyberspace because achieving national interests demands the free flow of data, China tends to impose strict cyber borders to defend cyber independence (Fang, 2018). This instance highlights the critical impact of the interest concept on state cyber policies. States can enforce data processing to ensure the legitimacy of exchanged data within their cyber borders and to track illegal cyber activities (Paice & McKeown, 2023). This practice enhances the integrity of the national cyber terrain and the true concept of cyber sovereignty. It is a critical contribution of the state interest concept to securing cyber borders. In particular, state interests are the chief motivation for nationalism in cyberspace (Cox, 2021); wherever a state cyber interest is threatened, a national intervention becomes obligatory to defend the integrity of national benefits. This conclusion accords with the core of sovereignty and nationalism in cyberspace. Furthermore, threatening state cyber interests triggers cyber warfare which includes mutual cyberattacks across states cyber borders to defend national economic and military facilities (Fang, 2018). Threats to cyber interests demand urgent state reactions to confront them, protecting national interests.

In 2024, a US Report pointed out the urgent need to draft a clear cyber diplomacy to protect state interests in cyberspace[10]. This report presented an official governmental admittance of the state cyber interest concept and utilized it to plan national diplomacy in cyberspace. Consequently, the concept of state cyber interest is affirmed in politics and diplomacy. Likewise, the EU adopted joint cyber diplomacy, which maintains the collateral cyber interests of the EU (Reiterer, 2022). He encouraged the EU to adopt the most advanced technologies to protect cyber interests against the ongoing growth of competitive cyber powers (Reiterer, 2022). Cyber interests have become a prominent element in drafting national grand strategies.

From a legal perspective, it is admitted that cyberspace is a virtual sphere of global interactions that generates real relations among nations. Cyber interactions cause impacts on human relations in the real world. This fact triggers the need to regulate cyberspace, providing a legal framework for these interactions (Fang, 2018). Thus, states impose their legislation in cyberspace to protect their national interests.

2.3. The Judicial Interpretation of State Cyber Interest Concept

Contextualizing the concept of state cyber interest is not solely rhetoric because studying case laws, including cyber litigations, figures out how national judiciaries utilized this concept to settle cyber disputes.

[10] US Government Accountability Office. (2024, January). Cyber Diplomacy. State's Efforts Aim to Support U.S. Interests and Elevate Priorities: Report to Congressional Addressees. https://clck.ru/3A7Y99

The US judiciary confronted the threat of online child pornography in State v. Hunt (2020) to defend American society. Their rulings were based on the gravity of exploiting minors in this heinous behaviour. Therefore, the court claimed that the possession of pornography materials expresses the defendant's criminal intent to view it according to 18 U.S.C. § 2252A. The judgment reflects that a state cyber interest, i.e., eliminating online child pornography, led the court to impose national legislation in cyberspace. Likewise, in People v. Jacobo (2019) the court applied the US definition of online human trafficking under the permission to prosecute this criminal actus reus universally granted by the Californians Against Sexual Exploitation Act (the CASE Act 2012) for law authorities to prosecute these activities if a US citizen is involved. It is a clear extension of the US cyber borders because the state interest requires this. The judicial shield is manifested in the US court intervention to protect the integrity of the electoral regime in Democratic Nat'l Comm. v. Russian Fed'n (2019) against foreign cyber attacks that threatened the whole US democratic system. Furthermore, economic state cyber interest was valid to initiate judicial proceedings to defend as in REGINA v CORY AGUILAR (2018); a UK court indicated that harm inflicted on the plaintiff by the defendant's cyber money fraud activity sufficed to imprison him upon found guilty. In addition, The UK judiciary countered internet smuggling in Regina v Stephen Brownlee (2020). The court approved targeting undisclosed websites that were used by smugglers as platforms of illegal goods exchange. The judgment considered these websites as state borders' penetration spots and permitted taking them down to protect national interests.

Defending national creativity, the UK judiciary confronted illegal online trade in unlicensed materials or artworks in Lifestyle Equities CV v Amazon UK Services Ltd. (2021) and Tunein Inc v Warner Music UK Limited, Sony Music Entertainment UK Limited (2021). Needless to say, unoriginal materials inflict moral and financial harm to patent owners whose protection manifests a critical state interest under the UK Copyright, Designs and Patents Act 1988.

Defending society against rumours, American judge O'Scannlian considered an inaccurate online business report in Robins v. Spokeo (2017) a violation of the US Fair Credit Reporting Act that grants the plaintiff the right to compensation. Similarly, the UK court admitted the same right in Ghannouchi v Middle East Online Ltd & Anor (2020). Thus, it confronted the spread of fake information on the websites defending the credibility of the national press.

To conclude, the previewed judgments reveal that judiciaries admitted the existence of the cyber borders concept by connecting it to the concept of state interest. This functional interpretation means that the state cyber borders are assigned according to the state interests in cyberspace; wherever an interest exists, states can extend their cyber sovereignty to defend it. Nonetheless, the judgments do not introduce a normative definition of cyber borders; the interests that they defended on the internet are the state's cyber borders according to the functional interpretation which accords with Osborn's (2017) and Zein's (2022) definition.

3. The Applicability of the State Interest Concept to Demarcate Cyberspace

3.1. Applicability Foundations

Needless to say, cyberspace still lacks a firm determinant of borders concept. States utilize several mechanisms to safeguard their national interests. The diversity of cyber domestic policies contradicts the universality of cyberspace which stability requires a unified set of normatives. The absence of multilateral conventions on cyberspace demarcation, the competitive political cyber interests, the diversity of national interpretations of legal notions, and the establishment of attribution and accountability in cyberspace are the chief odds before adopting a global determinant of cyber borders concept[11]. With the absence of a legal demarcator, the research introduces the notion of state interest as the required determinant of the cyber borders concept.

As a global common, cyberspace requires a universally admitted standard to assign political borders. Keep in mind that the pure technical nature of cyberspace does not prevent the contextualization of legal notions within its sphere. The traditional concept of sovereignty stretches to cyberspace, but in a form that complies with its technical theme (Choucri & Clark, 2013). Combining law and technology was the major odd that stood before scholars' endeavours to develop a normative to demarcate cyberspace. This odd drone Osborn to adopt an ultimate technical approach to define cyber borders as previously shown. Nevertheless, the scholarly evolution discloses the prominent approach to link borders and sovereignty concepts in cyberspace to the state interest concept.

Adaptability is the key to the successful integration of a legal notion into a digital environment (Akhmatova & Akhmatova, 2020). It is the challenge that stands before cyberspace legalization and governance. The adaptability of the state interest concept to the technical vague nature of cyberspace is glaring. Since cyberspace is full of different categories of human needs, the concept of interest is crystallized in the methods adopted by nations to satisfy those needs. As Wang (2022) indicated, interests are the true expression of social life among communities; they are the engine of human social interactions. Therefore, they should be prioritized when assigning boundaries and limits between groups. Therefore, the concept of state interests in cyberspace has evolved to formulate the threshold of state cyber policies. The adaptability of its pillars with cyber interactions qualifies this concept to be employed as a determinant of state authority in cyberspace.

[11] Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. https://clck.ru/3A7ZPU

Furthermore, national interests are the chief motivations for states intervention in cyberspace. Studying the Chinese and Western approaches discloses their hastened endeavours to crystallize their cyber sovereignty according to the national interests they plan to safeguard in cyberspace. In particular, the firm presence of nationalism in cyberspace motivates states to utilize their domestic legal toolkits to defend their cyber interests. Based on Benabid's[12] and Paice and McKeown's (2023) analysis, states interests are the active engines of national policies in cyberspace. These facts prove the national prioritization of state cyber interests, which are reflected in the political implications of this concept.

From a judicial perspective, the judgments of national courts in cyber disputes qualify the state interest concept to assign cyber borders. The US and UK judiciaries extended their jurisdiction in cyberspace wherever a national interest is threatened. Since jurisdiction manifests sovereignty, domestic courts impose national sovereignty to the extent that state interests are affected. This judicial interpretation employs the state interest concept as a determinant of state cyber sovereignty and, consequently, borders.

3.2. Demarcation Practical Framework

After establishing the legal foundation to utilize the concept of state cyber interest to determine cyber borders, it is obligatory to develop a practical framework for this process otherwise the whole establishment becomes fruitless. The article introduces several methods to employ this concept as a boundary determinant.

Because of the universality of cyberspace, scholars suggest using international law mechanisms through conventions and developing customary international law to support the adaptability of pure legal notions to the technical nature of cyberspace[13]. Thus, states should tend to sign conventions on adopting the state interest concept to assign cyber borders. Regulating universal cyberspace requires universal mechanisms because unilateral policies might jeopardize global regulation endeavours. In addition, multilateral understandings ensure international consensus on adopting state cyber interest as a demarcator in cyberspace. As a consequence, the concept of state cyber interest achieves disciplinary that enhances its contribution to cyberspace governance.

---

[12] Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. https://clck.ru/3A7YMR

[13] Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. https://clck.ru/3A7ZPU

Innovation is the key to overcoming techo-legal dilemmas (Linden & Shirazi, 2023). Scholars need to develop their traditional interpretation of legal notions to adapt them to technical environments like cyberspace. Moreover, innovation is a pillar of modern cyber operations because it grants states advantageous opportunities in cyberspace (Soare, 2023). In the judicial field, domestic courts combined technical tools with traditional legal notions to overcome the technical nature of cyber disputes. It is a unique mechanism to protect cyber borders, which has two pillars: law and technology. This hybrid structure provided that mechanism with flexibility that adapted legal concepts to technical cyberspace. Furthermore, flexibility enhanced the national courts' ability to counter cyber threats. Innovation is the key that enabled the judges to overcome the technical odds of cyber disputes and legislation stagnation by combining law and technology.

Handling a discourse with rapid leaps implies transcending realities to tackle obstacles. Therefore, depending solely on realistic logical reasoning to settle the techno-legal dilemma drives jurists to a standstill. In this case, imagination offers a critical contribution to pushing forward legal doctrine. In the legal aspect, imagination provides scholars with impressive, persuasive, and innovative opportunities to overcome traditional obstacles (d'Aspremont, 2022). Legal imagination constitutes a powerful tool against legal bureaucracy; it is "a thinking of the impossible for the sake of resistance" (d'Aspremont, 2022). Furthermore, imagination, from a legal perspective, enhances jurists' capabilities to reconceptualize existing norms within flexible technological environments, where changes occur rapidly and randomly (Pollicino, 2020). Thus, legal imagination enables scholars to develop traditional legal notions to suit the rapidly evolving technical spheres like cyberspace. It should be noted that the concepts of borders and sovereignty were imagination which scholars and courts had successfully interpreted and incorporated within realistic legal contexts through innovative techno-legal principles included within their judgments and interpretations. Likewise, the concept of state cyber interests, through legal imagination, could be contextualized effectively in cyberspace to assign borders and sovereignty. The aforementioned judgments adopted this concept to determine the scope of national jurisdiction, which manifests a direct implication of state sovereignty within national borders. Consequently, it could be concluded that the state cyber borders extend to each spot in cyberspace where a state interest is affected. This interpretation reflects the flexibility of the state interest concept that suits the vague nature of cyberspace where rigid norms are technically jeopardized. Thus, imagination resurrects traditional legal notions in cyberspace by granting them the effective feature of adapting to cyberspace, which is flexibility.

Conclusion

In summary, cyberspace has proven resistant to boundary imposture through traditional demarcation methods adopted to demarcate borders in the real world. Scholars sought to portray sovereignty and borders in cyberspace; the diversity of their attitudes created contradicting understandings of these concepts in cyberspace. Indeed, this contradiction destabilizes universal cyber relations. To overcome this dilemma, the research seeks to develop a modern legal mechanism to determine sovereignty and borders in cyberspace.

Unlike scholarly endeavours, this study adopts a pure legal notion to determine a technical concept. It presents the concept of state cyber interest as the cyberspace demarcation tool. The utilization of this concept implies imposing national sovereignty in cyberspace according to any effect on national interest. Ensuring the functionality of the state interest concept, the research sheds light on its adaptability to the technical nature of cyberspace to transcend traditional odds before integrating a pure legal notion into a technical environment. Furthermore, the required mechanisms to employ this concept have been elaborated on to defend the applicability of this article hypothesis.

References

Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, *16*(15), 423–443. (In Arabic). https://doi.org/10.21608/jocu.2022.134235.1172

Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, *2*(6), 632–646. (In Arabic).

Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, *5*, 6. https://doi.org/10.1186/s41018-020-00076-2

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

Cox, L. (2021), *Nationalism: Themes, Theories, and Controversies. Palgrave Macmillan*. https://doi.org/10.1007/978-981-15-9320-8

d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, *35*(4), 1017–1027. https://doi.org/10.1017/s0922156521000637

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13

Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, *1*, 119. https://doi.org/10.12688/openreseurope.14010.2

Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, *9*, 22. https://doi.org/10.1186/s40854-022-00432-8

Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, *3*, 97–114. https://doi.org/10.1007/s42533-021-00079-7

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. https://doi.org/10.1093/acref/9780199207800.001.0001

Omar, M. O., AlDajani, I. M., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.

Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity, Springer, Singapore*. https://doi.org/10.1007/978-981-19-6414-5_1

Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online. Edward Elgar Publishing*. https://doi.org/10.4337/9781788976688.00009

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action*. New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1

Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.

Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship, 3158*.

Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. https://doi.org/10.4324/9781003284093-6

St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-61386-0

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, *3*(3), 679–738. https://doi.org/10.21608/ijdjl.2022.138565.1159 (In Arabic).

Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*, 45. https://doi.org/10.1007/s44206-023-00067-x

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflicts of interest

The author 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 – September 21, 2023
Date of approval – October 12, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.3:004.9
EDN: https://elibrary.ru/sywsrk
DOI: https://doi.org/10.21202/jdtl.2024.14

Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре, Сохаг, Египет

Ключевые слова

государство,
граница,
кибербезопасность,
киберинтерес,
киберпространство,
киберсуверенитет,
национальный интерес,
право,
суверенитет,
цифровые технологии

Аннотация

Цель: обосновать существование национального киберсуверенитета как юридического понятия, наряду с которым путем введения инновационной детерминанты – концепции государственных киберинтересов – переосмыслить традиционные понятия национального суверенитета и государственных границ в условиях динамичной природы киберпространства и необходимости разработки гибридного механизма защиты кибергранниц, основанного одновременно на праве и технологиях.

Методы: на основе доктринального метода выявлены принципиальные расхождения в представлениях ведущих ученых разной отраслевой принадлежности по концептуальным теоретико-методологическим и понятийно-категориальным вопросам, в том числе по вопросу обоснования единого алгоритма для установления границ в киберпространстве. Доктринальный метод дополнен анализом судебной практики разных стран, позволяющим рассмотреть распространение судами своей юрисдикции на споры, связанные с киберпространством.

Результаты: в исследовании представлено применение традиционных и современных правовых концепций суверенитета в новой, цифровой среде, результатом чего стало сочетание правовых и технологических подходов. Раскрыто функциональное значение концепции государственных киберинтересов для демаркации киберпространства и определения границ национального суверенитета. Показана адаптируемость данной концепции к технически неопределенной природе киберпространства. Делается вывод об основных направлениях формирования концепции киберинтересов в киберпространстве, ее политических и правовых последствиях, основанных в том числе на практике судов разных стран по разрешению киберспоров.

Научная новизна: концепция государственных киберинтересов рассматривается в качестве инновационного метода определения кибергранниц, что обусловливает трансформацию смысла традиционного понятия суверенитета и тесно связанного с ними понятия национальных интересов применительно к киберпространству в контексте обеспечения требований безопасности и активизации национальной защиты от киберугроз.

Практическая значимость: полученные результаты устраняют имеющиеся противоречия в определении суверенитета и его пространственных пределов в условиях развития современных технологий; способствуют выработке дисциплинарного стандарта киберсуверенитета на основе надежного демаркатора, необходимого для определения государственного суверенитета и границ в киберпространстве; адаптируют традиционные юридические понятия суверенитета и национальных интересов к глобальным современным кибервызовам; способствуют трансформации традиционных правовых институтов и норм в области суверенитета и границ в условиях киберпространства.

Для цитирования

Абделькарим, Я. А. (2024). Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств. *Journal of Digital Technologies and Law*, *2*(2), 262–285. https://doi.org/10.21202/jdtl.2024.14

Список литературы

Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, *16*(15), 423–443. (In Arabic). https://doi.org/10.21608/jocu.2022.134235.1172

Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, *2*(6), 632–646. (In Arabic).

Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, *5*, 6. https://doi.org/10.1186/s41018-020-00076-2

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

Cox, L. (2021), *Nationalism: Themes, Theories, and Controversies. Palgrave Macmillan*. https://doi.org/10.1007/978-981-15-9320-8

d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, *35*(4), 1017–1027. https://doi.org/10.1017/s0922156521000637

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-0320-3

Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13

Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, *1*, 119. https://doi.org/10.12688/openreseurope.14010.2

Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, *9*, 22. https://doi.org/10.1186/s40854-022-00432-8

Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, *3*, 97–114. https://doi.org/10.1007/s42533-021-00079-7

McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press.

https://doi.org/10.1093/acref/9780199207800.001.0001

Omar, M. O., AlDajani, I. M., Juwaihan, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.

Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity, Springer, Singapore*. https://doi.org/10.1007/978-981-19-6414-5_1

Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online. Edward Elgar Publishing*. https://doi.org/10.4337/9781788976688.00009

Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacifc. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action*. New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2

Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1

Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.

Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship, 3158*.

Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. https://doi.org/10.4324/9781003284093-6

St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-61386-0

Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. https://doi.org/10.1007/978-981-19-3963-1

Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, *3*(3), 679–738. https://doi.org/10.21608/ijdjl.2022.138565.1159 (In Arabic).

Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-94736-1

Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*, 45. https://doi.org/10.1007/s44206-023-00067-x

Сведения об авторе

Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре, Министерство юстиции Египта
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Конфликт интересов

Автор сообщает 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: 10.15.41 / Государственный суверенитет
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 21 сентября 2023 г.
Дата одобрения после рецензирования – 12 октября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.15

Legal Issues of Cross-Border Data Transfer in the Era of Digital Government

Gulbakyt Bolatbekkyzy
Wuhan University, Wuhan, China

Keywords

cybersecurity,
data protection,
digital government,
digital technologies,
digitalization,
human rights,
law,
personal data,
privacy,
transboundary exchange

Abstract

Objective: to identify the main legal factors of cross-border data exchange in the context of digital technology proliferation and government digitalization, including legal guarantees, security issues, cybersecurity risks, approaches to regulating and improving the efficiency of data management in various jurisdictions.

Methods: the study relies on synthesis and critical analysis of various aspects of the stated problem, including analysis of primary and secondary sources. By the example of the regulatory policies of China, the US, the EU and EAEU member states, different approaches regarding the restriction or encouragement of free cross-border data transfer are compared. A comprehensive meta-analysis and literature assessment provided insights into the methods used for data protection in different jurisdictions and allowed outlining the framework and directions of the public policy required for effective cross-jurisdictional data transfer.

Results: the main challenges associated with cross-border data transfer in the context of digital technology proliferation and government digitalization, such as growing inequalities in digital development, legal uncertainties, privacy and cybersecurity, etc., were identified. The legal framework of cross-border data transfer in the context of government digitalization and its implementation were analyzed. It contributed to the search for ways to improve the government efficiency in the context of transnational data transfer, including rendering services and promoting openness and public participation.

Scientific novelty: based on the analysis of various jurisdictions' approaches to legal, security and sovereignty issues caused by transnational data transfer, the author reveals the role and applicability of international law, as well as the unique challenges arising in the member states of the Eurasian Economic Union on the way to the formation of transboundary trust space.

Practical significance: the study of these issues may help various public agencies, first of all, governmental and legislative bodies to the elaborate well-targeted political and legal decisions, aimed at achieving a balance between data availability and data security, between the effectiveness of public administration and respect for the human rights. The results obtained will also be of importance for other subjects of relations in cross-border data transfer and regulation of these relations.

For citation

Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. *Journal of Digital Technologies and Law, 2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Contents

Introduction

Transboundary transfer of data in the realm of digital government entails the crossing of national borders with personal or sensitive data for diverse objectives, encompassing the delivery of governmental services, fostering international partnerships, and facilitating data exchange between government agencies and private-sector collaborators. The transfer of data across borders within digital government is essential for enhancing government services and fostering international cooperation. This practice plays a vital role in the advancement of government services and the promotion of global cooperation.

Nevertheless, it presents legal, security, and sovereignty issues that necessitate resolution through international accords and robust data protection measures. Striking a balance between data accessibility and safeguarding is an intricate endeavor, demanding careful navigation by governments while upholding citizens' rights and adhering to international legal frameworks.

Furthermore, currently, there isn't a single globally accepted, harmonized law or regulation regarding transboundary data transmission or comprehensive data regulation that can be unanimously approved by members of the international community. It is worsened by the increasing inequality in proliferation of digital technologies, which are not equally available for all the nations regardless of their GDP.

1. Transboundary data transfer and its role in digital government

1.1. Categorization of transboundary transfer of data

Transboundary transfer of data is divided into four main categories of types, which include: Inter-Governmental (or Government to Government: G2G) data exchange among government agencies from distinct nations, serving objectives like diplomatic collaboration, law enforcement coordination, and disaster response. It is commonly accepted practice when international law enforcement agencies frequently exchange data to combat global crime. For instance, EuroPol facilitates information sharing among European law enforcement agencies to address organized crime and counter terrorism (De Moor & Vermeulen, 2010). In times of international crises, governments collaborate by sharing data to manage disaster response and humanitarian aid efforts. For example, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) facilitates data sharing during humanitarian emergencies (Bennett, 2002).

Second one is Government to Enterprise (or Government to Business: G2B) Data sharing with private-sector organizations to facilitate public-private cooperation or privatization of government functions (e.g., outsourcing tax administration to private companies). Data pertaining to international trade and customs, including shipping particulars and cargo manifests, are exchanged between governmental entities and

customs authorities to expedite the seamless transit of commodities across international boundaries. In order to prevent firms and people from paying multiple taxes on the same income, tax authorities from several countries may exchange taxpayer information as part of double taxation agreements (Niu et al., 2021).

Then the third one is Government-to-Individual (or Government to Citizen: G2C) Cross-border transfer of citizens' data for international services (e.g., accessing healthcare while overseas). When citizens from one nation travel abroad, their medical records may be accessible internationally to ensure consistent healthcare. For example, the EU's eHealth Digital Service Infrastructure (eHDSI) allows EU citizens to access healthcare data while traveling within the EU (Bruthans & Jiráková, 2023).

Legal frameworks and compliance of transboundary data transfer in digital government play an essential role, which encompasses Data Protection Laws and International Agreements in this regard. If in the first one (Data Protection Laws) data transfers should adhere to the data protection regulations of both the originating and receiving nations, here as an illustration, the European Union's General Data Protection Regulation imposes stringent conditions on transboundary transfer of data, focusing on adequacy determinations, standard contractual clauses, and binding corporate rules, along with that concerning this it would be worth mentioning Chinese Personal Information Protection Law (PIPL), which also has extraterritorial reach and requirements for both government and non-government sectors. Whereas in the second one (International Agreements) certain countries establish bilateral agreements to regulate data transfers. One such agreement was the EU-U.S. Privacy Shield, which facilitated data exchanges between the EU and the United States until it was invalidated in the "Schrems II" case.

Sovereignty concerns along with data localization are gradually becoming one of the most sensitive topics within cross-border data flow. Certain nations enforce data localization mandates, necessitating that specific data categories are kept within their own territory. As an illustration, Russia's data localization regulations dictate that the personal data of Russian citizens must be stored on servers located within Russia (Gurkov, 2021). As another example, just a recent case of Russian branch Yandex.kz in Kazakhstan[1], where Ministry governors and Yandex's representatives came to the agreement to physically relocate its servers to Kazakhstan after the incident of site's block on the territory of Kazakhstan due to the company's unwillingness to abide by the agreement's conditions.

When data is transferred across international borders, security and cybersecurity are equally important. Data must be protected to avoid unwanted access or breaches. In order

[1] Yandex transfers its structure to Kazakhstan under the threat of blocking (August 21, 2023). CNews. https://clck.ru/39o7xf

to guarantee the privacy and security of transferred data, it is essential to use encryption, secure protocols, and strong cybersecurity measures.

Improving government services and promoting international cooperation within digital government requires cross-border data sharing. However, it raises challenges related to sovereignty, security, and law that must be resolved by international agreements and strong data protection protocols. Finding a balance between data accessibility and security is a complex process that requires governments to navigate carefully while respecting the rights of their citizens and following international legal frameworks.

1.2. Data privacy and security concerns in transboundary transfer of data

The data transfer across borders in digital government gives rise to substantial apprehensions regarding data privacy and security. These concerns emanate from various factors, including legal safeguards, security vulnerabilities, cybersecurity risks, jurisdictional complexities, intricate regulations, and the necessity for strong data management. Effectively tackling these concerns mandates the implementation of legal protocols, cybersecurity tactics, and data management procedures aimed at safeguarding the private information of citizens within an ever more interlinked digital realm.

As new advanced technologies continue to evolve, people's expectations for enhanced services and improvements in various aspects of life are on the rise. Technological advancements bring forth better solutions to existing problems while also introducing new concerns related to security and privacy. The digitization of information resources presents increasing challenges to digital data and infrastructure. While advanced nations have rigorously tested security measures and optimization techniques, developing countries still face inadequacies in addressing these issues[2].

Transboundary transfer of data involves adhering to legal bases and regulatory requirements that are essential for the unobstructed movement of data. These requirements apply to both internal transfers within an organization that extends across national boundaries and external transfers to organizations in different countries. For instance, many jurisdictions, including the EU, UK and China have established regulations stipulating that to ensure the safe and lawful transfer of data from one country to another, the recipient country must uphold privacy standards for personal information that are at least on par with those of the sending country. Only when this equivalency is verified can an adequacy decision be granted by a data privacy regulatory

[2] UNGA. Nearly Half of the World's Population is Excluded from 'Benefits of Digitalization', the Speaker stresses as the Second Committee Debates Information Technology for Development. https://clck.ru/39o86M

body or government authority (in the EU case it is conducted by the European Commission), allowing for the unrestricted flow of data across borders.

2. Securing and enhancing transboundary transfer of data

2.1. Security mechanisms in the transboundary transfer of data

In order to comprehensively cover the current environment of security in the cross-border data-transfer, this chapter, examines the practices of various range in place. Despite the fact that there is no worldwide framework for certifying data protection adequacy to enable transboundary transfer of data, nevertheless, numerous countries and regional groups have implemented their own rules and regulations to oversee these data transfers across borders. For transboundary transfer of data there are five widely used mechanisms that are in place:

1. Decisions on adequacy: Some data protection rules allow data to be transferred to areas recognized by a public body as having data protection standards that are on par with or higher than those of the home country. The European Commission, under the EU's General Data Protection Regulation, is responsible for issuing adequacy determinations. Research conducted by the IAPP reveals that 74 jurisdictions authorize public entities, such as data privacy regulators or government authorities, to issue adequacy determinations for data transfers[3]. It's critical to understand that adequacy rulings are not always final and could be reevaluated in response to changing circumstances or modifications to data protection laws.

2. Contractual agreements: or data transfer contracts are employed to authorize data transfers beyond the boundaries of an organization's jurisdiction. These contracts guarantee the strict observance of pertinent compliance standards, such as those pertaining to data processing and storage. Standard Contractual Clauses (SCCs) are the most commonly used contractual clauses in practice. These are pre-written clauses that can be included into contracts between data importers and exporters for transboundary transfer of data. The European Commission has approved them as complying with the GDPR. 71 countries presently have drafts, templates, or standardized contractual clauses available, according to the IAPP's evaluation[4].

3. Intra-organization transfers or Binding Corporate Rules (BCRs) represent a collection of internal policies and agreements that govern data compliance and authorize transboundary transfer of data within a single organization. The recognition of BCRs extends to various jurisdictions, including the EU, UK, Brazil, Singapore, and South Africa. Many organizations opt to adopt EU BCRs to structure their global data privacy compliance initiatives. However,

---

3 International Association of Privacy Professionals. Infographic: Global Adequacy Capabilities. https://clck.ru/39o88u

4 Ibid.

implementing BCRs can be an intricate and time-consuming process, as it necessitates approval from pertinent data protection authorities.

4. Certification mechanisms: Several jurisdictions acknowledge certifications issued by approved data authorities for transboundary transfer of data. To achieve certification, businesses must secure approval from an independent Accountability Agent (AA). These AAs can be either public entities or private organizations. Presently, the sole certification-based transfer mechanism in use is the APEC Cross-Border Privacy Rules (CBPR) System. This certification validates compliance and holds recognition in eight countries: Australia, Canada, China, Japan, South Korea, Mexico, Singapore, and the US.

5. User consent: While challenging to scale, securing user consent has traditionally been the primary approach for transboundary transfer of data, especially in complex legal environments where consent is the central element amidst various data transfer frameworks. User consent must meet specific criteria, including being informed, explicit, and unambiguous, with standards for obtaining consent varying across jurisdictions. Under the GDPR, user consent may serve as a transfer mechanism only when no adequacy decision or suitable safeguards, such as SCCs or BCRs, are available. The lack of a global framework for the certification of adequate data protection can make it challenging for organizations to navigate the complex landscape of data protection regulations.

In this regard numerous governments are actively addressing the challenge of transboundary transfer of data. They are collaboratively striving to create a favorable setting for legitimate cross-border data flows, all the while safeguarding individual privacy rights and upholding data security.

2.2. Governments' initiatives enhancing the efficiency of transboundary transfer of data

Here are some recent initiatives undertaken by particular governments to enhance the efficiency of transboundary transfer of data.

The European Union and United States have collaboratively introduced a new EU-U.S. Data Privacy Framework (DPF)[5]. This framework replaces the former Privacy Shield framework, which was invalidated by the Schrems II ruling in 2020. The European Commission has been instructed not to approve the framework until it has been updated to adequately address the concerns expressed by the Schrems II case by both the EU Parliament and the EU Data Protection Board (Gao & Chen, 2022).

Under the leadership of Japan, G7 governments are actively developing the Institutional Arrangement for Partnership (IAP)[6]. This partnership aims to bridge the gap in creating

[5] International Association of Privacy Professionals. (n.d.). EU-U.S. Data Privacy Framework: Guidance and Resources. https://clck.ru/39o8Dg

[6] World Economic Forum. (2023, April 26). How and why data must flow freely and responsibly across borders. https://clck.ru/39o8Gf

an effective and trusted international cooperation mechanism for operationalizing Data Free Flow with Trust (DFFT).

As of June 1, 2023, China implemented the Measures on the Standard Contract for the Transboundary Transfer of Personal Information. These measures mandate that specific personal data processors, even those handling data for fewer than 1 million individuals, must enter into contracts with overseas recipients before transmitting data abroad. China's overarching legislative framework for managing data security encompasses three key laws: the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. These laws are supported by a range of governmental regulations that are consistent with the legal framework. Under these laws, the central government has established its regulatory system for the export of personal data.

Additionally, a Global Cross-Border Privacy Rules (CBPR) forum has been established (Joel, 2023). Member economies of the Asia-Pacific Economic Cooperation (APEC), including the United States, Canada, Japan, Singapore, and others, have initiated this forum with the objective of setting up an international certification system based on the APEC CBPR System and related Privacy Recognition for Processors (PRP) Systems.

As the digital economy undergoes rapid transformation, organizations must remain agile and proactively update their methods and protocols to align with the ever-changing regulatory environment. This is particularly crucial for large organizations with extensive global operations, as non-compliance can result in substantial fines. In 2021, for instance, European data protection supervisory authorities imposed fines amounting to nearly $1.2 billion USD, with the largest fine levied against a US-based online retailer[7]. Chinese companies based within the country, aiming for international initial public offerings, continue to grapple with the repercussions of the China's Cyberspace Administration (CAC) fining the prominent ride-hailing firm, Didi Global, a substantial 8 billion yuan ($1.2 billion) last year for violations of national security and personal information protection regulations[8].

Given the various mechanisms available for facilitating transboundary transfer of data, it is incumbent upon each organization to evaluate and choose the most suitable options based on their specific needs. There is no one-size-fits-all solution. Depending on the use cases, governments may discover the need to employ multiple frameworks to address their particular requirements. It is also vital to consider how the data transfer approval process can be seamlessly integrated into existing workflows. Failure to establish an efficient and appropriate process can result in prolonged and costly endeavors when seeking clearance for data transfers on an ad-hoc basis.

---

7 EDPB. (2023, May 22). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. https://clck.ru/39o8HK

8 Webster, G. (2022, July 21). Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. DigiChina. https://clck.ru/39o8KA

3. The relevance of international law in regulating transboundary transfer of data

3.1. Different approaches of jurisdictions on transboundary transfer of data

Needless to say, that the role of international law in the regulation of transboundary transfer of data is quite crucial, serving as a cornerstone for safeguarding privacy, upholding human rights, ensuring cybersecurity, facilitating trade, resolving conflicts, and establishing customized agreements. It lays the groundwork and outlines the standards for the appropriate management of data across international borders, promoting responsible data governance and nurturing confidence in digital interactions.

It was noted that the internet "cannot be regulated". The nation-state is irrelevant, not laws; that is the difference (Chuanying, 2020). A joint study commissioned for the Defense Department in 1998 observed:

It may be that the real problem created for governments by the proliferation of the Internet (and other IT-enhanced communications media) is not the proliferation of information so much as the proliferation of actors on the governmental and diplomatic stages. Organized groups and individuals can build, and in fact are building, coalitions, both domestic and international, that can bring unprecedented pressure to bear on national governments regarding virtually any activity or area of interest. These groups may in fact create faits accomplish that require no more action of governments than to accept what has already been accomplished. This raises the question of whether the nature of sovereignty has changed in the area of instant and ubiquitous communications and, if so, how (Press et al., 1998).

An associate professor at the University of Maryland, College Park Dr. Virginia Haufler disagrees, stating, "The decentralized, open, global character of... the Internet makes it difficult to design and implement effective regulations through top-down, government-by-government approaches" (Haufler, 2013).

The devastating circumstances of the 9/11 terrorist attacks and the terrorists' use of the Internet for communication accelerated the developed world's adoption of content restriction. According to an advocacy group that backed journalistic freedom, as early as September 2002, the United States, the United Kingdom, France, Germany, Spain, Italy, Denmark, the European Parliament, the Council of Europe, and the G8 countries had all expressed worries about their rights and freedoms online (Nijboer, 2004).

International governmental organizations have faced significant challenges as a result of substantial differences in state objectives for content restriction. During the inaugural session of the World Summit for the Information Society (WSIS) in December 2003, this division was made evident. The wording employed to address the consequences of any agreement on the management of Internet speech was one of the key areas of contention during the WSIS negotiations. China, not insignificantly, voiced its disapproval of the press freedom text that reflected American influence. As a result, the Declaration of Principles did mention press freedom, but it did so in a way that was more subdued and added language

emphasizing the integration of national sovereignty[9] (Berleur, 2007). Governments were required by the Action Plan to take necessary measures to address harmful and illegal media content while upholding the right to free speech (Jensen, 2006). External observers agreed that the plan of action covered up irreconcilable disagreements on content regulation and provided little guidance for the future (Souter, 2004).

As an example, the United States and the European Union have different approaches to data privacy. The American position on private rights is based mostly on the notion of non-interference from the government. As a result, there hasn't been much support in the US for extensive state laws pertaining to data privacy. Bessette and Haufler (2001) have observed that the US prefers a more market-driven method of data collection. "If private sector privacy protections can be adopted internationally, that would naturally become the prevailing method for safeguarding privacy", stated Ira Magaziner, one of the representatives of President Administration (Farrell, 2003).

In contrast, privacy is regarded in Europe as a fundamental right that needs to be safeguarded by the government. Bessette and Haufler point out that "European nations, in particular, have put in place robust privacy safeguards, defining privacy as a fundamental human right" as a result of past instances of privacy infringements by the government (Mai'a, 2023). The European Union passed the comprehensive Data Protection Directive in 1995, giving European businesses clear regulations and enforcement mechanisms. This directive was designed to prevent companies from operating outside of EU jurisdiction in order to evade the law. It prohibited the transfer of personal data belonging to EU citizens to nations that did not offer adequate security. In late 1998, the directive was scheduled to go into force (Long & Quek, 2002).

In view of the extent to which this prohibition was, nations like Australia, Canada, and Eastern Europe were compelled to change their own legal systems to comply with EU standards. Nevertheless, the US retaliated by pressuring US multinational corporations to establish self-regulatory frameworks compliant with EU laws.

Totalitarian regimes have employed straightforward yet efficient methods for regulating Internet content. There were cases of restricting use of personal computers, controlling and prohibiting objectionable content (in regards of pornographic materials; immoral websites; religious and politically sensitive content) which eventually led to the Internet censorship using filtering system extensively (Drezner, 2004).

Scholars studying globalization have frequently oversimplified the intricate web of governance interactions in international politics by focusing exclusively on the binary opposition between state and nonstate power. A more perceptive view of the effects

[9] McCarthy, K. (2003, December 8). Internet Showdown Side-stepped in Geneva. The Register Newsletter, 8. https://clck.ru/39o8LW

of globalization is offered by acknowledging the possibility of diverse global governance arrangements. An examination of Internet governance shows that governments may nevertheless intervene when necessary to further their own goals, even if they choose to assign governance duties to commercial organizations.

Whenever major powers are unable to cooperate, but other international players support no less than one of the main nations, the result is commonly referred to as "rival standards". Two instances of such rival standards were identified in the case studies: data privacy and regulations for genetically modified organisms (Trump et al., 2023). In both of these cases, the USA and the EU have each propagated distinct sets of rules for regulating these matters. Both parties have managed to secure some level of support, yet neither standard has achieved universal acceptance.

Lastly, it is projected that if the major powers concur but their interests do not align with those of other international actors, the outcome will be "club standards". These standards represent one of the most captivating facets of regulatory processes. In this scenario, the influence of major powers is readily apparent as they exert pressure on and negotiate with other states to establish a standard. This often begins with a small yet influential group, such as the OECD or the Financial Action Task Force on Money Laundering. These coalitions of like-minded states have the capacity to formulate regulations and subsequently persuade or persuade other states to conform to them.

3.2. The privacy shield of the EU-US and its impact on transboundary transfer of data between the EU and the US

The U.S.-EU Privacy Shield was a framework designed to regulate the transfer of personal data from the European Union to the United States. Ensuring that these data transfers followed European data protection regulations was its main goal. After the ECJ overturned the Safe Harbor framework in the wake of the 2015 "Schrems I" decision, this new structure was implemented in 2016. Establishing a legal framework for the transfer of EU personal information to the US and making sure US organizations upheld data protection standards comparable to those in the EU was its main goal.

The European Commission determined that the Privacy Shield offered a suitable level of data protection in the US, and as a result, the EU data protection framework awarded it an "adequacy decision". All pertinent facets of a data transfer operation, or series of related acts, were to be taken into account when determining the protection level. Many variables were considered in this review, including "the legal regulations, both overarching and specific to the third country involved, as well as the professional standards and security measures followed in that country" (Hijmans, 2006).

In order to prevent companies from processing data outside of the EU for the purpose to obtain an exemption from the 1995 Directive, the transfer limitation was implemented

(Drezner, 2008). Some nations did change their laws in an effort to achieve adequacy standards as a result of this clause. But rather than supporting enforceable legislative measures, the United States supported self-regulatory options that were consistent with the federal data privacy policy's self-regulatory nature (Voss, 2019).

Numerous studies have contrasted US and EU approaches to internet regulation policymaking. The results show that the EU generally produces broad and comprehensive legislation. But this legislative procedure frequently moves more slowly, which can be problematic, especially when dealing with the internet's rapid evolution and emerging technology. The US, on the other hand, has a more decentralized regulatory framework with multiple agencies and occasionally incompatible regulations (Reidenberg, 1996).

The substantial disagreement between the two stems from differences, further exacerbated by distinctions between data and metadata. US federal law grants law enforcement significant authority to access metadata (Schneider, 2009).

But with regard to the Privacy Shield, the European Commission's Decision No. 2016/1250 was declared illegal by the CJEU. This resulted from the decision's failure to guarantee a degree of personal data protection equivalent to that required by European legislation (Furramani, 2023).

2016 marked the establishment of European Commission Decision No. 2016/1250, which allowed the transfer of personal data from the EU to the US. This framework was used by EU and EEA businesses to send personal data to US entities listed under the Privacy Shield, offering specific safeguards for data protection (Furramani, 2023).

The case concerned a Facebook[10] user who was an Austrian national and disputed that his data have been transferred to the US because the US did not offer the same level of protection as required by EU legislation. This disagreement resulted in a 2013 complaint that the Data Protection Commissioner initially took an examination at.[11] After reevaluating, the Commissioner concluded that the transfer of personal data to the United States did not comply with Articles 7, 8, and 47 of the European Charter of Fundamental Rights[12]. This prompted the case to move to the High Court.

According to the High Court, the US did not ensure adequate protection for personal information in line with EU Charter of Fundamental Rights Articles 7 and 8. The Court identified several issues, including the application of the Fourth Amendment to European nationals, concerns about the National Security Agency's activities without judicial oversight,

[10] A social network blocked in the territory of the Russian Federation for disseminating illegal information.

[11] CJEU, Schrems II, 2020, July 16, paras 50, 51 and 52.

[12] CJEU, Schrems II, 2020, July 16, paras 55 and 56.

and the Privacy Shield's Ombudsperson not meeting Article 47 of the Charter. In light of these matters, the High Court referred the case to the CJEU[13].

As stated in Article 45 of the GDPR, the CJEU's decision established that transfers of personal information from the EU or EEA to a third country must be predicated on an adequate decision made by the Commission. If such a decision is not made, data may be transferred in accordance with Article 46 of the GDPR's "appropriate safeguards", which guarantee subject rights and legal remedies[14].

The Court highlights the importance of national supervisory bodies with respect to protecting personal information, in line with GDPR Articles 51(1) and 57(1). It highlights that national authorities are in charge of ensuring that the norms specified in EU regulations are adhered to when personal data is transferred from the EU or European Economic Area (EEA) to other nations or international organizations[15] [16].

National supervisory authorities should be able to look into complaints and assess if transferred data conforms with GDPR rules even in situations where the European Commission has approved an adequacy judgment allowing the transfer of personal information[17] [18].

According to the CJEU, the Privacy Shield does not guarantee data subjects' rights that are enforceable and effective in the face of interference, as stated in the European Union's Charter of Fundamental Rights. The right to a fair trial and an effective remedy are guaranteed by this charter. Furthermore, the CJEU determined that, in accordance with Article 47 of the Charter, the Secretary of State's designated Privacy Shield ombudsperson is neither an autonomous entity nor a tribunal[19].

The CJEU concluded, in essence, that the USA does not offer a level of data protection that is effectively comparable to that of the European Union, as required by Article 45(1) of the GDPR, taking into account Articles 7, 8, and 47 of the Charter. These articles guarantee the right to efficient legal protection, respect for one's privacy and family life, and protection of one's personal data. As a result, the sufficiency ruling was overturned. In light of this, data transfers between the US and the EU must rely on extra precautions specified in EU Regulation Chapter V, namely Article 46(2), which outlines appropriate safeguards.

On June 4, 2021, the European Commission approved two sets of standard contractual agreements in reaction to the withdrawal of the Privacy Shield[20]. The purpose of these regulations is to make it easier for personal data to be transferred from the EU to third

13 CJEU, Schrems II, 2020, July 16, para. 65.

14 CJEU, Schrems II, 2020, July 16, paras. 91 and 92.

15 CJEU, Schrems II, 2020, July 16, para. 107 and case C-362/14, 2015, October 6, Schrems I, para. 47.

16 This perspective aligns with the Court's reasoning in the Schrems II case of 2020 and the Schrems I case of 2015, as well as insights presented by scholars such as Piroddi in 2021 and De Mozzi in 2022.

17 CJEU, Schrems II, 2020, July 16, para. 120.

18 This principle was upheld in the Schrems II case of 2020.

19 CJEU, Schrems II, 2020, July 16, para. 168.

20 Commission implementing decision of 4 June, Nos. 2021/914/UE and No. 2021/915/UE.

countries. These commercial agreements cover the requirements for personal data transfers in compliance with the ECJ's Schrems II case judgment, as well as provisions to accommodate the variable number of parties adhering to the contract (De Mozzi, 2021).

3.3. Transboundary transfer of data within the Eurasian economic union

Digital technologies present novel opportunities for customs authorities to enhance both the speed and quality of their decision-making processes. The next phase in advancing digital government administration is closely linked to data centralization. This involves structuring public governance, where decisions increasingly rely on objective data (Vovchenko et al., 2019).

Creating a common platform for digital data exchange and transmission is another essential component in digitizing the customs regulatory system in the EAEU, which is highlighted in its Cross-Border E-Trust Space along with the treaty of the organizations, particularly in its Art. 23.

Additionally, the Eurasian Economic Commission has laid the groundwork for a transnational takeover of the digital economy. This was made possible by the October 11, 2017, Supreme Eurasian Economic Council No. 12 decision, which approved the primary plans for implementing the digital agenda of the EAEU through 2025 (Kolodnyaya, 2018).

Even though the bulk of the aforementioned laws were passed within the EAEU, there are still a number of barriers that make a smoother transition for all of the union's members more challenging. The persistent problem, remaining as a major obstacle of regulating data circulation throughout the Union is a significant barrier to the implementation of the digital agenda. Many digital ecosystems planned for implementation involve cross-border data exchange in various interaction formats, including G2G, G2C, G2B, B2B, and B2C. However, numerous aspects of data circulation in the EAEU remain underdeveloped. Consequently, there is a lack of terminological consistency in key concepts related to data, and the regulation in the category of data is inadequately developed, lacking common approaches to the legal categorization of data and risk management in this domain. Legal matters stemming from cross-border data exchange have yet to be addressed. As a result, regulatory measures are lagging behind practical considerations, impeding progress in the digital agenda. The situation is further complicated by requirements outlined in the national legislations of EAEU Member States, particularly those concerning the localization of personal data. As a result, it is crucial to create and enact legislation as well as an appropriate data protection mechanism for cross-border data circulation inside the EAEU, comprising both non-personal and personal data (Mikhaliova, 2022).

The Union has been engaged in prolonged discussions regarding the development of an international agreement concerning data circulation and data protection. However, the process of aligning approaches and crafting such an agreement continues to be intricate and time-consuming.

Moreover, challenges in the realm of electronic document management persist. Consequently, there is a need for legislative enhancements and the formulation of shared

approaches in the domain of electronic signatures. The issue of mutually recognizing electronic signatures stands out as a prominent barrier to seamless trade, significantly complicating interactions with suppliers in the internal market of the EAEU and the procurement process. The effective utilization of the Union's digital infrastructure remains unattainable without the resolution of these legal gaps.

A more intricate obstacle to the realization of the digital agenda pertains to the issue of unequal digital advancement among the Member States of the Union (Filatova et al., 2018). To demonstrate this challenge, we can examine the performance of these Member States within the Networked Readiness Index.[21]

The World Economic Forum created the Networked Readiness Index in 2002 and now administered by the Portulans Institute and provides a measure of the degree of information and communication technology development in different nations. This index assumes a pivotal role in assessing a nation's technological and innovative capabilities and provides a valuable means for conducting comparative evaluations of ICT progress across states.

Concerning information and communication technology advancement within the EAEU region, there is a noticeable disparity. For example, in 2022, the ICT development gap between Russia and Kyrgyzstan was a substantial 45 points. Armenia, Belarus, and Kazakhstan have reached comparable levels of ICT development, but their disparities with Russia are also considerable. Currently, the focus is on enhancing the connectivity of government bodies in EAEU Member States, updating the integrated information system, and implementing secure and continuous electronic document management, which has mitigated this issue to some extent.

However, in the future, as the Union's digital initiatives directly impact the interests of the population, this digital divide could significantly impede the efficiency of project implementation. Additionally, the current digital initiatives rely on the pre-existing national services, and the varying levels of development in these services complicate the execution of collaborative projects (Bolgov & Karachay, 2016). To expedite the digital transformation of the Member States, it is imperative to intensify the international exchange of digital technology expertise and the expansion of best technological practices.

Crucially, the internal digital infrastructure of the Union, notably the integrated information system, has yet to be fully established. Additionally, the execution of several pivotal projects within the digital agenda is experiencing delays. The primary hindrances impeding the advancement of the Union's digital ecosystem include deficiencies in the legal framework, a lack of coherent conceptual alignment in the implementation of national digital economy strategies, and disparities in ICT development across the region.

In recent years, the EAEU-states have been actively establishing their respective national digital ecosystems. These efforts have spanned both the realm of public administration and the advancement of digital economies within their own borders. However, the progress

21 Network Readiness Index Homepage. https://networkreadinessindex.org

of the EAEU's digital agenda has not kept pace with the development of national digital ecosystems. The initial delays have created challenges in harmonizing collective approaches and strategies, ultimately resulting in a decrease in the number of proposed digital initiatives.

To effectively realize the goals and objectives outlined in the digital agenda, it is imperative to consolidate the endeavors of EAEU-states in the field of digital economic transformation. This consolidation should involve a more robust engagement of national competence centers and the enhancement of national digital infrastructures.

Conclusion

It is obvious, that currently the international community more than ever needs a regulatory coordination framework, which concerns transboundary transfer of data that come along with legal safeguards and can highlight security vulnerabilities, cybersecurity risks and jurisdictional complexities.

Harmonized standards are established when there is significant agreement between major countries, major powers and other international entities. Instead of being managed by local or exclusive organizations, these norms are expected to form a vast "regime complex" that is overseen by "universal" intergovernmental organizations. One good example of harmonized standards, as it was mentioned earlier, is the widespread use of the TCP/IP Internet protocol.

References

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference "Information Society: Governance, Ethics and Social Consequences", University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union's countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects

and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Kolodnyaya, G. (2018). Digital economy: features of development in Russia. Ekonomist, 4, 63–69. (In Russ.).

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Author information

Gulbakyt Bolatbekkyzy – PhD Candidate and Doctoral Scholar, School of Law, Wuhan University
Address: Luojia Hill, Wuhan, Hubei Province, 430072, China
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313-2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Conflicts of interest

The author 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 – February 2, 2024
Date of approval – March 1, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.15

Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления

Гульбакыт Болатбеккызы

Уханьский университет, Ухань, Китай

Ключевые слова

государственное управление,
защита данных,
кибербезопасность,
конфиденциальность,
персональные данные,
права человека,
право,
трансграничность,
цифровизация,
цифровые технологии

Аннотация

Цель: определить основные юридические факторы трансграничного обмена данными в контексте распространения цифровых технологий и цифровизации государственного управления, включая правовые гарантии, проблемы безопасности, риски кибербезопасности, подходы к регулированию и повышению эффективности управления данными в разных юрисдикциях.

Методы: исследование опирается на синтез и критический анализ различных аспектов заявленной проблемы, в том числе на анализ как первичных, так и вторичных источников. На примере сравнения политики регулирования Китая, США, ЕС и государств-членов ЕАЭС сопоставляются различные подходы относительно ограничения или поощрения свободной трансграничной передачи данных. Комплексный мета-анализ и оценка литературы позволили сформировать представление о методах, используемых для защиты данных в разных юрисдикциях, а также обозначить рамки и направления государственной политики, необходимые для эффективной передачи данных между юрисдикциями.

Результаты: выявлены основные проблемы, связанные с трансграничной передачей данных в контексте распространения цифровых технологий и цифровизации управления, такие как растущее неравенство в развитии цифровых технологий, правовая неопределенность, обеспечение конфиденциальности и кибербезопасности и др. Проанализированы правовые основы трансграничной передачи данных в контексте цифровизации государственного управления и практика их реализации, что способствовало поиску путей повышения эффективности управления в условиях транснациональной передачи данных, включая предоставление услуг, развитие открытости и участия общественности.

Научная новизна: на основе проведенного анализа подходов различных юрисдикций к проблемам юридического характера, вопросам обеспечения безопасности и суверенитета, обусловленным трансграничной передачей данных, выявлены роль и применимость международного права, а также уникальные вызовы, возникающие в государствах-членах Евразийского экономического союза на пути формирования трансграничного пространства доверия.

Практическая значимость: исследование указанных вопросов имеет значение для выработки и принятия взвешенных политико-правовых решений государственными структурами, прежде всего правительственными и законодательными органами, направленных на достижение баланса между доступностью данных и их безопасностью, между эффективностью государственного управления и соблюдением прав граждан. Полученные результаты будут иметь значение также для иных субъектов отношений, связанных с трансграничной передачей данных и вопросами регулирования указанных отношений.

Для цитирования

Болатбеккызы, Г. (2024). Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления. *Journal of Digital Technologies and Law*, *2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Список литературы

Колодняя Г. (2018). Цифровая экономика: особенности развития в России. *Экономист*, *4*, 63–69.

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference "Information Society: Governance, Ethics and Social Consequences", University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union's countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Информация об авторе

Болатбеккызы Гульбакыт – соискатель степени PhD, докторант, школа права, Уханьский университет
Адрес: 430072, Китай, провинция Хубэй, г. Ухань, Луоцзя Хилл
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313–2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Конфликт интересов

Автор сообщает 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: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 2 февраля 2024 г.
Дата одобрения после рецензирования – 1 марта 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:347.45/.47:339
EDN: https://elibrary.ru/zkuagz
DOI: https://doi.org/10.21202/jdtl.2024.16

Configuration of Incoterms into Smart Contracts: a View of International Sales Contracts through a Futuristic Periscope

Prince Fater Audu ✉
Ahmadu Bello University, Zaria, Nigeria

Fatima Shabih
Jamia Millia Islamia University, New Delhi, India

Keywords

blockchain technology,
contract,
decentralized finance (DeFi),
digital technologies,
digitalization,
Incoterms,
international law,
international trade,
law,
smart contract

Abstract

Objective: to identify the prospects of international trade in the light of synchronizing Incoterms with smart contracts.

Methods: the study is based on the general scientific methods of analysis, synthesis, comparison, and formal-legal method necessary to analyze the provisions of Incoterms.

Results: the authors analyzed the provisions of Incoterms and technological innovations in commercial law; showed the connection between the practice of commercial law and technological development due to the inclusion of contractual terms in blockchain. It is noted that the integration of blockchain technology with smart contracts has led to a variety of automated business transactions and the creation of a platform for synthetic assets trading. The authors describe the possibilities of secure and easy transactions in international trade using blockchain. Despite the uniqueness of this technology, its different types are distinguished, namely: public, private, hybrid, and consortium blockchain. It is substantiated that the synchronization of Incoterms with smart contracts can improve the prospects of international trade (especially export-import contracts). It is emphasized that smart contracts based on blockchain can revolutionize the application of Incoterms, consequently increasing the efficiency of transactions between parties to export-import relationships. One of the fundamental changes that smart contracts will bring to these trade transactions is the reduction of errors and misinterpretations of Incoterms. The authors use specific cases

✉ Corresponding author

to demonstrate disputes arising at the stages of transaction conclusion and execution, which could have been avoided using modern technologies.

Scientific novelty: The paper shows the phenomenon of synchronizing Incoterms with blockchain and how it can affect the form of contracts and facilitate their smooth execution. The proposed approach to analyzing the phenomenon takes into account the revolutionary innovations in cross-border trade, which are compared with the usual ways of applying Incoterms in traditional international trade contracts.

Practical significance: the research provides suggestions and recommendations for further development of innovations in the field of smart contracts, especially export-import trade contracts on a global scale.

For citation

Audu, P. F., & Shabin, F. (2024). Configuration of Incoterms into Smart Contracts: a View of International Sales Contracts through a Futuristic Periscope. *Journal of Digital Technologies and Law, 2*(2), 308–327. https://doi.org/10.21202/jdtl.2024.16

Contents

Introduction

The advent of digitalization in the kaleidoscope of scientific evolution is rapidly changing the traditional patterns of human endeavour, blowing off long-standing conventions and methods of doing things in the process. Even in the sphere of global commerce, so many revolutionary digital technologies have set the gears of change in motion. One of such unprecedented technological breakthroughs changing the narrative is the blockchain technology. It has created safe systems that provide security, data integrity, and anonymity in commercial transactions between parties, free from the control of a central repository or authority. This decentralized data management technology that became operational in 2008 as a catalyst for Bitcoin cryptocurrency has summoned the aura of future business

operations to the present. More so, this distributed software has heralded the vicissitudes of automated business transactions and has created a platform for smart contracts to thrive. The idea of incorporating the terms of a contract into series of blockchain has created a nexus between the practice of business law evolution and machines. The integration of blockchain technology with smart contracts will make the dream of a "peer-to-peer market" come true (Zibin Zheng et al., 2020). This form of digital contract is predicated on the automatic execution of terms that are embedded in series of blockchain, structured with predefined conditions, which, if met, activate the contract (Souei et al., 2023; Stojanović & Ivetić, 2020; Vatiero, 2022). Despite the nascence of smart contracts, the prospects of them eradicating certain shortcomings of "paper and pen" contracts are very high.

At the international front, trade transactions dealing with export contracts involving buyers and sellers have over time been subjected to certain regulations by the International Chamber of Commerce (ICC). These regulations which are known as International Commercial Terms (Incoterms) have been continuously employed to ease the implementation of international trade transactions as far back as 1936 (Coetzee, 2002). In order to be in the loop with prevailing circumstances looming along the horizon of global business, these terms are updated at intervals, of which the current version became operational in 2020. These Incoterms directs the course of transactions between parties in export/import trade transactions by defining their duties, rights, and responsibilities of contracting parties.

Adopting a futuristic disposition in the line of analysis, this paper explores the possibility of easing transactions in international trade safely and easily by reclining on the leverage of blockchain technology. Dwelling particularly on the Incoterms, this paper canvasses argument on how their synchronization into smart contracts can change the outlook of international trade (especially export/import contracts) for the better.

1. Basic concepts

1.1. Incoterms

International Commercial Terms, colloquially known by the short form "Incoterms" are universal terms that define transactions between importers and exporters. These are a set of rules/regulations established by the International Commercial Chamber (ICC) to ease the course of international sales transactions between parties by defining the various features associated with trade viz. risk involved, the rights and obligations of the parties, and transportation management between exporters and the importers. Although Incoterms are only formal procedures, they also apply as a contract language and law in export/import trade transactions (Davis & Vogt, 2022; Lim & En-Rong, 2021). Be that as it may, Incoterms do not automatically set in to commandeer the course of a transaction between parties. This is due to the fact that these terms are not mandatory, and can only come into effect when parties have them incorporated into the terms of their sales contract[1].

[1] Incoterms in International Trade. (2020, June 18). Aceris Law LLC. https://clck.ru/3BefKf

Incoterms were first introduced into the regulatory framework of international sales contracts in 1936 by the International Chamber of Commerce (ICC) to minimize misunderstandings in foreign trade contracts by clearly defining the rights and obligations of sellers and buyers. In order to conform to dynamic circumstances within the global business landscape, Incoterms are regularly updated[2]. The Incoterms 2020 are the version of Incoterms that are operational currently. The quest to promote an open international market and enhance global economic growth being the defining purpose of the International Chamber of Commerce (ICC) has been bolstered by Incoterms due to their instrumental role in enhancing seamless trade transactions across the globe.

Despite their mandatory nature, Incoterms have over time been incorporated into international trade to facilitate the smooth execution of export/import contracts between numerous parties across several nations of the world. Since 1936 when the first Incoterms were published, they have been revised several times – in 1953, 1967, 1976, 1980, 1990, and 2010, in order for them to meet the demands of changes looming across the global business landscape (Agaoglu, 2020). The Incoterms 2020 which replaced the Incoterms 2020 came into effect on the 1st of January, 2020, and is still the version that is globally in use currently[3]. The Incoterms 2020 has improved on the visible weaknesses of the 2010 version despite the absence of significant additions to the number of terms. The rules are updated and grouped into two categories that reflect transportation modes. Out of the 11 incoterms, seven are provisions of trade to be done in “any mode” and the other four are for the sale of goods via transportation on “land” or “sea” or “inland waterway”. They closely correspond with the U.N Convention on Contracts for International Sales of Goods.

For the importer, the most advantageous Incoterms in terms of favourable costs are the Delivered at Place (DAP), Delivered Duty Paid (DDP), and the Delivered At Terminal (DAT). While the exporter, the most advantageous Incoterms are the Ex Works (ExW), Free Carrier (FCA), Carriage Paid To (CPT), Free Alongside Ship (FAS), Free On Board (FOB), Carriage and Insurance Paid To (CIP), Cost and Freight (CFR), and Cost Insurance and Freight (CIF). “The choice of the most suitable Incoterms for an importer or exporter will depend on whether they want to control costs, contract the main transport, reduce risks or have greater security in the logistics chain”[4].

Unlike domestic trade policies, incoterms embrace a far-reaching applicability, and can be used by any country for trading internationally. By the virtue of its nature, they are not legally binding, hence, their explicit incorporation into an international sale of good contract is strictly at the discretion of the parties involved. Consequently, the

2 Troy Segal. (2023, December 22). Incoterms Explained: Definition, Examples, Rules, Pros & Cons. Investopedia. https://clck.ru/3BefPS

3 Ibid.

4 Incoterms: how to choose to import and export. (2022, September 11). Logisber. https://clck.ru/3BegEu

incorporation of incoterms in the contract does not set the provisions of contractual rights and obligations except in the matters of deliveries. They are not remedial in nature and do not carry solutions for breach of any contractual obligation.

1.2. Blockchain

Blockchain is a decentralized digital channel to record transactions between two parties. Unlike other transactions where there is an involvement of a third party organization to authenticate the transaction, blockchain works without any central authority or repository. More so, the immutable feature of blockchains makes it impossible for transactions stored on it to be tampered with or traced. Arguments abound that blockchain creates room for digitalized trust by enhancing certainty of execution and creation of efficiency through the removal of intermediaries and their concomitant costs (Durovic & Janssen, 2019).

The breakthrough for the establishment of blockchain technology was laid by Satoshi Nakamoto (the inventor of Bitcoin) when he published a paper on Bitcoin in the year 2008[5]. The paper titled "Bitcoin: A Peer-to-peer Electronic Cash System" described, inter alia, a systematic electronic means of payment of payment strictly based on cryptography[6]. Prior to this period, important steps were taken by scholars such as Stuart Haber, Scott Stornetta, David Chaum, and Adam Back who had published whitepapers centred on the creation of digital currencies anchored on cryptography[7]. Hence, the advent of Bitcoin marked the maturity of a digital currency revolution that had been brewing beneath the digital technology space for decades.

Generally, blockchains are distributed ledger systems maintained by individual nodes that form a record of all the transactions carried out within them (Papadouli & Papakonstantinou, 2023). As a result of their immutability, the information about every transaction available across the nodes on such ledgers creates a great amount of data integrity[8]. However, all the nodes are anonymous but their identifiers are not. This creates a transparency in the process and makes it more secure for the other nodes to comply and confirm transactions. Another advantage that blockchain technology holds is high resistance to any modification or alteration. Since it is a database of records, which are not tampered with nor deleted at any point in time, it is highly favourable in fields that require data security and scalability. Blockchain technology has today not only flourished in transactions concerning the digital trade of commodities or services, via cryptocurrencies alone, but is also gaining grounds in different fields of governance, finance, healthcare, utilities, and smart contracts. Its various implementations can be designed based on its functions and purposes in mind.

---

5 Sarmah, Sh. S. (2018). Understanding Blockchain Technology. Computer Science and Engineering, 8(2), 23–24.

6 Id. at 23.

7 Id. at 23.

8 Id. at 23.

It is pertinent to note that despite the general uniqueness of blockchain technology, blockchains belong to various categories. There are four categories of blockchain, namely: public blockchain, private blockchain, hybrid blockchain, and consortium blockchain. From these categories, public technology is the most decentralized one because it lacks any form of restrictions; hence, it can be accessed by anybody who has access to the internet[9]. Examples of public blockchain include Bitcoin and Ethereum. Private blockchain also works in a similar way as public blockchain, however, they operate with a sort of centralized database that grants access only to those users who are part of the network (Vijai et al., 2019). Good examples are Hyperledger and Corda. Hybrid blockchain as the name implies combines the features of both public and private blockchain where it is partially under the control of an organization while it is still projected as a public blockchain on the flipside[10]. Some known examples of hybrid blockchain are Ripple network and XRP Token. The structure of a consortium blockchain revolves around a handful of organizations whose pioneering assigned users define the process of its operations (Vijai et al., 2019). Some examples of consortium blockchain include Multichain and Tendermint. Be it as it may that these categories of blockchain technology vary along certain lines, it is still a fact that all of them operate on decentralized software system that processes transactions across a broad-range of computers in such a way that no alteration, hacking, or cheating is possible.

1.3. Smart contract

"Smart contract" is a term used to describe computer codes that automatically execute all or parts of an agreement stored on a blockchain-based platform[11]. This unprecedented form of contract stands out from all other forms because its terms are automatically executed (Huang et al., 2024). The automatic execution of smart contracts is facilitated by their attachment to blockchain, which works by automating value transfer when certain predefined conditions are met by parties. Due to the efficient execution of terms in a smart contract, its defining nature is considered to be effective in the reduction of transaction and legal costs, risks, and other forms of inefficiencies commonly associated with conventional forms of contract (Zibin Zheng et al., 2020). Smart contracts work by storing, replicating, and updating the transactions in an agreement on blockchains (Dixit et al., 2022; Detwal et al., 2023). The codes containing the content of an agreement in smart contracts are decentralized across a blockchain network, hence, making transactions carried out on them free from any form of repository censorship and prying eyes of a third party.

---

9 GEEKSFORGEEKS. https://clck.ru/3Beg9Y

10 Ibid.

11 Levi, S., & Lipton, A. (2018, May 26). An Introduction to Smart Contracts and their Potential and Inherent Limitations, Harvard Law School Forum on Corporate Governance. https://clck.ru/3BegAy

Smart contracts first came into light through Nick Szabo in 1994, who conceived the idea of a digital realm where synthetic assets could be traded using computerized contracts embedded into distributed ledgers[12]. Since 1994 when Nick Szabo first brought forth the idea of smart contract, knowledge of its revolutionary functionalities has been gradually sweeping across the world. In recent years, the business world is gradually getting absorbed in its dogma (Ante, 2021; Chu et al., 2023). Describing this unprecedented form of contract, Nick Szabo defined smart contracts as "computerized transaction protocols that execute terms of a contract" (Szabo, 1996). This brief description clearly distinguishes smart contracts from conventional contracts due to their unique functionalities and features. The concept is based on the idea of translating the contractual clauses related to various provisions, for example, that of collateral, lien, or bonding, into codes which are to be embedded in property such as a hardware or a software which can self-enforce them (Eenmaa & Schmidt-Kessen, 2019; Ferro et al., 2023). This would terminate the need of any trusted intermediary as a third party organization. The code can be a mere manifestation of the contract or a traditional fully drafted contract. It leverages the blockchain technology. The code is deployed using cryptographically signed transactions on a blockchain. The codes are replicated via the multiple nodes registered on the blockchain and are therefore safe from any modification or deletion. The users of the blockchain where the code is registered can create transactions, while the blockchain saves the data in the database and sends it to public functions offered by a smart contract[13].

From a strict legal perspective, it has been argued that smart contracts are neither legal contracts in the traditional sense nor are they smart; the term is therefore a misnomer. A broad range of argument have spanned the spectrum of thoughts as regards the legal enforceability of smart contracts in the same way as conventional contracts. It is argued that smart contracts will improve the instantiation of the contract conditions through the digitalization of the enforcement process by automatically enforcing the terms by way of responding to the fulfilment of conditional statements embedded in the blockchain; hence, they obviate the need for a third party, i.e. a judge, to enforce the terms (Raskin, 2017). On the other hand, it is argued that smart contracts do not fulfil all the universal conditions defining the existence of a contract; hence, in the occurrence of certain eventualities, the essence of indulging in such contracts will be defeated by the peculiarities of the blockchain technology[14]. Whichever lane of thought one toes, it is without an unmistakable ring of truth that smart contracts are a pre-emptive form

12 Frankein, J. (2022, August 30). Smart Contracts. Investopedia. https://clck.ru/3BegCJ

13 Mell, P. M., Kelsey, J. M., & Shook, J. (2022, August 30). Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness. NIST. https://clck.ru/3BegDG

14 O'Connell, J. (2019, December 19). The Trouble with Smart Contracts. Mayo Wyne Baxter Solicitors. https://clck.ru/3BegGR

of contact that will sweep the world in due time, while creating an intersection between the law and technology. Since smart contracts and blockchain technology are still in the stage of nascence, we should wait and see how the legal systems across the world will handle these agreements in terms of taxation and other laws.

2. Smart contracts and decentralized finance: a leverage for trading synthetic assets

One of the most celebrated relevances of blockchain technology is the installation of decentralized platforms over which financial services like those of a bank or any financial institution are provided. The trade happening on these networks employs synthetic assets, which are tokenized derivatives of an underlying asset. Crypto-currency based synthetic assets are the ones that possess the value of the derivative without needing to hold the underlying asset. They offer users all the benefits of decentralization of their investments, as they are open and available to all the users across the world by the means of smart contract. The decentralized platform on which these synthetic assets are traded is known as Decentralized Finance (DeFi). It is a blockchain-based financial infrastructure that refers to an open, permissionless, and highly functional protocol stack built on public smart contract platforms. Reports have it that the assets on Defi protocols as of September 2021 were worth US$92 billion[15].

The DeFi works on a multi-layered system. Every layer in the architecture performs a distinct function. The layers build on each other and create an open and highly composable infrastructure that allows everyone to build on, rehash, or use other parts of the stack. The first layer is the settlement layer. It consists of the blockchain and the native protocol assets. For the ownership information to be stored securely, it is done on the settlement layer and any state changes are to be in accordance with its ruleset. It serves as a settlement and dispute resolution layer making the blockchain a foundation for trustless execution. The second layer is the asset layer, which consists of all the assets issued on the settlement layer. Standardized smart contracts are used to construct base assets in the asset layer as a fundamental financial operation. It includes all the native protocol assets as well as those assets that are additional and are issued on the blockchain. The third layer is the protocol layer where standards are provided for certain use cases like decentralised exchanges, debt markets, derivatives, and on-chain asset management. Any user can access these standards, which are often implemented as a collection of smart contracts (or DeFi application). These protocols are therefore very interoperable. The fourth layer is the application layer. In this layer, the assets serve as the foundation of the increasingly sophisticated financial products. Here, DeFi applications are implemented as complex smart contracts which enable deterministic execution of supplied business logic.

[15] McDonald, E. (2021, November 5). Smart Contracts. Columbia Business Law Review. https://clck.ru/3BegHv

The interaction is powered by web browser-based front end, which makes the protocols easier to use. The applications implemented are user-oriented for easy connection to the individual protocols. The fifth layer is the aggregation layer. The DeFi applications provide a range of various financial services that are user-friendly and transparent making them attractive for use. All kinds of activities like trading, lending, insurance services and asset management can become easy with the use of DeFi. The rate and the comparison of the services for the purpose of these activities across the ecosystem are well managed by the aggregation layer. The aggregators provide user-centric platforms to connect to several applications and protocols. This provides tools that can help in comparing the services and determining the rates and perform complex task by connecting to several protocols simultaneously. Finally, these user-friendly applications combine and concise the data to build a service similar to banking applications.

3. Redefining international trade contracts: synchronization of law with blockchain technology

Over a long stretch of time, the course of export and import trade has been defined by different versions of International Commercial Terms (Incoterms) formulated by the International Chamber of Commerce (ICC). These Incoterms enhance the transactions between parties by properly defining their roles, duties, responsibilities, and risk transfer in the course of the transactions. It is without a doubt that Incoterms have played an instrumental role in facilitating the execution process of international trade transactions involving buyers and sellers. On the other hand, it is also true that the functionalities of Incoterms have umpteen times failed to shelve transactions from latent circumstances capable of distorting the smooth sail of such international trade transactions (Petrová et al., 2021). These drawbacks are in themselves intrinsic parts of the complex and dispute-prone nature of export and import trade transactions. While a good number of these sabotaging factors are occasioned by frustrating factors beyond the control of the parties, others are manifestations of weaknesses in the contract execution process. Despite the regular revision of Incoterms to suit the contemporary global business climate, putting such drawbacks in reins have not been entirely successful. It is to this end that smart contracts suffice to hem every loose edge using blockchain technology.

Generally, the adoption of smart contracts in international trade would eliminate intermediary intervention, reduce costs, enhance security of transactions, and facilitate transparency in the process (Belú, 2019). The automated execution process of smart contracts is capable of absorbing parties of hitches that can be identified with the current mode by which incoterms are implemented. Despite the significant improvements made in the latest operational version of Incoterms (Incoterms 2020) in response to dynamics such as intermodal complexities, e-commerce, and service proliferation in international trade, the difficulties concomitant with the implementation of these amendments still loom over the horizon. This spectrum of challenges surrounding the implementation

of Incoterms can be totally absorbed by smart contracts. Smart contracts, enabled by the blockchain technology, can be employed in the realm of international trade to drive efficiency and reduce friction along the lines of identity verification, ownership proof, cost reduction, and other logistical issues.

The process of configuring Incoterms into a smart contract will ease the execution of an export-import trade for both parties involved. The advantages of this synchronization will not just ease the execution process alone, but will also guarantee the credibility of the transactional mechanism.

One fundamental difference that smart contracts will make in export/import trade transactions lies in the aspect of reducing errors and misinterpretations of the Incoterms Rules. This is best explained in reference to the complex nature of export/import contracts, which are normally fraught with a lot of terms that are quite cumbersome to understand. The assimilation of smart contracts will not only simplify the transaction mechanism (Belú, 2019), but will also ease the logistics. The scope of an export/import operation involves so many people, protocols, and logistics. As a result of the lengthy procedures and intermediaries that are involved in the export/import transactions, firms or individuals involved in it end up getting frustrated. More so, firms dealing with time sensitive products even end up defeated in the pursuit of their goals[16].

This issue of logistics and protracted protocols reposes a more profound effect on traders in developing nations. A good example of an international sales contract that got entangled in a lot of legal controversy as a result of complicated logistics of export/import trade is the dispute that ensued between Pharmaplast (an Egyptian shareholding company in Alexandria), a manufacturer of care products, and Urica, a California-based corporation, that imports and distributes wound care products. Through the reliance on the role of URI (a limited liability company) as a third party handling the execution process, they entered into a contract (an exclusivity agreement) on the 10th of February, 2004. The contract terms stated that Pharmaplast would supply Urica with wound care products through URI for the span of ten years, to be distributed in the United States. In the course of following the agreement terms, series of issues arose due to the misinterpretation of certain terms, hence giving rise to a law suit[17] that protracted for many years, sweeping many persons along as parties. Disputes akin to this case abound in international sale of goods contracts. However, the adoption of smart contracts will eradicate such difficulties and reduce the chances of international sales transactions ending up in disputes. Smart contracts operate based on the protocol of "if this..., then that" (Lasmoles & Diallo, 2022). Hence, if the terms of international trade contracts (especially export/import contracts) are programmed based on this "precondition" and "execution" protocol across series of blockchains

16 Nordas, H. K., Pinali, E., & Grosso, M. G. (2006). Logistics and Time as a Trade Barrier. OECD Yrade Policy Working Papers, 35, 1, 4.

17 Urica, Inc. v. Pharmaplast SAE, CV 11-02476 MM (RZx).

that allows self-execution, then the number of misinterpretation incidents in the course of execution will be reduced.

On another note, smart contracts are capable of easing the documentation of export/import contracts. It is a known fact that the paperwork, transactional agreements, and correspondence between contracting parties as well as intermediaries is cumbersome. "In international trade, the number of documents required and the nature of the documentation will vary greatly depending on the underlying contract (e.g. sales contract), the nature of the goods, the value of the cargo, the complexity of the export sale, the shipment/transport required and the rules, restrictions and trade agreements of the countries concerned" (Sang Man Kim, 2021). However, the constant factor remains that these documents are normally bulky, and sometimes too complex to work on within a short time.

The bulkiness of contracts alone makes it difficult for some parties to fully understand the terms of such contracts, talk more of their execution process. In an export/import transaction, the elaborate paperwork documenting several Incoterms to control the entire process of execution span across several intermediaries, each with its own indispensable role. These documents are: documents issued by the importer, the exporter, by the authorities, bank documents, and documents issued by the carrier (Belú, 2019). All the aforementioned series of documents play instrumental roles in the formulation and execution of a typical import/export transaction. In the course of sorting out this long chain of documents, some contracts end up being discharged by frustration. It is to the above end that smart contracts suffices as the best way to cut down the lengthy correspondence between contracting parties, and with intermediaries. Since smart contracts work automatically by executing incorporated terms when certain conditions are met, then the incorporation of all conditions and Incoterms applicable in international sales contracts into series of blockchains will eradicate the delays and issues that comes with conventional manual documentation.

Another aspect that the synchronization of Incoterms into smart contracts will prove effective is in the process of making payments in the course of international trade. Conventionally, the process of payment in international trade transactions is fraught with a lot of risks; hence, parties are very meticulous and careful with the payment methods. Commonly, importers make payments after goods are received[18]. Invariably, the most secured payment method for the importer is most likely the least secure for the exporter and vice versa. The known methods of payment in international trade contracts are: Cash in advance, letter of credit, documentary collection, open account terms, the consignment and trade finance (Sang Man Kim, 2021).

[18] Djon Ly, 5 Common Payment Methods and Terms for International Trade. Statrys, (September 11, 2022, 1: 15 PM WAT). https://clck.ru/3BegmU

It is not uncommon for disputes to spring up at this point in a transaction. A good example of things going wrong in the course of an international trade transaction is in the case of Comptoird'Achar v. Luis de Ridder[19] where rye sold by Argentine sellers to some Belgian buyers under Cost Insurance and Freight (CIF) Incoterms failed to reach the latter despite the full payment of all fees. This transaction resulted in a lot of dispute snowballing into the courtroom when the buyers requested for a refund. This kind of incidents could have been avoided if the entire agreement terms were smartly done by encoding them into series of blockchains that will automatically disburse the funds when the terms have all been fulfilled. Smart contracts can regulate transaction payments through one of this linkage clause types – conditional effective type, contract joint type, and contract link type[20]. However, in the case of international trade transactions, the conditional effective type is the most suitable. In it, money can only be transferred when certain predefined conditions are met[21]. With this secured method of payment, the insecurities of all parties in a transaction will be allayed and the extra costs incurred in the process of making payment through traditional methods will be obviated, hence, facilitating smooth transactions.

4. Transformation of international trade: on the renovated technological configuration of Incoterms

Today, smart contracts are a prototypical example of Amara's Law, the concept articulated by Stanford University computer scientist Roy Amara that we tend to overestimate new technology in the short run and underestimate it in the long run[22]. Although smart contracts are still nascent, they have the potential of revolutionizing the reward structure and incentive system that will define the state of contracting parties in time to come. While it is true that they are yet to fully evolve to carry out complex commercial transactions, experts are optimistic about their potential to change the nature of business transactions entirely[23].

In international trade transactions, smart contracts do not just have the potential to minimize the level of risks involved, but can also create the platform for people across continents to engage in trade without having to go through the long correspondences that ensue before the execution of contract terms begins. In the aspect of risk management,

19 Comptoird'Achar v. Luis de Ridder, (1949) 1 ALL E.R. 26.

20 Xinyuan Ge. (2021). Smart Payment Contract Mechanism Based on Blockchain Smart Contract Mechanism. Scientific Programming, 2021. https://doi.org/10.1155/2021/3988070

21 Weber, I., & Staples, M. (2021). Programmable Money: Next-Generation Conditional Payments Using Blockchain. Proceedings of the 11th International Conference on Cloud Computing and Services Science (Vol. 1, pp. 7–14). https://doi.org/10.5220/0010535800070014

22 Levi, S., & Lipton, A. (2018, May 26). An Introduction to Smart Contracts and their Potential and Inherent Limitations, Harvard Law School Forum on Corporate Governance. https://clck.ru/3Begbw

23 McDonald, E. (2021, November 5). Smart Contracts. Columbia Business Law Review. https://clck.ru/3BegTr

the insurance industry could also leverage on smart contracts to create premium packages that pay out in the event of unfortunate eventualities, without the hassle of navigating through a prolonged and costly claim validation process[24].

Even supply chains could also be managed by smart contracts. Smart contracts have the potential of getting rid of factors that tend to strain the efficiency of supply chains in international trade – the issue of trust and coordination[25]. The solution that smart contracts can provide to attend to the issue of trust and coordination along international supply chains includes developing, at an affordable management cost, a control system that can direct the supply chain's overall goals in order to achieve a greater common good medium-term as opposed to the current situation where each participant pursues, on its own behalf, lower but immediate returns. Acting as an enabling technology, smart contracts will redefine supply chain management in international trade by occasioning an increased collaboration between international actors across supply chains, which, by extension, will enhance the economic health of participating businesses.

With all the amazing prospects that smart contracts hold, their manifestation cannot take place in vacuum. Certain frameworks and regulations need to be put in place before the vast benefits of smart contracts can be brought into fruition. It is in view of this fact that we recommend the following measures that would enhance a global economic environment where smart contracts can thrive.

Amendment of Incoterms. Smart contracts in the domain of international trade will gain more reception if the International chamber of Commerce (ICC) should amend the Incoterms and empower it as a medium of framing export/import contracts. The formulation of an international legal framework will validate smart contracts as a safer method of framing trade contracts where parties have more control over the pulse of the transaction. This formal acknowledgement of smart contracts will create a favourable business climate for its evolution within the space of international trade.

Creation of a global export/import trade oracle. "Smart contracts cannot directly take input data from (sic) the real world, they must get that data from sources already on the Blockchain"[26]. It is to this end that oracles come into play. An oracle is the bridge linking off-chain information and on-chain information[27]. It serves as an on-chain Application Programming Interface (API) that parties to a smart contract can query for certain information. The role of oracles in smart contracts is to facilitate complex real-life activities such as finding data online –stock prices, temperature data, insurance, price reports, et cetera.

---

24 Ibid.

25 Bottoni, P., Gessa, N., Massa, G., Pareschi, P., Hesham, S., & Archuri, E. (2020, November 26). Intelligent Smart Contracts for Innovative Supply Chain Management. Frontiers in Blockchain. https://doi.org/10.3389/fbloc.2020.535787

26 McDonald, E. (2021, November 5). Smart Contracts. Columbia Business Law Review. https://clck.ru/3BegTr

27 Mojtahedi Arshia. A Guide to Oracles: What Are They, Types and Use Cases, AI Multiple, (12 September 2022, 2: 12 PM).

Considering the important role of oracles as a catalyst for smart contracts, the creation of a special system of oracles strictly for the propagation of export/import trade contracts will lay a solid foundation for the growth of smart contracts in the realm of international trade. The creation of this system of oracles will enable contracting parties to insert Incoterms of their choice in their contracts on series of blockchains, and would still be able to perform other functions that are rationed amongst intermediaries.

Conclusion

Smart contract is a revolutionary concept that will change the landscape of the corporate world. Its features will remedy the flaws and shortcomings of traditional contracts. In the same vein, smart contracts will eradicate the systemic difficulties concomitant with the reliance on third parties in the process of contract execution. In the domain of international trade, the prevalence of smart contracts will not just ease the course of transactions alone, but will also reset the pulse of international trade transactions by giving contracting parties more control over their object of contract. Unlike traditional international trade contracts that are fraught with the far-reaching interference of third parties acting in different capacities, smart contracts synthesize the roles of third parties into series of blockchains that operate based on the agreed terms of the parties, encoded in them.

Hemming loose edges that are common in traditional contracts, the reliance on smart contracts will not just fasten the execution process of international trade contracts, but it will also allay the fears of being outsmarted in a transaction. Given the porous nature of international trade contracts, smart contracts will suffice to facilitate certainty in the agreement execution, thsu easing the process of doing business worldwide. Therefore, in order to enhance more efficiency in the world of trade and business, an updated technology-friendly configuration of Incoterms can take us to new heights of developments.

References

Agaoglu, C. (2020). Incoterms. *Public and Private International Law Bulletin*, *40*(2), 1113–1149. https://doi.org/10.26650/ppil.2020.40.2.0008

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Belú, M. G. (2019). Application of Blockchain in International Trade: An Overview. *The Romanian Economic Journal*, *22*(71), 2–15.

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*, 107221. https://doi.org/10.1016/j.infsof.2023.107221

Coetzee, J. (2002). Incoterms: Development and Legal Nature – A Brief Overview. *Stellenbosch Law Review*, *13*, 115.

Davis, J., & Vogt, J. (2022). Incoterms® 2020 and Missed Opportunities for the Next Version. *International Journal of Logistics Research and Applications*, *25*(9), 1263–1286. https://doi.org/10.1080/13675567.2021.1897974

Detwal, P. K., Soni, G., Jakhar, S. K., Srivastava, D., Madaan, J., & Kayıkçı, Y. (2023). Machine learning-based technique for predicting vendor incoterm (contract) in global omnichannel pharmaceutical supply chain. *Journal of Business Research*, *158*, 113688. https://doi.org/10.1016/j.jbusres.2023.113688

Dixit, A., Deval, V., Dwivedi, V., Norta, A., & Draheim, D. (2022). Towards user-centered and legally relevant smart-contract development: A systematic literature review. *Journal of Industrial Information Integration*, *26*, 100314. https://doi.org/10.1016/j.jii.2021.100314

Durovic, M., & Janssen, A. (2019). The Formation of Blockchain-based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, *6*, 753–772. https://doi.org/10.54648/erpl2018053

Eenmaa, H., & Schmidt-Kessen, M. J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Giacomo Corrias, Moncada, R., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Huang, H., Guo, L., Zhao, L., Wang, H., Xu, C., & Jiang, S. (2024). Effective combining source code and opcode for accurate vulnerability detection of smart contracts in edge AI systems. *Applied Soft Computing*, *158*, 111556. https://doi.org/10.1016/j.asoc.2024.111556

Lasmoles, O., & Diallo, M. (2022). Impacts of Blockchains on International Maritime Trade. J*ournal of Innovation Economics & Management*, *1*(37), 91–116. https://doi.org/10.3917/jie.pr1.0114

Lim, A. G., & En-Rong, P. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Petrová, M., Krügerová, M., & Koziel, M. (2021). Incoterms – History and Future Development. *Proceedings of the 15th International conference liberec economic forum* (pp. 589–590).

Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(2), 306–315.

Sang Man Kim. (2021). *Payment methods and finance for international trade*. Springer.

Souei, W. B. S., Hog, C. E., Djemaa, R. B., Sliman, L., & Amous, I. (2023). Towards smart contract distributed directory based on the uniform description language. *Journal of Computer Languages*, *77*, 101225. https://doi.org/10.1016/j.cola.2023.101225

Stojanović, Đ., & Ivetić, J. (2020). Possibilities of using Incoterms clauses in a country logistics performance assessment and benchmarking. *Transport Policy*, *98*, 217–228. https://doi.org/10.1016/j.tranpol.2020.03.012

Szabo, N. (1996). Smart contracts: building blocks for digital markets. E*XTROPY: The Journal of Transhumanist Thought*, *16*, 18–20.

Vatiero, M. (2022). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Vijai, C., Elayaraja, M., Suriyalakshmi, S. M., & Joyce, D. (2019). The Blockchain Technology and Modern Ledgers Through Blockchain Accounting. *Adalya Journal*, *8*(12), 545–557.

Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, & Muhammad Imran (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Authors information

Prince Fater Audu – Bachelor of Law, Faculty of Law, Ahmadu Bello University
Address: 810107, Kongo Campus, Zaria, Nigeria
E-mail: pfateraudu@gmail.com
ORCID ID: https://orcid.org/0009-0000-8289-3081

Fatima Shabih – Bachelor in Arts and Law, Faculty of Law, Jamia Millia Islamia University
Address: 110025, Jamia Nagar, New Delhi, India
E-mail: Shabihfatima010@gmail.com
ORCID ID: https://orcid.org/0000-0003-1661-232X

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 – November 18, 2023
Date of approval – December 14, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:347.45/.47:339
EDN: https://elibrary.ru/zkuagz
DOI: https://doi.org/10.21202/jdtl.2024.16

Применение смарт-контрактов в сфере международной торговли и перспективы дальнейшей эволюции Инкотермс

Принс Фатер Ауду ✉

Университет Ахмаду Белло, Зария, Нигерия

Фатима Шабих

Университет Джамия-Миллия-Исламия, Нью-Дели, Индия

Ключевые слова

децентрализованные финансы (DeFi),
Инкотермс,
контракт,
международная торговля,
международное право,
право,
смарт-контракт,
технология блокчейна,
цифровизация,
цифровые технологии

Аннотация

Цель: выявить перспективы международной торговли в свете синхронизации положений Инкотермс со смарт-контрактами.

Методы: в основе исследования лежат общенаучные методы анализа, синтеза, сравнения, а также формально-юридический метод, необходимый для анализа положений Инкотермс.

Результаты: авторами проанализированы положения Инкотермс и технологические новации в торговом праве; показана связь между практикой торгового права и технологическим развитием, обусловленная включением условий договора в блокчейн. Отмечается, что интеграция технологии блокчейн со смарт-контрактами привела к разнообразию автоматизированных бизнес-транзакций и созданию платформы для торговли синтетическими активами. Раскрыты возможности безопасного и простого осуществления сделок в международной торговле с помощью технологии блокчейн. Несмотря на уникальность данной технологии, выделяются различные ее виды, а именно: публичный, частный, гибридный и консорциумный блокчейн. Обосновано, что синхронизация положений Инкотермс со смарт-контрактами может изменить перспективы международной торговли (особенно экспортно-импортных контрактов) в лучшую сторону. Подчеркивается, что на основе технологии блокчейн смарт-контракты могут произвести революцию в применении Инкотермс, и, как следствие, повысить эффективность транзакций между сторонами экспортно-импортных отношений. Одно из фундаментальных изменений, которое смарт-контракты внесут в данные торговые операции, заключается в сокращении количества ошибок и неправильного толкования правил Инкотермс.

✉ Контактное лицо

Авторы на конкретных случаях демонстрируют возникающие на этапе заключения сделки и ее исполнения споры, которые можно было бы избежать посредством использования современных технологий.

Научная новизна: показаны феномен синхронизации Инкотермс с технологией блокчейн и то, как это может повлиять на форму контрактов и способствовать их беспрепятственному исполнению. Предложенный подход к анализу феномена учитывает революционные инновации в трансграничной торговле, которые сравниваются с обычными способами применения Инкотермс в традиционных международных торговых контрактах.

Практическая значимость: проведенное исследование содержит предложения и рекомендации для дальнейшего развития инноваций в области смарт-контрактов, особенно экспортно-импортных торговых контрактов в глобальном масштабе.

Для цитирования

Ауду, П. Ф., Шабих, Ф. (2024). Применение смарт-контрактов в сфере международной торговли и перспективы дальнейшей эволюции Инкотермс. *Journal of Digital Technologies and Law*, *2*(2), 308–327. https://doi.org/10.21202/jdtl.2024.16

Список литературы

Agaoglu, C. (2020). Incoterms. *Public and Private International Law Bulletin*, *40*(2), 1113–1149. https://doi.org/10.26650/ppil.2020.40.2.0008

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Belú, M. G. (2019). Application of Blockchain in International Trade: An Overview. *The Romanian Economic Journal*, *22*(71), 2–15.

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*, 107221. https://doi.org/10.1016/j.infsof.2023.107221

Coetzee, J. (2002). Incoterms: Development and Legal Nature – A Brief Overview. *Stellenbosch Law Review*, *13*, 115.

Davis, J., & Vogt, J. (2022). Incoterms® 2020 and Missed Opportunities for the Next Version. *International Journal of Logistics Research and Applications*, *25*(9), 1263–1286. https://doi.org/10.1080/13675567.2021.1897974

Detwal, P. K., Soni, G., Jakhar, S. K., Srivastava, D., Madaan, J., & Kayıkçı, Y. (2023). Machine learning-based technique for predicting vendor incoterm (contract) in global omnichannel pharmaceutical supply chain. *Journal of Business Research*, *158*, 113688. https://doi.org/10.1016/j.jbusres.2023.113688

Dixit, A., Deval, V., Dwivedi, V., Norta, A., & Draheim, D. (2022). Towards user-centered and legally relevant smart-contract development: A systematic literature review. *Journal of Industrial Information Integration*, *26*, 100314. https://doi.org/10.1016/j.jii.2021.100314

Durovic, M., & Janssen, A. (2019). The Formation of Blockchain-based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, *6*, 753–772. https://doi.org/10.54648/erpl2018053

Eenmaa, H., & Schmidt-Kessen, M. J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Giacomo Corrias, Moncada, R., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Huang, H., Guo, L., Zhao, L., Wang, H., Xu, C., & Jiang, S. (2024). Effective combining source code and opcode for accurate vulnerability detection of smart contracts in edge AI systems. *Applied Soft Computing*, *158*, 111556. https://doi.org/10.1016/j.asoc.2024.111556

Lasmoles, O., & Diallo, M. (2022). Impacts of Blockchains on International Maritime Trade. J*ournal of Innovation Economics & Management*, *1*(37), 91–116. https://doi.org/10.3917/jie.pr1.0114

Lim, A. G., & En-Rong, P. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Petrová, M., Krügerová, M., & Koziel, M. (2021). Incoterms – History and Future Development. *Proceedings of the 15th International conference liberec economic forum* (pp. 589–590).

Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(2), 306–315.

Sang Man Kim. (2021). *Payment methods and finance for international trade*. Springer.

Souei, W. B. S., Hog, C. E., Djemaa, R. B., Sliman, L., & Amous, I. (2023). Towards smart contract distributed directory based on the uniform description language. *Journal of Computer Languages*, *77*, 101225. https://doi.org/10.1016/j.cola.2023.101225

Stojanović, Đ., & Ivetić, J. (2020). Possibilities of using Incoterms clauses in a country logistics performance assessment and benchmarking. *Transport Policy*, *98*, 217–228. https://doi.org/10.1016/j.tranpol.2020.03.012

Szabo, N. (1996). Smart contracts: building blocks for digital markets. E*XTROPY: The Journal of Transhumanist Thought*, *16*, 18–20.

Vatiero, M. (2022). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Vijai, C., Elayaraja, M., Suriyalakshmi, S. M., & Joyce, D. (2019). The Blockchain Technology and Modern Ledgers Through Blockchain Accounting. *Adalya Journal*, *8*(12), 545–557.

Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, & Muhammad Imran (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Сведения об авторах

Ауду Принс Фатер – бакалавр права, юридический факультет, Университет Ахмаду Белло
Адрес: Нигерия, Зария 810107, кампус Конго
E-mail: pfateraudu@gmail.com
ORCID ID: https://orcid.org/0009-0000-8289-3081

Шабих Фатима – бакалавр права и гуманитарных наук, юридический факультет, Университет Джамия-Миллия-Исламия
Адрес: Индия, Нью-Дели 110025, Джамия Нагар
E-mail: Shabihfatima010@gmail.com
ORCID ID: https://orcid.org/0000-0003-1661-232X

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 – 18 ноября 2023 г.
Дата одобрения после рецензирования – 14 декабря 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

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

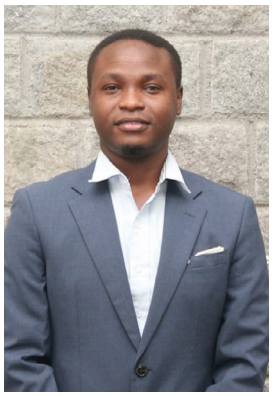
Torrubia, A., Mora, F. J., & Marti, L. (2001). Cryptography Regulations for E-commerce and Digital Rights Management. *Computers & Security*, *20*(8), 724–738. https://doi.org/10.1016/s0167-4048(01)00814-8

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.

Research article
UDC 34:004:347.21:004.4
EDN: https://elibrary.ru/uxqado
DOI: https://doi.org/10.21202/jdtl.2024.18

Experience of Legal Regulation of Lootboxes in Different Countries: a Comparative Analysis

Seppy Pour
Kun Consulting Group, Sydney, Australia

Keywords

comparative legal studies,
consumer protection,
digital technologies,
gambling,
gaming industry,
law,
licensing,
Loot box,
video games,
virtual goods

Abstract

Objective: to show how the use of a new business model called Loot boxes, on which modern video games are based, has become a legal problem for jurisdictions in different countries.

Methods: drawing on existing literature and contemporary sources, the article explores the potential negative consequences of Loot boxes, provides a comprehensive analysis of existing or proposed regulation, and compares the approaches taken in various national jurisdictions.

Results: the article examines the growing concern surrounding the widespread use of a particular form of in-game purchases called Loot boxes. It is strongly criticized on the grounds that Loot boxes are presumed to be a form of gambling within a video game. On this basis, this article argues in favor of their legislative regulation. Having examined the regulatory framework in countries that have already taken action against the use of Loot boxes, such as Belgium, the Netherlands, China, Japan and the Republic of Korea, as well as in countries currently debating their regulation, the author emphasizes the need to adopt consumer protection measures in the gaming industry. This is particularly relevant for vulnerable strata exposed to gambling-related harms. In addition, there is a need to ensure the ethical and responsible use of Loot boxes, as well as to reduce the health and financial risks associated with the use of this business model.

Scientific novelty: the paper presents a comparative study of the problems of current or projected social regulation of Loot boxes in video games. The author proposes to seek the solution in a balance between game industry innovations, consumer protection and user well-being, which will ultimately contribute to the creation of a healthier environment for gamers.

Practical significance: the study highlights the international scope of the problem the difference in legal and ethical regulatory measures taken in different countries to address the psychological, social and financial consequences associated with the proliferation of lootboxes in video games. These measures are yet to be assessed, taking into account the findings concerning the gaming industry.

For citation

Pour, S. (2024). Experience of Legal Regulation of Lootboxes in Different Countries: a Comparative Analysis. *Journal of Digital Technologies and Law*, *2*(2), 345–371. https://doi.org/10.21202/jdtl.2024.18

Contents

Introduction

Over 3 billion people play video games[1]. With this number expected to reach 3.6 billion by 2025, the video game industry stands to increase in market value to a purported $211.2 billion[2]. This value is in part derived through 'microtransactions', a business model which allows users to purchase virtual goods in video games or other in-game advantages with real life currency. Loot boxes are one such virtual good which can be purchased via a microtransaction.

Loot boxes (also referred to as loot crates or gachas) describe any in-game mechanism in which a randomised game-related item can be obtained from a virtual box (Drummond & Sauer, 2018). These boxes are typically purchased using real life currency, or otherwise opened using 'keys' which must be purchased using real currency. The boxes do not award a specific item, instead offering a range of items which could be obtained, varying in rarity, strength, value, and likelihood of being awarded, with stronger or more valuable items being less likely to appear (Gong & Rodda, 2022). Due to their resemblance to traditional forms of gambling such as slot machines or lottery tickets, the use of loot boxes in modern video games has sparked a fiery debate about its ethical and legal implications.

Stories of excessive spending on loot boxes, often by minors, are not uncommon[3]. Nor are stories involving what would traditionally be described as gambling-like behaviours[4]. Research has indicated a correlation between loot box engagement and problem-gambling severity, suggesting that certain individuals may be particularly susceptible to the addictive nature of loot boxes (Zendle & Cairns, 2019). It is therefore imperative to address these concerns and implement regulatory measures that protect consumers, particularly those vulnerable to gambling-related harms.

This paper will explore the various arguments in favour of regulating loot boxes. It will first consider the definition and prevalence of loot boxes in modern video games. Second, it will examine the potential psychological and financial consequences of loot boxes. It will then analyse existing policy approaches and regulatory frameworks in different jurisdictions and discuss the rationale and history of these frameworks. Finally, it will briefly discuss challenges of implementation of loot box regulation. By highlighting the various approaches to loot box regulation, this paper seeks to contribute to ongoing academic and industry discussion relating to loot box mechanics, advocate for consumer protection measures within the gaming industry, and mitigate the health and financial risks associated with loot boxes.

---

1 Wijman, T. (2023). Free Global Games Market Report. Newzoo. https://clck.ru/3A9d8c

2 Ibid.

3 Gach, E. (2017, November 30). Meet The 19-Year-Old Who Spent Over $17,000 On Microtransactions. Kotaku. https://goo.su/cQpxD6g

4 Ibid.

1. Loot Boxes: Origins and Definition

1.1. The Origin of Microtransactions

The use of real currency to purchase in-game items is not a novel concept; traceable back to the 1990 arcade game Double Dragon 3: Rosetta Stone – infamous for the invention of microtransactions[5]. A classic side-scrolling, single-player fighting game, at the commencement of each of the first three stages of the game players have the option to enter a shop and purchase weapons, special attacks (called 'tricks'), and additional playable characters.

In typical arcade fashion, Rosetta Stone was engineered to encourage players to pour in the quarters[6]. Without any purchases in the in-game shop, playable characters had less health than in previous Double Dragon games, had only one life, and had no access to weapons (which also precluded the player from using certain attacks and seeing weapon-based fighting animations)[7]. When the game was ported for Japanese audiences, microtransactions were entirely removed, likely due to the controversy they had caused in the North American market[8]. Concurrently, the game was 'rebalanced' to allow all characters to be selectable from startup, have increased health, have access to every 'trick', and weapons to be organically found throughout the game.

1.2. Loot boxes in the mainstream

Microtransactions began to become the norm throughout the 2000s. During this time, a gaming format known as a massively multiplayer online game (MMO) had become intensely popular. These MMOs, which could be played by tens of millions of people[9], varied in their business models[10].

One approach was the subscription or 'pay-to-play' model, typically in the region of $15 per month. This was the cost for the most popular MMO of all time, World of Warcraft, for example[11]. Other popular games such as Guild Wars and Elder Scrolls Online were 'buy-to-play', requiring players to purchase the full game initially but then allowed them to play in perpetuity with no further costs. While many 'free-to-play' games existed, the developers of these games often sought to increase their player base before introducing a subscription requirement or simply selling the game to another developer.

---

5 Derboo, S. (2016, November 4). Double Dragon 3 (Arcade). Hardcore Gaming 101. https://clck.ru/3A9dYA

6 (2022, June 9). Double Dragon 3: The Rosetta Stone (Arcade). The Cutting Room Floor. https://clck.ru/3A9dZS

7 Derboo, S. (2016, November 4). Double Dragon 3 (Arcade). Hardcore Gaming 101. https://clck.ru/3A9dbT

8 (2022, June 9). Double Dragon 3: The Rosetta Stone (Arcade). The Cutting Room Floor. https://clck.ru/3A9dc6

9 Top MMOs. MMO Populations. https://clck.ru/3A9ddP

10 Olivetti, J. (2016, 30 April). Massively OP's guide to MMO business models. Massively Overpowered. https://clck.ru/3A9de5

11 Assuming the player purchased one month at a time, with lower monthly rates available if 6 or 12-month memberships were purchased up front.

In practice, MMOs often utilized hybrid business models. RIFT, for example, advertises itself as a free-to-play game, but allows players to purchase a 'Patron Pass' to receive "access to the benefits of a subscription for a set amount of time"[12]. It also maintains an in-game item shop where players can spend 'Credits', an in-game currency which could be purchased using real currency. The hybrid approach meant that games could implement microtransactions regardless of whether they were free, buy-to-play, or pay-to-play, bringing into existence a new revenue model: the item-based model (So & Westland, 2012).

While the exact origins of loot boxes are disputed, So & Westland trace it back to the Chinese gaming community in which players typically did not own home PCs nor gaming consoles, the latter of which were banned nationwide in 2000 (Liao, 2016). This meant that gamers predominantly undertook their gaming in internet cafes, circumventing the need to purchase full-title games upfront and leaving game developers seeking alternative forms of revenue. Here, a developer by the name of Zhengtu Network saw an opportunity and released Zhengtu Online. Officially launching in 2007, Zhengtu was a free-to-play MMO which allowed players to purchase "virtual treasure boxes, which may contain in-game items worth more than the cost of the box itself" (So & Westland, 2012). The game achieved unprecedented success that same year, both financially and in player numbers (So & Westland, 2012). With profits justifying the means, other developers quickly began to take note of the viability of loot boxes in achieving large-scale commercial success.

1.3. Definition and Prevalence

Legally accepted definitions of gambling generally require three elements: (a) consideration, (b) chance, and (c) a reward (Devereux, 1979). This interpretation overtly omits games which dominantly require skill (Brenner & Brenner, 1990). This definition would certainly be satisfied by some, if not most, existing loot box systems. Policymakers in some jurisdictions have interpreted this definition narrowly, declaring loot boxes legal under their regulatory framework because the rewards do not allow players to receive a prize in the form of real currency (or in a form that can be directly exchanged for real currency, e.g. casino chips)[13].

Others have argued that the predatory and entrapping nature of loot boxes justifies its categorisation as a form of gambling (King & Delfabbro, 2018). King and Delfabbro suggest that loot boxes and other predatory schemes in video games "contribute to the increasing similarity of gaming and gambling" because they "disguise or withhold the long-term cost of the activity until players are already financially and psychologically committed". Griffiths has similarly propounded that the unpredictable result of opening loot boxes inherently constitutes gambling because the value of the rewards are often less than the price paid (1995).

---

12 Game Guide | FAQ. Rift. https://clck.ru/3A9dgs

13 Nettleton, J., & Chong, K. (2013, October 16). Online social games – the Australian position. Mondaq. https://clck.ru/3A9dhY

Loot boxes have gone on to be featured in many games since Zhengtu. High-profile titles such as Call of Duty, Counter-Strike, FIFA, Destiny, Valorant and Overwatch currently make slightly different forms of loot boxes available in their mainline games. Counter-Strike, for example, allows for 'skins' to be obtained via 'containers', enabling players to customise the look of their in-game weapons without providing any change in how the weapons operate (i.e. purely cosmetic rewards)[14]. In contrast, players can open 'packs' in FIFA to obtain better players to add to their team; the better the players obtained, the better the player's team becomes for competitive play[15].

A 2021 report by Juniper Research estimated $15 billion revenue generated from loot boxes in 2020, with predicted spending to exceed $20 billion by 2025 without regulatory intervention[16]. Loot boxes appear to be highly prevalent in video games, especially on mobile platforms (2020a). Analysis by Zendle et al revealed that 58% of the 100 top-grossing mobile games on the Google Play store and 59% of those on the Apple App store contained loot boxes. Comparatively, an analysis of the top 463 most-played games on the Steam platform, a digital video game distribution service, found that 71% contained loot boxes (2020b). This represents a 67% increase in the prevalence of loot boxes in desktop games between 2010-2019, accelerated by rapid growth in 2012-2014. Among adult gamers, 78% have purchased at least one loot box (Zendle et al., 2020a).

2. Arguments for Legal Regulation

2.1. Ensuring Ethical Conduct

2.1.1. Psychological Manipulation

The allure of uncertain rewards and the use of persuasive techniques can have a significant psychological impact on individuals, potentially leading to addictive behaviors or the normalization of gambling-like tendencies. Akin to traditional forms of gambling, the random nature of loot boxes taps into psychological principles such as operant conditioning (Staddon & Cerutti, 2003) and variable-ratio scheduling (Zuriff, 1970) to increase engagement and satisfaction among players.

Players are motivated by the anticipation and excitement of what they might receive, creating a sense of reward and euphoria upon obtaining rare or valuable items. As documented in behavioural psychology literature, these phenomena prey on the notion that unpredictable rewards are more motivating and addictive than those which are predictable or expected. The intermittent nature of rewards in loot boxes, sometimes resulting in a 'near miss' scenario, can fuel a cycle of anticipation and continuous engagement as players strive to obtain newer and more valuable items.

---

14 Container. Counter Strike Wiki. https://clck.ru/3A9dji

15 Your Guide to: FIFA Ultimate Team Packs. FIFA. https://clck.ru/3A9dk3

16 Moar, J., & Hunt, N. (2021, March 9). 'Video Game Loot Boxes to Generate Over $20 Billion in Revenue by 2025. Juniper Research. https://clck.ru/3A8Xn6

The uncertainty and element of chance can trigger further cognitive biases like the illusion of control and the gambler's fallacy, leading players to believe they have more control over the outcome than they do. This can result in addictive behaviors and excessive spending as players chase after desired items or experience a sense of loss aversion.

2.1.2. Financial Exploitation

Critics argue that the use of loot boxes may normalize gambling-like behaviours among young players, potentially leading to gambling-related issues later in life. Recent analysis by Primi et al showed that loot box engagement had a significant effect on video game frequency, problem video gaming, and gambling frequency (2022). The repetitive nature of opening loot boxes, driven by the desire to obtain rare or valuable items, can create a reward-seeking loop that reinforces impulsive behavior and undermines the concept of earning rewards through skill-based achievements or progression.

Moreover, loot boxes employ various subliminal techniques to entice players to make purchases. These include eye-catching and aesthetic visuals, such as flashy animations, music and sound effects, to enhance the perceived value of opening a loot box regardless of its objective value. Additionally, limited-time offers, exclusive items, and in-game events create a fear of missing out (FOMO), fostering a sense of urgency and driving players to spend more money.

Overall, the mechanics of loot boxes combine chance, anticipation, and variable rewards to create a psychological impact that can be both enticing and potentially detrimental to players, necessitating careful consideration and regulation to protect consumers. Understanding the mechanics and psychological implications of loot boxes is essential to addressing the associated concerns and develop responsible regulatory measures.

2.2. Harm Minimisation

2.2.1. Vulnerable Populations

The psychological impact of loot boxes disproportionately affects vulnerable populations who may be more susceptible to gambling-related behaviors. For individuals with predispositions to gambling, the similarities between loot boxes and traditional forms of gambling can trigger addictive tendencies or lead to problematic behaviors. A large-scale survey by Zendle and Cairns (2019) identified a link between the amount that gamers spent on loot boxes and the severity of their problem gambling. The link was stronger than a link between problem gambling and buying non-loot box items with real currency, suggesting that the gambling-like features of loot boxes are specifically responsible for the observed relationship between spending on loot boxes and problem gambling.

Another study by Drummond (2022) demonstrated that purchasers of loot boxes were approximately 1.87 times higher risk of severe psychological distress on a standardised clinical screening tool than people who did not purchase loot boxes. This effect was observed even in subjects who did not exhibit problem gambling symptoms.

2.2.2. Children and Adolescents

Loot box mechanics are also highly targeted towards minors, who may be less capable of understanding the implications of spending real money or the negative effects of gambling. Analysis by Zendle et al. (2020b) shows that of the top 50 most played games on the Steam platform that contain loot boxes, 43% are classified as suitable for children aged 12+. For mobile platforms, 93% and 94% of the 100 top-grossing games on the Google Play and Apple App stores, respectively, that contain loot boxes are considered suitable for children aged 12+.

A recent Australian study found that up to 40% of adolescents have gambled on digital games in the past 12 months, including 36.5% of participants who had purchased loot boxes[17]. In teenagers, buying loot boxes has been associated with higher gambling frequency and gambling problems (Rockloff et al., 2021), and greater risk for gaming disorder (Hing et al., 2023a). In particular, teenage girls who had engaged with loot boxes more often had positive attitudes towards gambling compared to girls who had not. This suggests that gambling interests in girls may develop around or at the same time as interest in loot boxes.

A 2023 study by Hing et al found that adolescents who engage in simulated gambling in video games engage in simulated gambling more frequently and in more diverse settings later in life, and that the activities they seek out become more akin to monetary gambling (2023b). Concerningly, the study identified that young people often fail to realise that simulated gambling in video games resembles gambling and can have both gaming and gambling-related harms (Hing et al., 2023b).

3. Comparative analysis of national approaches to regulation

3.1. Belgium

On 17 November 2017, Electronic Arts Inc. ('EA') released Star Wars Battlefront II on Windows, Playstation 4 and Xbox One[18]. The game received widespread criticism for its painstaking progression system and option to engage in microtransactions to skip this progression, including the availability of loot boxes[19]. Shortly after the game's release,

[17] Hing, N., Rockloff, M., & Browne, M. Submission to the Inquiry into online gambling and its impacts on those experiencing gambling harm. No 24. Parliament of Australia Standing Committee on Social Policy and Legal Affairs, Inquiry into online gambling and its impacts on those experiencing gambling harm. https://goo.su/lkp6

[18] (2023, 17 July). Star Wars Battlefront II (2017 Video Game). Wikipedia. https://clck.ru/3A9due

[19] Ibid.

reddit user MBMMaverick posted a thread on the StarWarsBattlefront subreddit entitled 'Seriously? I paid 80$ [sic] to have Vader locked?'[20]. The thread received over 228,000 net positive votes and nearly 3,000 comments, almost of which condemned the game design which ostensibly drove players to spend money to progress in the game. The post received a response from the EA community engagement division who claimed that the laborious progression system was intended to provide players "with a sense of pride and accomplishment"[21]. The comment unsurprisingly received a wave of negative responses and quickly became the most negative voted comment in Reddit's history[22]. Shortly thereafter, EA updated the game to remove all microtransactions[23]. Battlefront II is credited for bringing the controversy of microtransactions and loot boxes to mainstream discussion[24].

The media coverage surrounding Battlefront II convinced Belgian Minister of Justice, Koen Geens, to order an investigation into the legality of loot boxes under its gambling legislation[25]. Belgium's Gaming Commission considered loot box mechanics with against the definition of 'gambling' under Belgian law; three conditions need to be satisfied: "a game element, a bet [which can] lead to profit or loss, [with] chance playing a role in the course of the game"[26]. Having analysed four of the most well-known online games in 2017–2018 (Overwatch, FIFA, Star Wars Battlefront II, and Counter-Strike: Global Offensive), the Commission ruled that the elements required under Belgian gambling law to constitute 'gambling' were satisfied and therefore loot boxes should be regulated as a gambling product[27].

In outlining its findings, the Commission stated its compliance regime as follows:

"Despite the fact that the system of loot boxes in the… video games can be seen as a game of chance, the protection of the players is always lacking. The fact that it often involves underage players is disturbing. The hidden nature of games of chance is particularly problematic in the case of children. If not properly intervened, games of chance in video games will cause great damage to people, families and society…"[28]

---

20 MBMMaverick, (2017). Seriously? I paid 80$ [sic] to have Vader locked?. Reddit. https://goo.su/zw33

21 Ibid.

22 Baculi, S. (2019, September 11). EA's Response to Star Wars Battlefront II Microtransaction Complaint Recognized by Guinness World Records as "Most-Downvoted Comment on Reddit". Bounding into Comics. https://clck.ru/3A9dzX

23 Corden, J. I (2018, November 21). Confirmed: EA has removed all microtransactions from Star Wars Battlefront II (update). Windows Centra. https://clck.ru/3A9e25

24 Kim, M. (2019, August 27). Star Wars Battlefront 2 Loot Box Controversy: 'We Hit Rock Bottom,' EA DICE Says. IGN. https://clck.ru/3C4D37

25 (25 April 2018). Loot boxen in drie videogames in strijd met kansspelwetgeving. Koen Geens. (Translated from Dutch to English). https://clck.ru/3A9e2Z

26 Ibid.

27 Ibid.

28 Ibid (translated from Dutch to English).

"The investigated games with paying loot boxes, as they are currently offered in our country, are therefore in violation of the legislation on games of chance and can be dealt with under criminal law. The loot boxes must therefore be removed. If not, the operators risk a prison sentence of up to five years and a fine of up to 800,000 euros. When minors are also involved, those sentences can be doubled"[29].

As at time of publication, Belgium is the only jurisdiction in Europe to have unambiguously outlawed the use of loot boxes.

3.2. Netherlands

The ongoing debate on loot boxes in the Netherlands can be traced back to 2019, when the Netherlands Gaming Authority imposed a €5 million civil penalty on EA, the developer of the FIFA series, for violation of the Dutch Gambling Act[30]. In a media release discussing the infringement, the Authority described FIFA's loot box system as: "...determined by chance, the contents [of which] cannot be influenced. The fact that [the contents] sometimes have a high value and that they can occasionally be traded constitutes a violation of the Gambling Act. Under Dutch law, a game of chance that allows a prize or premium to be won can only be provided if a relevant licence has been granted"[31].

The Authority's enforcement efforts were based on a 2018 study it undertook which found a correlation between playing games containing loot boxes and gambling addiction[32]. The Authority imposed a policy of "strict separation between gaming and gambling".

EA promptly challenged the penalty before the District Court of the Hague, which ruled in favour of the Authority on 15 October 2020[33]. EA contended that while 'pack' openings were luck-based, the openings were encapsulated within a broader game of skill, the overall game of FIFA. It further contended that the players obtained from packs were not directly convertible to money as required under Dutch gambling law. The Court resoundingly rejected these arguments, opining that the game mode within FIFA which utilised loot box mechanics could be viewed in its own right, distinct from the rest of the game.

On appeal, the Dutch Council of State overturned the District Court's decision, finding that the game mode involving pack openings was not a distinct game[34]. The Council found this view impossible to maintain as obtaining players through pack openings were a necessary venture to build a team to play competitive matches, and was therefore

29 Ibid (translated from Dutch to English).

30 Wet op de kansspelen, Artikel 33f(1).

31 (2020, October 29). Imposition of an order subject to a penalty on Electronic Arts for FIFA video game. Kansspelautoriteit. https://clck.ru/3A9e5i

32 Ibid.

33 Electronic Arts Swiss Société à responsabilité limitée en de raad van bestuur van de Kansspelautoriteit (2020) AWB-20_3038.

34 Raad van State, Uitspraak 202005769/1/A3, ECLI:NL:RVS:2022:690.

an inherent part of the broader game which was not a game of chance under Dutch gambling law. In a judgment that could guide future loot box regulation around the world, the Council identified criteria which, if satisfied, would mean the video game in question falls outside the scope of the Dutch Gambling Act: a) The loot box mechanic is part of a broader game; b) the broader game is a game of skill; c) the loot boxes are earned and opened in the game, not on a separate platform; and d) the loot boxes in the game are mostly obtained by playing the game organically (without necessarily using real currency).

As at time of publication, the Dutch Government has communicated its willingness to agitate for a ban on loot boxes under European Union law[35].

3.3. Spain

Spain's Ministry of Consumer Affairs announced its interest in regulating loot boxes on 1 July 2022 by publishing a draft law seeking to impose strict consumer protections on games which contained randomised reward mechanisms.[36] The law proposes to treat video games containing loot boxes almost identically to gambling, imposing measures such as identity verification to ensure users are of age,[37] banning advertisements outside the hours of 1am and 5am,[38] publication of probability rates of receiving each potential reward (i. e. drop rates),[39] mandatory implementation of a self-exclusion system,[40] and pre-determined spending limits.[41] Breaches of these measures would be punishable by fine ranging from €200,000 to €5,000,000 per infraction and potential shut down of the game's loot box offering[42].

Most notably, the draft law expressly precludes licenced gambling operators from using loot box mechanics in any service or product offerings[43]. This prohibition extends to preclude organisations who market traditional gambling products as third-parties from doing the same in relation to loot box-related products[44]. This approach, in combination with the aforementioned gambling-like harm minimisation measures, would make Spain the toughest regulatory environment for loot box products.

---

35 (2023, June 29). Consumentenagenda minister Adriaansens: aanpak deurverkoop, eenvoudig online opzeggen. Rijksoverheid. https://clck.ru/3A9e8L

36 Ministerio de Consumo. Anteproyecto de Ley por el que se regulan los mecanismos aleatorios de recompensa asociados a productos de software interactivo de ocio. https://clck.ru/3A9e8q

37 Ibid. P. 9.

38 Ibid. P. 10.

39 Ibid. P. 11.

40 Ibid. P. 12.

41 Ibid.

42 Ibid. P. 15.

43 Ibid. P. 16.

44 Ibid.

3.4. United Kingdom

As early as 2016, the UK Gambling Commission expressed its concern about the potential risks of loot boxes to children and young people, resulting in the publication of its Virtual currencies, eSports and social casino gaming position paper[45]. While the Gambling Commission had already utilised its compliance powers in relation to skin gambling websites[46], it opined that it held no powers in cases where loot box rewards were not clearly redeemable for real currency[47].

Unwilling to accept the status quo, both House of Commons Digital, Culture, Media and Sport Committee[48] and the House of Lords Select Committee on the Social and Economic Impacts of the Gambling Industry[49] called for the Gambling Act 2005 to be amended to bring loot boxes within the scope of the UK's gambling regulatory framework.[50] In a review of the Gambling Act undertaken in response to calls for reform, the UK Government acknowledged the potential harms associated with loot boxes in video games, but was unwilling to scope them into the Gambling Act in the absence of clear academic evidence establishing a causal link between loot box spending and problem-gambling[51]. The Government expressly stated that pending greater research on the harms of loot boxes, its position would be kept under review[52].

Notwithstanding its legislative inaction, the UK Government made two recommendations on the treatment of loot boxes: 1) that children or young people should not be able to purchase loot boxes without the consent of a parent or guardian, and 2) that all players should have access to spending controls and transparent information in the name of safe gameplay[53]. These recommendations ultimately led to a self-regulation approach by the industry in July 2023, which published a set of 'Industry Principles' purported to improve protections for players[54]. The Principles include the disclosure of drop rates, targeting of unauthorised third-party websites fostering the sale of items, a commitment to "lenient" refund policies,

---

45 Gambling Commission. (2017, March). Virtual currencies, eSports and social casino gaming – position paper. https://clck.ru/3A9eBu

46 Gambling Commission. (2017, February 6). Two men convicted after offering illegal gambling parasitic upon popular FIFA computer game. https://clck.ru/3A9eCc

47 Gambling Commission. (2017, November 24). Loot boxes within video games. https://clck.ru/3A9eDE

48 (2019, 12 September). House of Commons Digital, Culture, Media and Sport Committee. Immersive and addictive technologies. https://clck.ru/3A9eDr

49 House of Lords. Select Committee on the Social and Economic Impact of the Gambling Industry. (2020, July 2). Gambling Harm – Time for Action. https://clck.ru/3A9eEs

50 Gambling Act 2005 (UK).

51 (2022, July 18). Department for Digital, Culture, Media & Sport, Government response to the call for evidence on loot boxes in video games. https://clck.ru/3A9eG4

52 Ibid.

53 Ibid.

54 UKIE, New Principles and Guidance on Paid Loot Boxes. https://goo.su/me0Y3

and a 12-month review of the effectiveness of the Principles in collaboration with the Government[55].

As the Principles have only been in place for a few weeks as at time of publication, it remains to be seen whether a self-regulation model is an effective measure in reducing the harms of loot box mechanics.

3.5. Finland

Regulatory interest has similarly arisen in Finland. In September 2022, Sebastian Tynkkynen of the Finish Parliament introduced a bill to regulate loot boxes as a form of gambling[56]. The bill would amend the definition of 'lottery' under the Finnish Lotteries Act 2001 to include "virtually utilisable profits", i.e. items with only a virtual value[57]. The change would scope in loot boxes as a form of gambling under existing gambling laws, even in cases where obtainable in-game items cannot be sold externally or be exchanged for real currency. This places Finland in a league of its own among the EU in which exchangeability for real currency was the saving grace for developers in other jurisdictions. It would also make Finland's loot box regulations the most difficult to circumvent given the breadth of its application.

3.6. China

The video game regulatory environment in China is complex. Underlying concerns of addiction which gave rise to China's console ban in the 2000s have manifested a series of other regulatory requirements; inter alia, games cannot depict obscenity or nudity, 'scary' scenes or images, glorification of war or crime, slandering of cultural traditions, or promotion of drug use or drug trafficking[58]. Adherence to these requirements is overseen by China's State Administration of Publication, Press, Radio, Film and Television (SAPPRFT).

Shortly after the disbandment of its video game console ban, China moved to regulate loot boxes citing similar concerns about Star Wars Battlefront II as the Belgian Government. China's Ministry of Culture imposed heavy limitations on the use of loot boxes on 1 May 2017, barring loot boxes from being purchased with real currency (or virtual currency purchased with real currency), mandating the disclosure of drop rates, and further mandating that developers publicly disclose player spending for the previous 90 days[59].

---

55 Ibid.

56 LA 42 /2022 vp, Bill to amend Section 2 of the Lotteries Act 2001.

57 Heilbuth, H. (2022, December 15). Exploring Finland's proposed loot box regulation. GamesIndustry.Biz. https://clck.ru/3A9eQv

58 Kuhns, T. (2016, May 24). Mobile Game Content Standard (2016 Edition). AppInChina. https://clck.ru/3A9eRa

59 Tang, T. (2018, May 16). A Middle-Ground Approach: How China Regulates Loot Boxes And Gambling Features In Online Games. Mondaq. https://clck.ru/3A9eYS

As traditional gambling is unlawful in China, loot box mechanisms are subject to further restrictions designed to keep loot box use from constituting gambling. As the regulatory body for game content and approval, SAPPRFT does not approve the release of any game which contains a 'compulsion loop' – any mechanism designed to lead a player to the use of loot boxes (or any gambling-like system)[60]. For example, if a certain item can only be obtained through opening loot boxes, the game is unlikely to be approved by SAPPRFT. This means that aspects of a game containing loot boxes may bar it from publication in China.

3.7. Japan

Japan was the first jurisdiction to regulate loot box mechanics. The nation has long been host to 'gacha' games – a typically free-to-play game, especially mobile game, which induces players to spend money (both in-game and real) to acquire specific items or characters to progress the storyline[61]. On 18 May 2012, the Japanese Consumer Affairs Agency declared "complete gacha" games illegal – a form of gacha game in which complete sets need to be collected before the player can progress[62]. The Agency cites "extremely high charges imposed on players" and complaints received in relation to such charges[63].

Notably, at the time of the Agency's announcement, several of the biggest complete gacha developers had already ceased their use of the mechanic[64]. Developers expressed differing reasons for cessation, including sub-par sales numbers of their gacha game[65], a preference for industry self-regulation[66], and an expectation that impact of the ban to revenue will be minimal[67].

3.8. Republic of Korea

Like China, South Korea has a demonstrated history of video game regulation. Its Youth Protection Revision Act, dubbed 'Shutdown Law', made international news in 2011 when it banned children under the age of sixteen to play online video games between the hours of midnight and 6am (Sang et al., 2017). This curfew was compounded in 2012 when

60 Ibid.

61 (2023, August 20). Gacha. Wiktionary. https://clck.ru/3A9ixg

62 Gantayat, A. (2012, May 18). Complete Gacha Officially Deemed Illegal. Andriasang. https://clck.ru/3A9eZZ

63 (2012, May 6). 'Kompu gacha' online games may be illegal. The Yomiuri Shinbun. https://goo.su/Z2k9Q

64 Gantayat, A. (2012, May 18). Complete Gacha Officially Deemed Illegal. Andriasang. https://clck.ru/3A9ebn

65 Gantayat, A. (2012, May 10). DeNA and GREE Stock Values Plummet Following Reports of Government Regulation. Andriasang. https://clck.ru/3A9edQ

66 Gantayat, A. (2012, May 9). Social Game Maker KLab Puts Halt to Complete Gacha Sales. Andriasang. https://clck.ru/3A9eeT

67 Gantayat, A. (2012, May 8). Analysts Expect Major Social Game Losses if Sales Tactics is Banned. Andriasang. https://clck.ru/3A9efC

further legislation was introduced to require large gaming companies to implement a selection system of game availability period – a technical name for what is effectively a customisable parental curfew option[68]. To date, only China and Vietnam have imposed similar restrictions[69].

By early 2021, the Shutdown Law was being reconsidered in light of significant logistical issues in its enforceability[70]. On a separate front, calls to regulate online games for deceptive use of loot boxes were growing[71]. These calls were catalysed by controversy surrounding the use of loot boxes in MapleStory, a highly popular Korean MMORPG[72]. While loot boxes typically offer a random in-game item, MapleStory players could acquire three randomly chosen 'abilities'. The games developer, Nexon, admitted that it was impossible to hit a 'jackpot' (i.e. three very powerful abilities) through this mechanic; the mechanic was designed to prevent the most powerful abilities from appearing simultaneously[73]. Backlash and an investigation by Korea's Fair Trade Commission resulted in Nexon refunding the previous two years of loot box purchases – the period for which Nexon had kept purchase logs[74].

A day after Nexon's announcement to provide refunds, the Korea Game Industry Association announced a new set of regulations requiring probability disclosure of random chance events resulting in improvement to character abilities, skills, or equipment upgrades – not just the acquisition of items[75]. Unsatisfied with industry self-regulation, the National Assembly of South Korea passed an amendment to the Game Industry Promotion Act on 27 February 2023, almost unanimously, mandating the disclosure of loot box probability rates in game, on the game's official website, and advertisements[76]. Failure to disclose rates, or doing so falsely, is now punishable by fine of up to ₩20 million ($15,000 USD) or imprisonment for up to two years[77].

---

68 Tassi, P. (2012, July 2). New Korean Law Lets Parents Decide When Their Kids Can Play Games. Forbes. https://clck.ru/3A9ejW

69 (2023, August 9). Shutdown Law. Wikipedia. https://clck.ru/3A9ek3

70 (2021, November 16). Shutdown law shuttered. Korea Herald. https://clck.ru/3A9eke

71 K. Byung-wook. (2021, March 9). Game firms under increasing scrutiny over loot box odds. Korea Herald. https://clck.ru/3A9s2F

72 Ibid.

73 Ibid.

74 Maple Story. (2021, May 28). (Compensation payment completed) We apologize for not meeting the customer's expectations in the process of disclosing the cube probability. https://clck.ru/3A9emF

75 Min-Je, P. (2021, May 29). Game association introduces own loot box disclosure rules. Korea JoongAng Daily. https://clck.ru/3A9emd

76 Mi-hee, K. (2023, February 27). Stochastic Item Information Disclosure Act, passed the plenary session of the National Assembly. GameMeca. https://clck.ru/3A9eqz

77 Obedkov, E. South Korea passes new amendment on loot box probability disclosure. Game World Observer. https://clck.ru/3A9eru

3.9. Germany

In March 2021, the national parliament of Germany passed amendments to the Jugendschutzgesetz (Protection of Young Persons Act) to strengthen protections for children and young people relating to media content[78]. The changes included an update to the German video game classification standards to allow consideration of 'interaction risks', including, inter alia, the presence of loot boxes and other in-game purchases[79].

The German age classification board, Unterhaltungssoftware Selbstkontrolle (USK), ratified the law into its procedural guidelines from 1 January 2023[80]. In its communications, USK highlighted the inclusion of "possible online risks – such as purchasing or communication options" in the classification of newly submitted digital games[81]. Under the new rules, a higher age rating would be appropriate for a game if it could "impair the development of children and young people or their upbringing to become self-reliant and socially competent personalities"[82]. It further states: "The participation of minors in games of chance is strictly prohibited, as this is part of the medically recognized clinical picture of a gambling addiction with serious psycho-social consequences and significant financial risks for those affected… If digital games are not subject to the statutory ban on gambling, the age classification of digital games must take into account… that [they] are likely to impair or endanger the personality development of children or young people with regard to their attitude to gambling. In particular, this is game content that can lead to habituation to or trivialization of gambling by promoting a positive attitude towards gambling, contributing to desensitization to gambling losses or causing unrealistic profit expectations"[83].

3.10. Canada

In September 2020, two men filed a class action claim against EA in the Supreme Court of British Columbia[84]. The suit contended that EA's use of loot boxes in dozens of its games put it in violation of British Columbia's consumer protection laws[85] and the gambling

78 Puppe, M. (2021, March 10). German Bundestag passes new Youth Protection Act. The German Games Industry Association. https://clck.ru/3A9iuW

79 Ibid.

80 (2022, December 14). In-game purchases, chats and loot boxes: USK expands test criteria. Unterhaltungssoftware Selbstkontrolle. https://clck.ru/3A9is6

81 Ibid (translated from German to English).

82 (2022, December). Unterhaltungssoftware Selbstkontrolle, Guiding criteria of the USK for the evaluation of youth protection law digital games, 8 (translated from German to English). https://clck.ru/3A9isY

83 Ibid 23 (translated from German to English).

84 Sutherland v Electronic Arts Inc. (2020, September 30). Vancouver S-209803 (BCSC) (Plaintiff's Notice of Civil Claim). https://clck.ru/3A9evu

85 Business Practices and Consumer Protection Act [SBC 2004].

provisions within the federal Criminal Code[86]. Judge Fleming held on March 2023 that while the consumer protection claim may proceed, the claim in respect of the Criminal Code could not. The Judge opined that loot box rewards in EA's game offerings could only be exchanged using the in-game marketplace and that in the absence of "[the] prospect of gaining, or losing, anything with a real-world value", the claim had no reasonable prospects of success[87]. The firm representing the plaintiffs in Sutherland has filed class-actions against dozens of video game companies in British Columbia and Quebec[88]. Accordingly, the judicial, regulatory, and social consequences of these actions remains to be seen.

3.11. Australia

Australian Member of Parliament Andrew Wilkie introduced a private member's bill on 28 November 2022 to amend the Classification (Publications, Films and Computer Games) Act 1995[89]. The bill would have required the Australia Classification Board to classify computer games which contain loot boxes as either R 18+ or RC (Refused classification, barring the product from sale, rent, advertising or importation into Australia), and require a warning to displayed when games contain loot boxes or similar features, similar to Germany's amended classification standards[90]. As at 1 August 2023, the bill was removed from the parliamentary agenda as it had not progressed within the time required by parliamentary rules[91].

4. Challenges to Implementation

4.1. Challenging the Status Quo

Loot boxes in their current form are often considered akin to traditional gambling[92]. However, there still appears to be resistance against categorising loot box mechanics as gambling in most jurisdictions. Bases for this resistance vary, but the commonality among them appears to be an unwillingness to consider something to be gambling simply

86 Criminal Code, RSC 1985, c C-46, Part VII.

87 Dring, Ch. (2023, March 21). Canada Judge rejects unlawful gambling accusation in EA loot box lawsuit. GamesIndustry.Biz. https://clck.ru/3A9exW

88 Loot Boxes Class Action Lawsuits – Canada. Slater Vecchio LLP. https://clck.ru/3A9eyM

89 Classification (Publications, Films and Computer Games) Act 1995 (Cth).

90 Classification (Publications, Films and Computer Games) Amendment (Loot Boxes) Bill 2022. Parliament of Australia. https://goo.su/NkJWUmp

91 Ibid.

92 Moar, J., & Hunt, N. (2021, March 9). 'Video Game Loot Boxes to Generate Over $20 Billion in Revenue by 2025. Juniper Research. https://clck.ru/3A8Xn6

because it does not look, on face value, to be traditional gambling, notwithstanding the accepted definition of gambling having been met.

For example, Australian regulatory bodies have opted against regulating loot boxes under existing gambling laws on the basis that the obtainable rewards did not consist of real currency, nor was there a facility or method available to directly convert the rewards obtained into real currency[93]. While this interpretation may have been accurate in the early days of loot boxes, the stance fails to account for the sale value of in-game items within the gaming ecosystem, as well as the growing ubiquity of buy/swap/sell and gambling websites designed to trade or stake loot box rewards (i.e. skin gambling) (Greer et al., 2023). Most of these third-party websites openly market themselves as 'gambling' or 'slots' websites, offering inducements almost identical to those used by traditional online betting sites (Deans et al., 2017).

Eilers & Krejcik estimate that roughly 3 million people wagered $2.3 billion worth of skins on the outcome of e-sports games in 2015[94]. They also estimates that $5 billion worth of skins were wagered in 2016, with roughly 60% of this amount being wagered on "casino-style gaming" websites[95]. These websites are generally targeted towards minors, often partnering with video game personalities and influencers to promote the service to their audience[96]. Skin gambling websites have also sponsored or managed their own e-sports teams, raising concerns about advertising to adolescent viewers and potential for match fixing[97].

Moreover, Hing et al argue that the 'real currency' requirement by regulators is not fit-for-purpose given that the harms caused can occur regardless of whether the rewards can be exchanged for real currency or not (Hing et al., 2023a). The psychological attractiveness of loot box mechanics does not require rewards to be financial, but simply something that is of perceived value. This could be an in-game weapon of high strength, a purely cosmetic item (i.e. skin), or any other socially-endorsed indicator of success. This argument is supported by findings of a 2023 study in which adolescents who engaged in simulated gambling in video games transitioned from valuing its virtual prizes to valuing its social benefits and the opportunity to learn new gambling games, compete against other players, and demonstrate skill (Hing et al., 2023b).

---

93 Nettleton, J. & Chong, K. (2013, October 16). Online social games – the Australian position. https://goo.su/tuWnN

94 Brustein, J. & Novy-Williams, E. (2016, April 20). Virtual Weapons are Turning Teen Gamers into Serious Gamblers. Bloomberg. https://goo.su/lnjzto

95 Assael, Sh. (2017, January 20). Skin in the Game. ESPN. https://goo.su/dMvYMsR

96 Sacco, D. (2016, July 4). Syndicate apologises after failing to disclose ownership of CSGO Lotto gambling site. Esports News UK. https://goo.su/fGi5t

97 Wynne, J. (2015, September 15). Popular betting website to sponsor pro Counter-Strike team. Dot eSports. https://clck.ru/3A9fJp

4.2. Industry Transparency and Insight

In their 2021 Juniper Research report, James Moar and Nick Hunt stated, "we expect to see game publishers react to [increased regulatory action against loot boxes] in future by changing loot box formats, in order to keep them compelling and outside the legal realms of gambling"[98]. To some extent, this expectation has come to fruition. In China, for example, Blizzard, one of the largest video game developers in the world, circumvented the Chinese ban on the sale of loot boxes by selling in-game currency for real currency, with which it gave players 'free' loot boxes as part of the transaction[99]. As at the time of publication, no enforcement action has been taken on this overt circumvention of the law.

Adding to the lack of transparency is the unwillingness of developers to provide loot box-related data for inquiry. Etchells et al. (2022) highlight the need for further research on the relationship between loot box spending and player wellbeing but emphasise the need for researchers to be given access to relevant industry data to accomplish this. Pronouncements of the 'gamblification' of video games by academics provides the ideal platform for the industry to garner good will by working with researchers, health and community workers, and other stakeholders to achieve wellbeing outcomes (Greer et al., 2023). Conversely, industry players may be unwilling to undertake consultations if it could lead to additional regulation which could result in diminished profits. Some positive representation has been seen in this space, however, with Valve, one of the biggest gaming companies in the world, recently making it a bannable offence for users to partake in running contests, gambling, or selling items[100].

4.3. Enforceability

The recency of the loot box regulation activity around the world poses difficulty in assessing their effectiveness. In respect of Belgium's regime, one of the earliest jurisdictions to impose restrictions on loot boxes, poor enforcement of its loot box ban has been identified. Xiao found that 82 % of the 100 high-grossing iPhone games in the Belgium App Store continued to use some form of randomised monetisation method, including 80.2 % of games rated suitable for ages 12+ (2023). This was in spite of some high-profile developers entirely removing random chance mechanics from games marketed in Belgium[101] and the Belgium

[98] Moar, J., & Hunt, N. (2021, March 9). 'Video Game Loot Boxes to Generate Over $20 Billion in Revenue by 2025. Juniper Research. https://clck.ru/3A8Xn6

[99] Handrahan, M. (2017, June 6). Blizzard avoids China's loot laws by selling Overwatch in-game currency. GamesIndustry.biz. https://clck.ru/3A9fPN

[100] Biazzi, L. (2023, May 11). Valve launches offensive against gamblers on Steam, possibly affecting CS:GO's skin market. Dot Esports. https://clck.ru/3A9fPz

[101] Statement Belgium. 2k Games. https://goo.su/qsuW

Gaming Commission's threats to criminally prosecute video game companies using loot boxes without a gambling licence[102].

In the same study, Xiao found that the use of a virtual private network (VPN) proxy allowed players to access loot box offerings which had otherwise been removed from the Belgium version of a mobile game. In a study of the effectiveness of the UK's ban on access to pornography by minors, Thurman and Obster found that 46 % of 16 and 17 year olds had used a VPN or private browser to access pornographic websites which otherwise would have required the satisfaction of an age-verification check (2021)[103]. In a separate study undertaken by VPN provider ExpressVPN, 24 % of respondents admitted to lying about their age to use social media (which typically have a minimum age requirement of 13)[104]. 16% also stated that they had lied about their address or location[105]. From a regulatory standpoint, enforceability of loot box regulations therefore requires focus on both the developer and consumer's conduct.

Conclusions

This paper provided a comprehensive examination of the need for legal regulation of loot boxes in video games. By analysing the commentary on regulatory approaches taken in various jurisdictions, a foundation for understanding the potential negative impacts of loot boxes on consumers was established, particularly in relation to children and young adults. The concerns raised in this paper support the argument that stringent government regulation is necessary to protect consumers, promote industry transparency and accountability, and ensure the ethical and responsible use of loot box mechanics. By implementing effective regulatory measures, policymakers can strike a balance between innovation in the gaming industry, consumer protection, and user wellbeing, ultimately fostering a healthier environment for gamers.

This paper analysed a variety of approaches in the regulation or proposed regulation of loot box mechanics in video games. Some have assessed whether loot boxes fall within the definition of 'gambling' under existing legislation in their respective jurisdiction. In the case of Belgium and the Netherlands, regulators determined this test in the affirmative, despite judicial review negating the determination in the case of the latter. Comparatively,

---

102 Belgian Gaming Commission. (2018, April). Research report loot boxes., 18 (Translated from Dutch to English). https://goo.su/qsuW

103 Thurman, N. & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. Policy Internet, 13(3), 415.

104 (2023, January 19). Dangers of social media for kids and how to protect them. ExpressVPN. https://goo.su/Ks8N1JT

105 Ibid.

cases like Australia demonstrate that the understanding of the subject matter by regulators, or lack thereof, can have a fundamental impact on political appetite for regulation.

Other jurisdictions have taken an educative approach to regulation. Germany's approach for example results in consumers (and in the case of minors, their guardians) being more informed about the presence of loot boxes in products. More detailed yet is the approach taken by China and Korea, in which probability rates of all loot boxes, including ones which reward things other than items, must be displayed to the player. If this approach is demonstrated to be an effective way to reduce loot box or gambling-related harm to players, more jurisdictions may choose to take this lighter-handed approach to harm-minimisation, avoiding the need for a limitation or ban on loot boxes.

It requires reiterating that most regulatory measures analysed in this paper have yet to be reviewed for their effectiveness. As a result, one focus of future research would be the assessment of these measures on not only their impact on loot box consumption, but their flow on impact on player wellbeing, mental health, and finances. For the purposes of undertaking this assessment, the author further reiterates the need for developers and industry stakeholders to make available loot box purchase and use data to independent researchers.

Another aspect of loot box regulation which was alluded to in this paper, but did not form part of its primary focus, is the status of skin gambling websites under the law. Analysis of the relationship between loot box use and skin gambling could establish the 'exchangeability with real currency' element required by several jurisdictions to consider loot boxes under existing gambling laws. Moreover, the combined impacts of loot box use and skin gambling should be investigated. In theory, their combined use could have an amplified psychological or financial impact on consumers.

References

Brenner, R., & Brenner, G. A. (1990). *Gambling and speculation: A theory, a history, and a future of some human decisions*. Cambridge University Press.

Deans, E. G., Thomas, S. L., Derevensky, J., & Daube, M. (2017). The influence of marketing on the sports betting attitudes and consumption behaviours of young men: implications for harm reduction and prevention strategies. *Harm Reduction Journal*, *14*, 1–12. https://doi.org/10.1186/s12954-017-0131-8

Devereux, E. (1979). Gambling. In *The International Encyclopedia of the Social Sciences* (vol. 17). New York: Macmillan.

Drummond, A., & Sauer, J. D. (2018). Video game loot boxes are psychologically akin to gambling. *Nature human behaviour*, *2*(8), 530–532. https://doi.org/10.1038/s41562-018-0360-1

Drummond, A., Hall, L. C., & Sauer, J. D. (2022). Surprisingly high prevalence rates of severe psychological distress among consumers who purchase loot boxes in video games. *Scientific Reports*, *12*(1), 16128. https://doi.org/10.1038/s41598-022-20549-1

Etchells, P. J., Morgan, A. L., & Quintana, D. S. (2022). Loot box spending is associated with problem gambling but not mental wellbeing. *Royal Society Open Science*, *9*(8), 220111. https://doi.org/10.1098/rsos.220111

Gong, L., & Rodda, S. N. (2022). An exploratory study of individual and parental techniques for limiting loot box consumption. *International Journal of Mental Health and Addiction*, *20*, 398–425. https://doi.org/10.1007/s11469-020-00370-5

Greer, N., Rockloff, M., Hing, N., Browne, M., & King, D. L. (2023). Skin gambling contributes to gambling problems and harm after controlling for other forms of traditional gambling. *Journal of Gambling Studies*, *39*, 225–247. https://doi.org/10.1007/s10899-022-10111-z

Griffiths, M. D. (1995). *Adolescent gambling*. London: Routledge.

Hing, N., Lole, L., Thorne, H., Sproston, K., Hodge, N., & Rockloff, M. (2023b). 'It Doesn't Give Off the Gambling Vibes… It Just Feels Like a Part of the Game': Adolescents' Experiences and Perceptions of Simulated Gambling While Growing Up. *International Journal of Mental Health and Addiction*. https://doi.org/10.1007/s11469-023-01119-6

Hing, N., Russell, A. M., King, D. L., Rockloff, M., Browne, M., Newall, P., & Greer, N. (2023a). Not all games are created equal: Adolescents who play and spend money on simulated gambling games show greater risk for gaming disorder. *Addictive Behaviors*, *137*, 107525. https://doi.org/10.1016/j.addbeh.2022.107525

King, D. L., & Delfabbro, P. H. (2018). Predatory monetization schemes in video games (eg 'loot boxes') and internet gaming disorder. *Addiction*, *113*(11), 1967–1969. https://doi.org/10.1111/add.14286

Liao, S. X. (2016). Japanese console games popularization in China: Governance, copycats, and gamers. *Games and Culture*, *11*(3), 275–297. https://doi.org/10.1177/1555412015583574

Primi, C., Sanson, F., Vecchiato, M., Serra, E., & Donati, M. A. (2022). Loot boxes use, video gaming, and gambling in adolescents: Results from a path analysis before and during COVID-19-pandemic-related lockdown in Italy. *Frontiers in psychology*, *13*, 1009129. https://doi.org/10.3389/fpsyg.2022.1009129

Rockloff, M., Russell, A. M., Greer, N., Lole, L., Hing, N., & Browne, M. (2021). Young people who purchase loot boxes are more likely to have gambling problems: An online survey of adolescents and young adults living in NSW Australia. *Journal of Behavioral Addictions*, *10*(1), 35–41. https://doi.org/10.1556/2006.2021.00007

Sang, Y., Park, S., & Seo, H. (2017). Mobile Game Regulation in South Korea: A Case Study of the Shutdown Law. In D. Jin (Eds.). Mobile Gaming in Asia. *Mobile Communication in Asia: Local Insights, Global Implications* (pp. 55–72). Springer, Dordrecht. https://doi.org/10.1007/978-94-024-0826-3_4

So, Sh., & Westland, J. Ch. (2012). Red Wired: China's Internet Revolution. Marshall Cavendish.

Staddon, J. E. R, & Cerutti, D. T. (2003). Operant conditioning. *Annual Review of Psychology*, *54*, 115–144. https://doi.org/10.1146/annurev.psych.54.101601.145124

Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, *13*(3), 415–432. https://doi.org/10.1002/poi3.250

Xiao, L. Y. (2023). Breaking Ban: Belgium's ineffective gambling law regulation of video game loot boxes. *Collabra: Psychology*, *9*(1), 57641. https://doi.org/10.1525/collabra.57641

Zendle, D., & Cairns, P. (2019). Video game loot boxes are again linked to problem gambling: Results of a large-scale survey. *PLoS ONE*, *14*(3), e0214167. https://doi.org/10.1371/journal.pone.0214167

Zendle, D., Meyer, R., & Ballou, N. (2020b). The changing face of desktop video game monetisation: An exploration of exposure to loot boxes, pay to win, and cosmetic microtransactions in the most-played Steam games of 2010–2019. *PloS ONE*, *15*(5), e0232780. https://doi.org/10.1371/journal.pone.0232780

Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020a). The prevalence of loot boxes in mobile and desktop games. *Addiction*, *115*(9), 1768–1772. https://doi.org/10.1111/add.14973

Zuriff, G. E. (1970). A comparison of variable-ratio and variable-interval schedules of reinforcement. *Journal of the Experimental Analysis of Behavior*, *13*(3), 369–374. https://doi.org/10.1901/jeab.1970.13-369

Author information

Seppy Pour – LLB (Hons), BA, LLM, Principal Consultant, Kun Consulting Group
Address: NSW 2006, Sydney, Australia
E-mail: seppypour@gmail.com
ORCID ID: https://orcid.org/0000-0001-9032-062X

Conflicts of interest

The author 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 – August 25, 2023
Date of approval – September 20, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:347.21:004.4
EDN: https://elibrary.ru/uxqado
DOI: https://doi.org/10.21202/jdtl.2024.18

Опыт правового регулирования лутбоксов в различных странах: сравнительный анализ

Сэппи Пор

Группа компаний «Кун Консалтинг», Сидней, Австралия

Ключевые слова

азартные игры,
видеоигры,
виртуальный товар,
защита прав потребителей,
игровая индустрия,
лицензирование,
лутбокс,
право,
сравнительное правоведение,
цифровые технологии

Аннотация

Цель: показать как использование новой бизнес-модели, получившей название лутбоксов и лежащей в основе современных видеоигр, стало правовой проблемой для юрисдикций разных стран.

Методы: опираясь на существующую литературу и современные источники, в статье раскрываются потенциальные негативные последствия использования лутбоксов, проводится комплексный анализ действующего или предлагаемого регулирования, а также сравнение подходов, применяемых в различных национальных юрисдикциях.

Результаты: в данной статье рассматривается растущая обеспокоенность вокруг широкого распространения особой формы внутриигровых покупок называемой лутбоксами. Она подвергается резкой критике на том основании, что лутбоксы предположительно являются своего рода азартной игрой в составе видеоигры. Исходя из этого, в данной статье приводятся аргументы в пользу их законодательного регулирования. Изучив нормативно-правовую базу в странах, которые уже приняли меры против использования лутбоксов, таких как Бельгия, Нидерланды, Китай, Япония и Республика Корея, а также в странах, где в настоящее время обсуждается вопрос их регулирования, подчеркивается необходимость принятия мер по защите потребителей в игровой индустрии. Особенно это относится к уязвимым слоям населения, подверженных вредным последствиям, связанным с азартными играми. Кроме того, отмечается необходимость обеспечения этичного и ответственного использования лутбоксов, а также снижения рисков для здоровья и финансовых рисков, связанных с использованием данной бизнес-модели.

Научная новизна: в работе представлено сравнительное исследование проблем действующего или проектируемого социального регулирования лутбоксов в видеоиграх, решение которых предлагается искать на основе баланса между инновациями в игровой индустрии, защитой потребителей и благополучием пользователей, что в конечном итоге будет способствовать созданию более здоровой среды для геймеров.

Практическая значимость: представленное исследование подчеркивает международный масштаб рассматриваемой проблемы, различие принятых в странах регулятивных мер юридического и этического характера, направленных на решение психологических, социальных и финансовых последствий, связанных с распространением лутбоксов в видеоиграх, оценку которым еще предстоит дать в дальнейшем с учетом полученных данных в отрасли игровой индустрии.

Для цитирования

Пор, С. (2024). Опыт правового регулирования лутбоксов в различных странах: сравнительный анализ. *Journal of Digital Technologies and Law, 2*(2), 345–371. https://doi.org/10.21202/jdtl.2024.18

Список литературы

Brenner, R., & Brenner, G. A. (1990). *Gambling and speculation: A theory, a history, and a future of some human decisions*. Cambridge University Press.

Deans, E. G., Thomas, S. L., Derevensky, J., & Daube, M. (2017). The influence of marketing on the sports betting attitudes and consumption behaviours of young men: implications for harm reduction and prevention strategies. *Harm Reduction Journal*, *14*, 1–12. https://doi.org/10.1186/s12954-017-0131-8

Devereux, E. (1979). Gambling. In *The International Encyclopedia of the Social Sciences* (vol. 17). New York: Macmillan.

Drummond, A., & Sauer, J. D. (2018). Video game loot boxes are psychologically akin to gambling. *Nature human behaviour*, *2*(8), 530–532. https://doi.org/10.1038/s41562-018-0360-1

Drummond, A., Hall, L. C., & Sauer, J. D. (2022). Surprisingly high prevalence rates of severe psychological distress among consumers who purchase loot boxes in video games. *Scientific Reports*, *12*(1), 16128. https://doi.org/10.1038/s41598-022-20549-1

Etchells, P. J., Morgan, A. L., & Quintana, D. S. (2022). Loot box spending is associated with problem gambling but not mental wellbeing. *Royal Society Open Science*, *9*(8), 220111. https://doi.org/10.1098/rsos.220111

Gong, L., & Rodda, S. N. (2022). An exploratory study of individual and parental techniques for limiting loot box consumption. *International Journal of Mental Health and Addiction*, *20*, 398–425. https://doi.org/10.1007/s11469-020-00370-5

Greer, N., Rockloff, M., Hing, N., Browne, M., & King, D. L. (2023). Skin gambling contributes to gambling problems and harm after controlling for other forms of traditional gambling. *Journal of Gambling Studies*, *39*, 225–247. https://doi.org/10.1007/s10899-022-10111-z

Griffiths, M. D. (1995). *Adolescent gambling*. London: Routledge.

Hing, N., Lole, L., Thorne, H., Sproston, K., Hodge, N., & Rockloff, M. (2023b). 'It Doesn't Give Off the Gambling Vibes… It Just Feels Like a Part of the Game': Adolescents' Experiences and Perceptions of Simulated Gambling While Growing Up. *International Journal of Mental Health and Addiction*. https://doi.org/10.1007/s11469-023-01119-6

Hing, N., Russell, A. M., King, D. L., Rockloff, M., Browne, M., Newall, P., & Greer, N. (2023a). Not all games are created equal: Adolescents who play and spend money on simulated gambling games show greater risk for gaming disorder. *Addictive Behaviors*, *137*, 107525. https://doi.org/10.1016/j.addbeh.2022.107525

King, D. L., & Delfabbro, P. H. (2018). Predatory monetization schemes in video games (eg 'loot boxes') and internet gaming disorder. *Addiction*, *113*(11), 1967–1969. https://doi.org/10.1111/add.14286

Liao, S. X. (2016). Japanese console games popularization in China: Governance, copycats, and gamers. *Games and Culture*, *11*(3), 275–297. https://doi.org/10.1177/1555412015583574

Primi, C., Sanson, F., Vecchiato, M., Serra, E., & Donati, M. A. (2022). Loot boxes use, video gaming, and gambling in adolescents: Results from a path analysis before and during COVID-19-pandemic-related lockdown in Italy. *Frontiers in psychology*, *13*, 1009129. https://doi.org/10.3389/fpsyg.2022.1009129

Rockloff, M., Russell, A. M., Greer, N., Lole, L., Hing, N., & Browne, M. (2021). Young people who purchase loot boxes are more likely to have gambling problems: An online survey of adolescents and young adults living in NSW Australia. *Journal of Behavioral Addictions*, *10*(1), 35–41. https://doi.org/10.1556/2006.2021.00007

Sang, Y., Park, S., & Seo, H. (2017). Mobile Game Regulation in South Korea: A Case Study of the Shutdown Law. In D. Jin (Eds.). Mobile Gaming in Asia. *Mobile Communication in Asia: Local Insights, Global Implications* (pp. 55–72). Springer, Dordrecht. https://doi.org/10.1007/978-94-024-0826-3_4

So, Sh., & Westland, J. Ch. (2012). Red Wired: China's Internet Revolution. Marshall Cavendish.

Staddon, J. E. R, & Cerutti, D. T. (2003). Operant conditioning. *Annual Review of Psychology*, *54*, 115–144. https://doi.org/10.1146/annurev.psych.54.101601.145124

Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, *13*(3), 415–432. https://doi.org/10.1002/poi3.250

Xiao, L. Y. (2023). Breaking Ban: Belgium's ineffective gambling law regulation of video game loot boxes. *Collabra: Psychology*, *9*(1), 57641. https://doi.org/10.1525/collabra.57641

Zendle, D., & Cairns, P. (2019). Video game loot boxes are again linked to problem gambling: Results of a large-scale survey. *PLoS ONE*, *14*(3), e0214167. https://doi.org/10.1371/journal.pone.0214167

Zendle, D., Meyer, R., & Ballou, N. (2020b). The changing face of desktop video game monetisation: An exploration of exposure to loot boxes, pay to win, and cosmetic microtransactions in the most-played Steam games of 2010–2019. *PloS ONE*, *15*(5), e0232780. https://doi.org/10.1371/journal.pone.0232780

Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020a). The prevalence of loot boxes in mobile and desktop games. *Addiction*, *115*(9), 1768–1772. https://doi.org/10.1111/add.14973

Zuriff, G. E. (1970). A comparison of variable-ratio and variable-interval schedules of reinforcement. *Journal of the Experimental Analysis of Behavior*, *13*(3), 369–374. https://doi.org/10.1901/jeab.1970.13-369

Сведения об авторе

Пор Сэппи – бакалавр права (по углубленной программе), бакалавр искусств, магистр права, главный консультант, группа компаний «Кун Консалтинг»
Адрес: Австралия NSW 2006, г. Сидней
E-mail: seppypour@gmail.com
ORCID ID: https://orcid.org/0000-0001-9032-062X

Конфликт интересов

Автор сообщает 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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 25 августа 2023 г.
Дата одобрения после рецензирования – 20 сентября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:346.6:004.4
EDN: https://elibrary.ru/vdvuuk
DOI: https://doi.org/10.21202/jdtl.2024.19

Prospects and Issues Concerning the Regulatory Regime of E-Payment System in Nigeria

Ismaila Ozovehe Haruna ✉
Prince Abubakar Audu University, Anyigba, Nigeria

Paul Atagamen Aidonojie
Kampala International University, Kampala, Uganda

Onivehu Julius Beida
Bingham University, Karu, Nigeria

Keywords

authentication,
digital technologies,
digitalization,
electronic payments,
electronic signature,
electronic transaction,
law,
Nigeria,
privacy,
security

Abstract

Objective: to reveal the legal challenges impeding the smooth operation of electronic payment systems in Nigeria, given that Nigerian official bodies and individuals have already taken some steps to regulate the electronic payment system in the country, but the said step are insufficient.

Methods: the study is built on several approaches to the issues of the legal regime of electronic payments in Nigeria. Alongside with the doctrinal interpretation of the legal framework regulating the relations associated with the use of electronic payment system, the authors used sociological cognitive tools and conducted a survey of respondents residing in different geopolitical zones of Nigeria. The description and analysis of the data obtained shows the actual attitude of the respondents to the ongoing processes.

Results: international regulation and national legislation on electronic payments in force in Nigeria were examined. The study revealed that e-payments are an effective means of transactions but there are some legal challenges that may hinder the smooth use of e-payments in Nigeria. It was found that although the country has enacted a number of laws relating to the regulation of banking and other financial activities, they are not sufficient to address the challenges posed by modern technologies. The article reflects

✉ Corresponding author

the issues of electronic signature, trust in technology, data privacy, security of electronic transactions, fraud, authentication and authorization, certainty of rights and obligations, jurisdiction and platforms for resolving online disputes, taxation of electronic payments, and others. The authors note that the task of creating a secure digital environment for the smooth operation of e-commerce and e-payments in Nigeria should not be solely imposed on the government.

Scientific novelty: by the example of one of the most promising African states, the authors revealed a spectrum of issues related to the work of electronic payment systems, supporting it with a survey of public opinion. They managed to find out the citizens' attitude to a number of issues that are most often faced when using the system of electronic payments, and possible areas of change.

Practical significance: the current legal issues raised in the study largely hinder the smooth use of the electronic payment system in Nigeria. Hence, the possible ways to improve it suggested by the authors are increasingly significant.

For citation

Haruna, I. O., Aidonojie, P. A., & Beida, O. J. (2024). Prospects and Issues Concerning the Regulatory Regime of E-Payment System in Nigeria. *Journal of Digital Technologies and Law, 2*(2), 372–393. https://doi.org/10.21202/jdtl.2024.19

Contents

Introduction

The advent of the internet brought with it several blessings (Iriobe & Akinyede, 2017). One of those blessings is the electronic payment system which is a payment solution software that facilitates the transfer of monetary values using digital resources (Adkwodimmah & Ochei, 2019). The various benefits of electronic payments, which include; speed, anonymity, openness, inter-operability, digitisation, and global acceptability, have made it a choice medium of real-time payment for a variety of transactions (Dupas et al., 2018).

However, in Nigeria, the trend of technology in virtually all sectors of the Nigerian economy (most especially the banking sector) is no doubt laudable (Sobehart, 2016). This is concerning the fact that most of the activities within the banking sector have also been digitalised, there making the transaction a smooth ride between parties involved in commercial activities (Aidonojie & Ong Argo, 2022). One of the most beneficial areas that have been well enhanced with the use of technology is the e-payment system (Sokolowska, 2015). The e-payment system enables an individual to pay for any form of transaction with ease without having physical cash or contact with other parties. However, suffices to opine that this development, which enhanced human activities, also came with some concomitant forms of threats to the application of e-payment in the conduct of contractual and financial-related transactions (Sokolowska, 2015). This is a result of abuse by bad actors that exploit the loopholes created by inadequate legislation on an e-payment system in Nigeria. The situation is further exacerbated by a low level of I.T know-how by the majority of individuals who, oftentimes, (were only compelled by circumstances too) use the e-payment channels for transactions.

Furthermore, other key challenges brought by the trending of e-payment include, but are not limited to: e-signature, 'Trust and confidence', 'Privacy', 'Security engineering for e-transactions', 'Fraud', 'Authentication and Authorisation', 'Certainty of Rights and Obligations', 'Jurisdiction and Forum on Internet Disputes' 'Taxation on e-payment'. These listed challenges are majorly mitigating the smooth use of e-payment in Nigeria (Laven & Bruggink, 2016). Although there are laws concerning the regulation of banking activities and other financial activities, however, these laws are not sufficient to cater to threat technology-related issues (Gabor & Brooks, 2017). Furthermore, it suffices to state that irrespective of the challenges concerning the use of the e-payment system in Nigeria, the central bank of Nigeria (Omoyajowo, 2021), which is the supervisory authority or stakeholder of the Nigerian financial system, seems to have initiated some steps toward the regulation of e-payment systems in Nigeria, however, several infrastructure, legal and I.T. related challenges still bedevil the smooth operation of e-payment. These challenges can only be met by expanding the scope of some of the existing laws while amendments are put in place where necessary (Aidonojie & Ong Argo, 2022).

It is concerning the above that this study sort to adopt a hybrid method of study in analysing the laws concerning e-payment systems in Nigeria. The study will also embark on a cursory review concerning the conceptual nature of e-payment in Nigeria. The study will also identify some of the legal issues and challenges mitigating the e-payment system in Nigeria and further propose possible remedies for enhancing the e-payment system in Nigeria.

1. Legal Framework concerning E-Payment in Nigeria

The concept of e-payment has received global recognition, in this regard, there are international that regulate e-payment. In this regard, it suffices to state that in Nigeria the international and national laws concerning e-payment. These laws as they relate to e-payment are examined as follows;

United Nations Commission for International Trade Law Model Law on Electronic Signatures (UNCITRAL) came about as a reaction to the increased use of electronic authentication techniques as a replacement for handwritten signatures and other traditional modes of authenticating transactions. UNCITRAL suggested the need for a specific legal regime to reduce uncertainty as to the legal effect arising from the use of such modern techniques (i.e «electronic signatures»). The need for legal harmony, as well as technical interoperability in legislation on electronic transactions at the international level, was seen as a desirable objective (Tasneem, 2014). The major objectives of the Model Law are as follows:

1. Enabling or facilitating the use of electronic signatures;
2. Providing equal treatment to users of paper-based documentation and users of computer-based information.

These objectives are essential for fostering the economy and efficiency in international trade. However, it suffices to state that these internationals do not have the force of law given the fact that section 12 of the Nigerian constitution requires all internationals to be domesticated and ratified by the National Assembly before they can be enforceable in Nigeria.

Furthermore, it suffices to state that Evidence Act is a national law that also deals with e-payment in Nigeria. The relevance of the Evidence Act is that it gave credence to the significant use of computer-document in related evidence. The greatest challenge to the admissibility of electronic evidence in Nigeria relates to the statutory recognition of electronic documents within the purview of the law. The evidential burden under the Evidence Law in Nigeria concerning the admissibility of documents was provided for under sections 34 and 84 of the Evidence Act, 2011 (as amended) which gave recognition to documents stored in electronic forms. These provisions were absent in the Evidence Act, 1945 which failed to recognize electronic documents. The provisions point out the weight to be attached to admissible statements.

The issues which may arise concerning electronic evidence in Nigeria are as follows: whether computer printouts are admissible in evidence in civil or criminal trials. Assuming they are; would they be considered primary or secondary evidence? Or, are they to be categorised as one the hearsay exceptions? Can electronically generated documents be considered documentary evidence? (Tasneem, 2014).

The Supreme Court of Nigeria held that electronically generated evidence is admissible. Also, in Kajala V. Noble (1982) 75 CR APP R.149 the court upheld the admissibility of a video recording of the original BBC news film which shows the defendant participating in a riot. The Courts in Nigerian Courts have adopted a liberal approach in interpretation and application concerning the Evidence Act and existing legal rules to accommodate computer printouts and kindred types of evidence.

It also suffices to state that the government in Nigeria has shown greater awareness of the need to strengthen cyber security. To this end, it has initiated several policies and laws which include: the registration of GSM users in 2011 and the centralised biometric identification system for the banking industry, known as Bank Verification Number (BVN), introduced by the Central bank of Nigeria (CBN). In furtherance of this effort, the first legislation that specifically deals with cyber security was passed in 2015. The Cybercrime Act 2015 gives effect to the ECOWAS directive on fighting crime locally and globally.

By Section 58 of the Act, financial institutions have been recognised as stakeholders in the cyber security framework. The term 'Financial Institution' is defined as "any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business and such other businesses as the Central bank or appropriate authorities may, from time to time, designate. The Principal responsibilities placed on financial institutions are contained in Part IV of the Act (Ezike, 2013). However, the Cyber Crime Act is not the primary legislation that regulates e-payment but rather the incidence of cyber security in Nigeria.

Furthermore, in an attempt to place Nigeria on the right pedestal in the quest of sustaining the gains of cyberspace and ensuring Nigeria taps into the benefits that come with globalisation, the Nigerian legislature proposed the Electronic Transaction Bill (Abubakar & Adebayo, 2015). The bill proposed salient provisions which when passed would advance the cause of e-payment in Nigeria. Part III of the Bill provides for the validity of electronic transactions and aspects governing the formation of electronic agreements. Part IV of the Bill provides for the liability of online intermediaries and online content editors as well as the protection of online users. Part V regulates various facets of electronic commerce, such as consumer protection, and online advertising of electronic commerce operations. Part VI deals with security in the digital economy. The bill also made provisions for the integrity of information and recognition of foreign electronic documents and signatures.

Although the Bill has not yet been assented to by the Nigerian government, however, if the Bill is finally passed into law, it will help in providing confidence to the business community as to the reliability and enforceability of their various business transactions online. It will as well accelerate the goal of achieving economic growth by ensuring seamless and accurate contractual and financial transactions, most especially issues of e-payment.

2. Legal Issues and Challenges concerning E-payment in Nigeria

2.1. Privacy

Electronic transactions ring with them the opportunity for citizens and government to collect customer or data subjects' information that may later be used for data marketing or as a key input to operational and policy decision-making (Tasneem, 2014). Although electronic transactions provide a vista of opportunities to citizens, it nevertheless exposes them to threats to personal privacy while online. This, therefore, calls for strict data security

procedures to protect citizens from the activities of illegal purveyors of information, who may use citizens' details for purposes not connected to the reasons for collecting such data.

Although there is a specific provision of the constitution concerning citizens' right to privacy, there is still room for specific laws on data privacy. Section 37 of the Nigerian Constitution provides as follows: "The privacy of every Nigeria citizens, their telephone conversation, homes, correspondence, and telegraphic communications is therefore guaranteed and protected"[1]. However, this may not be adequate or sufficient to cater to the issues and complexities of personal data processing. A good example of Nigeria's adapting is the United Kingdom Data Protection Act which has salient Principles.

The principles are enumerated as follows:

"1. Data shall be processed fairly and lawfully;

2. It is only obtained for one or more specific and lawful purposes;

3. It must be accurate and seem to be up-to-date;

4. It must not be kept for longer than required or necessary;

5. It is required to be processed by the data subject's rights;

6. It is kept secure or safe using organisation and technical methods;

7. Furthermore, It is not transferred or move out of the European Economic Area (EEA) except or unless there is an adequate or sufficient level of protection for the data subject"[2].

2.2. Certainty of Rights and Obligations

A cardinal component of any successful market economy in the digital environment is the existence of the rule of law and the legal enforceability of written agreements and transactions that follow predetermined rules of notice, disclosure rights, and obligations (Zhaohui, 2012). Just as obtainable in traditional payment systems, issues of certainty of rights and obligations occupy important space in the e-payment discussion. This, particularly, relates to:

1. Ascertaining when an e-payment can be said to be far-reaching or complete;

2. Whether or not e-payment operates to acquit payment responsibility in a commercial business;

3. Beneficiary's access to capitals that were transferred by e-payment;

4. Revocability of e-payment contract.

Concerning the above, it suffices to state that there seems to be an absence of a definitive legal framework on this issue, which continues to be placed in a haze of uncertainty and unpredictability of the rights of the parties to an electronic payment transaction. Incidentally, the balance of power mostly weighs in favour of the banks, who are the service provider, as against the consumers who are oftentimes foisted with a one-sided contract. Unfortunately, there is, as of now, no legislation on the aforementioned issues in Nigerian jurisprudence.

---

1 Constitution of the Federal Republic of Nigeria 1999. https://clck.ru/3B7Cpa

2 Nigerian Data Protection Act. https://clck.ru/3B7DZp

2.3. Fraud

Altough, e-payment systems seem to have a lot of relevances to the Nigerian economy, however, there huge issues relating to cyber crime and fraud in Nigeria, that the Nigerian government have been unable to stem (Aguda, 2021). One of the areas of fraud in E-payment is 'Phishing'. Phishing involves the unsolicited sending of an e-mail to another person. This kind of e-mail purports to be from a financial institution, but it may sometimes be said to be from a government agency where the recipient is disguised as a contractor requesting that you send some key parts of your personal information for some official or administrative reasons (e.g to make an update on your account). The e-mail sometimes adds a warning that failure to forward this information may result in a suspension or closing of your account. This specie of fraud is committed using the mechanism of the internet and involves a party misrepresenting their identity to lure the victim into releasing personal information such as access codes and passwords, which they now use for their criminal benefit. Such activity may include illegal access to the victim's bank accounts to siphon funds from them.

Another area of fraud in e-payment is 'Identity Theft'. Here, a criminal gets access to your personal information through any means including phishing. This may then be used to open bank accounts for illegal transactions purportedly in your name, such as loan facilities, using state documents such as passports and driving licenses. The emergence of e-payment systems, in the information age, opens citizens up to these types of crimes. In many jurisdictions, specific laws make it a crime to use another person's identity for personal gain. In Nigeria, at the moment the law which deals directly with the prevention or criminalising of this kind of fraud is the Cybercrime Act, of 2015.

2.4. Electronic Authentication

Identity authentication methods help in reducing the speed and efficiency of electronic transactions (Aguda, 2021). Financial institutions have, therefore, adopted alternative authentication methods. These include:

1) personal identification numbers and Passwords;

2) digital certificates using open key infrastructure;

3) microchip-based devices which may include smart cards or other relevant types of tokens;

4) database comparisons or contrasts e.g. fraud screening applications;

5) biometric ID devices.

These authentication methods provide differing levels of security and reliability. The cost and complexity of their underlying infrastructures also vary. It has, therefore, been observed that the choice of which technique(s) to use should be commensurate with the risks in the products and services for which they control access

3. Jurisdiction and Forum for Settlement of E-payment Dispute

A key component of internet-related activities is its universal reach and wider coverage compared to interactions through other traditional mediums. This phenomenon obviates the interference of time, borders, space, and other physical obstacles in the way of speedy and seamless transactions. Merchants are, therefore, gifted the opportunity of harvesting from a wide audience and an endless horizon. As such, there arise issues relating to the determination of internet jurisdiction, as online contracts are not territory-specific. Where disputes exist concerning contracts executed through the internet, and where parties to the online transaction live in different jurisdictions, what would be the factors that would inform the forum for settlement of such dispute? Issues may also revolve around a situation where a person floats a website on his home server and gives access to the such server by people from different locations around the world; does such a fellow become a universal citizen, subject of all jurisdictions across the globe? (Adkomolede, 2008).

1. To give effect to the jurisdiction governing a certain dispute over the internet, certain pertinent questions must be asked and answered:

2. Where did the internet-facilitated negotiation or conduct take place?

How does an internet-related activity or transaction have an effect within a state jurisdiction?

Incidentally, there are yet to be established subject-specific rules concerning 'model laws' dealing with internet jurisdiction. More so, the United Nations Commission on International Trade Laws (UNCITRAL) Model Law on E-commerce and the United Nations Convention on the use of Electronic Communications in International Contracts are yet to be domesticated in Nigeria. In this regard, by section 12 of the Nigerian constitution, international laws yet to be domesticated have little or no legal effect.

However, without prejudice to the above analysis, the general rule in internet contracts is that Jurisdiction is determined by ascertaining the place or country where a particular online contract was performed. In instances where the performance of internet-related activities or contracts took place in many places at the same time, the relevant jurisdiction will be the state where the dispute arose. Also, the place of domicile of the parties may be relevant in determining jurisdiction. However, the general rule applicable to consumer products is that consumers are allowed to sue and be sued in their home states.

4. Trust in E-Payment

The idea of e-payment was to breach the walls of distance and time between consumers and merchants during transactions (Jessah, 2019). This implies that most of the commercial and contractual activities that take place between the consumer and the merchant were carried out in the virtual space. Three key areas of concern may be identified as trust related:

1) expertise: this has to do with the belief in the relative skills and technical know-how of the trusted party;

2) benevolence: this relates to the belief that the other party has the disposition to deal with the customer in good faith while in the business and making profits; and

3) integrity: this is the belief that the trusted party would play by generally accepted rules of conduct by dealing with him in an honest and trustworthy manner. And that he would keep his end of every bargain and promise.

E-transactions by their very nature are more complex than the regular off-the-shelf shopping carried out in the traditional environment. It, therefore, means that trust is an essential element that grounds its operations. It is particularly difficult to establish trust between the customer and the merchant in an online transaction. This is because online transactions come with the shield of anonymity between the parties carrying out the transaction in a virtual environment (Acha, 2008).

5. Taxation in E-Payment

The economic leeway created by internet sales has generated traffic for online transactions which tends to push to the background the traditional paper-oriented modes of transaction. However, existing tax laws were not modeled to cater to the significant changes wrought by the internet phenomenon or "New Economy" (Udobi-Owoloja et al., 2020). The question in this regard is: how do you tax goods purchased online from consumers who do not reside within the state jurisdiction of the vendor's business or platform; or, should internet transactions even be taxed at all? Existing state and local laws on taxation are no doubt enormously challenged by the advent of electronic transactions in ways never before envisaged. The law regulating tax-related matters in Nigeria is the Federal Inland Revenue Service (FIRS) Establishment Act 2007, which empowers the FIRS to impose and collect tax. The traditional tax system relies on ascertaining where particular economic activity is located, but the internet has the potential of allowing an individual to carry out business transactions in many different countries while sitting at the same desk. These issues become more compounded with the fact that electronic commerce holds tremendous potential as a huge source of government revenue in the information age which comes with increasing automation of transactions in Nigeria.

Other relevant issues annexed to taxation in e-payment include: what are the infrastructural facilities required for a seamless, painless, and fair commerce tax system; how does the government police tax deductions without jeopardizing the need for the growth and development of the internet? Other issues are issues of tackling tax evasion and fraud. These, therefore raise the need for a law that would adequately cater to economic activities over the internet to be evolved, to enhance the government revenue base and sustain the growth and development of e-commerce in Nigeria.

6. Presentation and Analysis of Data

The data were through the use of an online questionnaire method of survey and it is therefore analysed as follows.

6.1. Sample Size and Techniques

Concerning the sample size of this study, the researchers adopt 302 respondents residing in the various geo-political in the Federal Republic of Nigeria as their sample size.

In this regard, in identifying the various respondents to respond to or react to the questionnaire, the researchers utilize simple random sampling techniques or methods. The reason for adopting a simple random sampling method in identifying the respondents is concerning the fact that a simple random sampling technique is considered more suitable and acceptable technique that are more reliable in arriving at a positive result (Majekodunmi et al., 2022). Furthermore, it has been adjudged in several studies that a sampling simple random technique possesses the following qualities (Aidonojie & Ong Argo, 2022) as follows:

1) that it is more suitable to sample a population from a heterogeneous;
2) it is more authentic in arriving at an unbiased result;
3) it is a hassle-free or easy method of sampling a population;
4) that is very suitable in a hybrid method of legal research.

6.2. Data Analysis

Concerning the data gathered and obtained in this study with aid of a questionnaire, it is therefore analysed as follows.

Table 1 shows the regions of the Federal Republic of Nigeria where the respondents reside.

Table 1. The geopolitical zone in Nigeria resided by respondents

S/N	Geopolitical Zones in Nigeria	Responses of Respondents	Percent
1	North Central	58	19.2%
2	North East	38	12.6%
3	North West	44	14.6%
4	South East	57	17.2%
5	South South	65	21.5%
6	South West	49	14.5%
	TOTAL	302	100%

Table 2 shows the answers to the question if electronic payments have prospects in the commercial sector of Nigeria.

Table 2. Valid respondents verifying that e-payment has several prospects in commercial activities

Answer	Cluster of Response	Percent
Valid Yes	247	82.1%
Valid No	54	17.9%
Total	301	100%

Table 3 shows various prospects of electronic payments in commercial activity of Nigeria mentioned by the respondents.

Table 3. Valid Cluster of Some of the prospect of e-payment system identified by the respondents

Answers	Cluster of Response	Percentage
It is a convenient method of transferring or payment of money	222	88.8%
It is cost effective	202	80.8%
E-payment has made it a choice medium of real-time payment for a variety of transactions	192	76.8%
It has a global acceptability	183	73.2%
Anonymity, that is enables a user to keep their identity confidential, if they so wish	166	66.4%
There is the speed in settlement of a transaction	107	42.8%

Table 4 shows that most of the respondents realize the presence of problems related to the functioning of e-payment system in Nigeria.

Table 4: Valid verification of challenges concerning the e-payment system in Nigeria

Answers	Cluster of Response	Percent
Valid Yes	247	82.1%
Valid No	54	17.9%
Total	301	100%

Table 5 shows the problems related to e-payment system in Nigeria, in the order of significance for the respondents.

Table 5: Valid cluster of challenges of an e-payment system in Nigeria identified by the respondents

Answers	Cluster of Responses	Percentage
Ineffective and inadequate legal framework concerning e-payment in Nigeria	236	94%
The challenge of data privacy of e-payment user	231	92%
Certainty of rights and obligations when there is a failure of an e-payment transaction	90	35.9%
Incidence of fraud	195	77.7%
A complex process of electronic authentication of e-payment users	88	35.1%
Jurisdiction and forum for settlement of an e-payment dispute	138	55%
Challenges in taxing e-payment mode of transaction	188	74.9%
Poor internet services	215	85.7%

Table 6 lists possible remedies to the problems related to e-payment system in Nigeria, suggested by the respondents.

Table 6: Valid cluster of possible remedies to enhance the e-payment system in Nigeria

Answers	Cluster of Responses	Percentage
Amendment of the legal framework to reflect adequate regulation of digital payment	221	88.4%
Provision of an avenue of safeguarding data privacy rights of the e-payment user	223	89.2%
Banks and various stakeholders must ensure to simplify the process involved in electronic authentication of e-payment	65	26%
Domesticating international treaties that seem to resolve issues about Jurisdiction and forum for settlement of an e-payment dispute	131	52.4%
Curbing incidence of internet fraud through legal and technological means	215	86%
Provision of effective internet services by services provider	212	84.8%

6.3. Discussion of Findings

The data obtain through the questionnaire and analysed above is hereby discussed as follows. In this regard, table 1 show that there are 302 respondents from the various geopolitical zones in Nigeria who responded to the questionnaire. In this regard, it suffices to state that the respondent is well enlightened and knowledgeable to reiterate with an informed response concerning issues relating e-payment system in Nigeria. It is concerning that in table 2, 82.1 % of the respondents identify that there several prospects concerning the introduction of e-payment in Nigeria. Furthermore, in table 3, the respondents through a cluster of responses identify some of the prospects of an e-payment as follows:

1) 80.8 % of the respondents stated that it is cost-effective;

2) 88.8 % agreed that it is a convenient method of transferring or settlement of a transaction;

3) 42.8 % identify that there is the speed in settlement of transactions through e-payment;

4) 66.4 % was of the view that it enables anonymity of identity of e-payment users if they so wish;

5) 73.2 % stated that it has a global acceptability;

6) Furthermore, 76.8 % of the respondents agreed that e-payment has made it a choice medium of real-time payment for a variety of transactions.

Concerning the above, it suffices to state that findings in table 3, is not indifferent from other studies that the use of technology has greatly enhanced financial transaction. However, in table 4, 82.1 % of the respondents were able to identify that there are challenges that often mitigate the smooth use of the e-payment system in Nigeria. In this regard, in table 5, the respondents were able to identify some of the challenges of an e-payment system in Nigeria as follows;

1) 94 % of the respondents stated that there is an ineffective and inadequate legal framework concerning e-payment in Nigeria;

2) 92 % of the respondents agreed that there is a challenge to the data privacy of e-payment user;

3) 35.9 % stated certainty of rights and obligations when there is a failure of an e-payment transaction as a challenge to the e-payment system;

4) 77.7 % and 35.1 % identify the incidence of fraud and a complex process of electronic authentication of e-payment users respectively as a challenge to the e-payment system;

5) 55.1 % of the respondents identify jurisdiction and forum for settlement of the e-payment dispute as also a major challenge to the e-payment system in Nigeria;

6) Furthermore, 74.9 % and 85.7 % of the respondents' Challenges in taxing e-payment mode of transaction and Poor internet services respectively often constitute a challenge.

It suffices to state that the relevance of e-payment to Nigeria's financial system is no doubt laudable. This is concerning the fact that the rigorous process involved in the manual payment of transactions has been greatly resolved. Furthermore, it also aids in implementing a cashless policy which the Nigerian government seems to target for some time. In this regard, it suffices to state that given the relevance and positive impact of e-payment on the Nigeria economy, in table 6, the respondents further identify some possible remedies concerning the challenges of an e-payment system in Nigeria as follows:

1) 88.4 % of the respondents stated that there is a need to amend the legal framework to reflect adequate regulation of digital payment;

2) 89.2 % agreed that government should provide an avenue for safeguarding data privacy rights of the e-payment user;

3) 26 % stated that banks and various stakeholders must ensure to simplify the process involved in electronic authentication of e-payment;

4) 52.4 % identify domesticating international treaties that seem to resolve issues about Jurisdiction and forum for settlement of an e-payment dispute;

5) 86 % stated that curbing the incidence of internet fraud through legal and technological means will aid in enhancing the e-payment system;

6) Furthermore, 84.8 % of the respondents stated that there is a need for the provision of effective internet services by services provider.

Concerning the above, it suffices to opine that if the above possible remedy as identified by the respondents is realized by the various stakeholder of the Nigerian economy, it will aid in enhancing the e-payment system in Nigeria.

Conclusion

The modern world has collapsed into a smaller more accessible structure. Elements that hitherto constitute barriers to human interactions in form of communication, business, and governance have been bulldozed by the phenomenon of the internet- time, space and geographic elements have been shrunk into the clicks of computers and other affiliated digital devices. The entire cosmos of human life is today influenced by technological innovations, which dimensions and capabilities continue to throw challenges at the existing traditional laws both at the domestic and international levels. The computer and the internet have helped man to conquer formerly inaccessible territories in terms of development and advancement of the course of humanity.

This very important development in the history of man has, however, due to the vanity and excesses of human nature been subject to manipulations of information, cyber-thefts, hacking, cyber-laundering, hacking, spamming, and several other nefarious activities on the internet. Nigeria has known its fair share of these species of threats in her cyberspace, which consequently call for efforts at ensuring the safety and security of the internet,

including e-payment facilities in the country. This paper explored the forms of security systems which helped in ensuring the integrity of e-payment facilities in Nigeria and also ex-rayed the existing laws relating to e-payment in Nigeria to analyse the areas of strengths and weaknesses.

The paper observed that there have been some commendable efforts by the legislature in Nigeria, which led to the passing of some key e-payment-related Bills. It, however, recommends immediate assent to these Bills to ensure that their operation results in the desired healthy atmosphere for the conduct of electronic transactions in Nigeria. However, it must be stated that the desire for a safe and healthy digital environment for the smooth running of e-commerce and e-payment in Nigeria is not a task solely to be left in the hands of the government. Operators of online businesses must ensure that necessary 'criminal intelligence analyses are fully integrated in the business operations. Cyber-security must also be of premium to e-commerce operators and should therefore develop broad security programs that would take care of contingencies.

References

Abubakar, A. S., & Adebayo, F. O. (2014). Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects. *Mediterranean Journal of Social Sciences*, *5*(2), 215. https://doi.org/10.5901/mjss.2014.v5n2p215

Acha, I. A. (2008). Electronic Banking in Nigeria: Concept, Challenges and Prospects. *International Journal of Development and Management Review*, *3*(1), 23–45.

Adkomolede, T. (2008). Contemporary Legal Issues on Electronic Commerce in Nigeria. *Potchefstroom Electronic Law Journal*, *11*(3) 9–18. https://doi.org/10.4314/pelj.v11i3.42234

Adkwodimmah, C., & Ochei, A. I. (2019). Financial Technology and Liquidity in the Nigerian Banking Sector. *Journal of Association of Professional Bankers in Education*, *5*(1), 243–162.

Aguda, O. O. (2021). An Appraisal of the Legal Framework for Online Banking in Nigeria and South Africa. *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law*, *3*(1), 11–17.

Aidonojie, P. A., & Ong Argo, V. (2022). The Societal and Legal Missing Link in Protecting a Girl Child against abuse before and Amidst the Covid-19 Pandemic in Nigeria. *Jurnal Hukum UNISSULA*, *38*(1), 61–80. http://dx.doi.org/10.26532/jh.v38i1.18412

Dupas, P., Karlan, D., Robinson, J., & Ubfal, D. (2018). Banking the Unbanked? Evidence from Three Countries. *American Economic Journal: Applied Economics*, *10*(2), 257–297. https://doi.org/10.1257/app.20160597

Ezike, E. O. (2013). Online Contracts in Nigeria –An Overview. *The Nigerian Juridical Review*, *11*, 53–82.

Gabor, D., & Brooks, S. (2017). The Digital Revolution in Financial Inclusion: International Development in the Fintech Era. *New Political Economy*, *22*(4), 423–436. https://doi.org/10.1080/13563467.2017.1259298

Iriobe, G., & Akinyede, O. M. (2017). The Effect of Financial Technology Services on Banks Customers Satisfaction in Nigeria. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2984215

Jessah, J. E. (2019). E-Commerce in Nigeria: Liability for Loss or Damage to Goods Supplied by a Seller Pursuant to an Electronic Contract. *IJOCLLEP*, *1*(3), 105–114.

Laven, M., & Bruggink, G. (2016). How FinTech is transforming the way money moves around the world. *Journal of Payments Strategy & Systems*, *10*(1), 6–12.

Majekodunmi, T. A., Akintola, J. O., Aidonojie, P. A., Ikubbanni, O. O., & Oyebade, A. A. (2022). Legal Issues in Combating the Scourge of Terrorism; Its Impact on International Trade and Investment: Nigeria as a Case Study. *KIU Journal of Humanities*, *7*(3), 129–139.

Omoyajowo, K. (2021). Crowdfunding Regulatory Framework in Nigeria: An Appraisal of the Highlights of SEC Crowdfunding Regulation. *SSRN Electronic Journal*.

Sobehart, J. R. (2016). The FinTech revolution: Quantifying earnings uncertainty and credit risk in competitive business environments with disruptive technologies. *Journal of Risk Management in Financial Institutions*, *9*(2), 67–78.

Sokołowska, E. (2015). Innovations in the payment card market: The case of Poland. *Electronic Commerce Research and Applications*, *14*(5), 292–304. https://doi.org/10.1016/j.elerap.2015.07.005

Tasneem, F. (2014). Legal Effect of Electronic Contracts in Australia. *Global Research Journal of Engineering, Technology and Innovation*, *3*(1), 020–026.

Udobi-Owoloja, P. I., Ahigbe, B. E., Ubi, A. E., Gbajumo-Sheriff, M. A., & Umoru, B. (2020). Digital Banking and Bank Profitability in Nigeria. *Nigerian Journal of Management Studies*, *20*(2), 24–34.

Zhaohui, L. (2012). Motivation of Virtual Goods Transactions Based on the Theory of Gaming Motivations. *Journal of Theoretical and Applied Information Technology*, *43*(2), 254–260.

Authors informations

Ismaila Ozovehe Haruna – LLB, BL, LL.M, PGDE, Long Essay Coordinator Faculty of Law, Prince Abubakar Audu University, Anyigba – Nigeria
Address: P.M.B 1008 Anyigba, Kogi State, Nigeria
E-mail: Ozovehe.ih@ksu.edu.ng
ORCID ID: https://orcid.org/0009-0006-8773-768X
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=8xkClmoAAAAJ

Paul Atagamen Aidonojie – PhD, Associate Dean of Research Kampala International University, Uganda
Address: Box 20000, Ggaba Road, Kansanga, Kampala, Uganda
E-mail: paul.aidonojie@kiu.ac.ug
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Onivehu Julius Beida – PhD, Head of Department, Public & Private Law, Faculty of Law, Bingham University Karu, Nasarawa State
Address: Bingham University P.M.B 005, KM 26 Abuja- Keffi Expressway Kodope , Karu, Nassarawa State, Nigeria
E-mail: beida.onivehu@binghamuni.edu.ng
ORCID ID: https://orcid.org/0000-0002-6089-5059
Google Scholar ID: https://scholar.google.com/citations?user=fxTBqIMAAAAJ

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 – September 22, 2023
Date of approval – October 21, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:346.6:004.4
EDN: https://elibrary.ru/vdvuuk
DOI: https://doi.org/10.21202/jdtl.2024.19

Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии

Исмаила Озовехе Харуна ✉
Университет принца Абубакара Ауду, Аньигба, Нигерия

Пол Атагамен Айдоноджи
Кампальский международный университет, Кампала, Уганда

Онивеху Джулиус Бейда
Университет Бингема, Кару, Нигерия

Ключевые слова

аутентификация,
безопасность,
конфиденциальность,
Нигерия,
право,
цифровизация,
цифровые технологии,
электронная подпись,
электронная транзакция,
электронные платежи

Аннотация

Цель: выявить правовые проблемы, мешающие бесперебойной работе электронных платежных систем в Нигерии в условиях, когда официальными лицами и нигерийскими органами власти уже предприняты определенные шаги по регулированию системы электронных платежей в стране, но их недостаточно.

Методы: исследование строится на нескольких подходах к изучению вопросов, касающихся правового режима электронных платежей в Нигерии. Наряду с применением доктринального толкования нормативно-правовой базы, регулирующей отношения, связанные с использованием системы электронных платежей, задействован социологический познавательный инструментарий в виде анкетирования респондентов, проживающих в различных геополитических зонах Нигерии. Описание и анализ полученных данных показывает реальное отношение опрошенных лиц к происходящим процессам.

Результаты: рассмотрены международное регулирование и национальное законодательство в области электронных платежей, действующее в Нигерии. Исследование показало, что электронные платежи являются эффективным средством транзакций, однако существует ряд юридических проблем, которые могут мешать беспрепятственному использованию электронных платежей в Нигерии. Установлено, что хотя в стране принят ряд законов, касающихся регулирования банковской и других видов финансовой деятельности,

✉ Контактное лицо

их недостаточно для решения проблем, обусловленных применением современных технологий. В статье нашли отражение вопросы, связанные с применением электронной подписи, доверием к технологиям, конфиденциальностью данных, безопасностью электронных транзакций, мошенничеством, аутентификацией и авторизацией, определенностью прав и обязанностей, юрисдикцией и площадкой для разрешения интернет-споров, налогообложением электронных платежей и др. Отмечается, что задачу создания безопасной цифровой среды для бесперебойной работы электронной коммерции и электронных платежей в Нигерии нельзя возлагать исключительно на правительство.

Научная новизна: на примере одного из перспективных государств Африки раскрывается спектр проблематики, касающийся работы электронных платежных систем, подкрепленный опросом общественного мнения для выяснения отношения по целому ряду вопросов, с которыми чаще всего сталкиваются граждане при использовании системы электронных платежей, и возможных направлений изменений в этой области.

Практическая значимость: актуальные правовые вопросы, поднимаемые в проведенном исследовании, в значительной степени препятствуют нормальному использованию системы электронных платежей в Нигерии, в связи с чем возрастает значимость предлагаемых авторами возможных путей для ее совершенствования.

Для цитирования

Харуна, И. О., Айдоноджи, П. А., Бейда, О. Дж. (2024). Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии. *Journal of Digital Technologies and Law*, *2*(2), 372–393. https://doi.org/10.21202/jdtl.2024.19

Список литературы

Abubakar, A. S., & Adebayo, F. O. (2014). Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects. *Mediterranean Journal of Social Sciences*, *5*(2), 215. https://doi.org/10.5901/mjss.2014.v5n2p215

Acha, I. A. (2008). Electronic Banking in Nigeria: Concept, Challenges and Prospects. *International Journal of Development and Management Review*, *3*(1), 23–45.

Adkomolede, T. (2008). Contemporary Legal Issues on Electronic Commerce in Nigeria. *Potchefstroom Electronic Law Journal*, *11*(3) 9–18. https://doi.org/10.4314/pelj.v11i3.42234

Adkwodimmah, C., & Ochei, A. I. (2019). Financial Technology and Liquidity in the Nigerian Banking Sector. *Journal of Association of Professional Bankers in Education*, *5*(1), 243–162.

Aguda, O. O. (2021). An Appraisal of the Legal Framework for Online Banking in Nigeria and South Africa. *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law*, *3*(1), 11–17.

Aidonojie, P. A., & Ong Argo, V. (2022). The Societal and Legal Missing Link in Protecting a Girl Child against abuse before and Amidst the Covid-19 Pandemic in Nigeria. *Jurnal Hukum UNISSULA*, *38*(1), 61–80. http://dx.doi.org/10.26532/jh.v38i1.18412

Dupas, P., Karlan, D., Robinson, J., & Ubfal, D. (2018). Banking the Unbanked? Evidence from Three Countries. *American Economic Journal: Applied Economics*, *10*(2), 257–297. https://doi.org/10.1257/app.20160597

Ezike, E. O. (2013). Online Contracts in Nigeria –An Overview. *The Nigerian Juridical Review*, *11*, 53–82.

Gabor, D., & Brooks, S. (2017). The Digital Revolution in Financial Inclusion: International Development in the Fintech Era. *New Political Economy*, *22*(4), 423–436. https://doi.org/10.1080/13563467.2017.1259298

Iriobe, G., & Akinyede, O. M. (2017). The Effect of Financial Technology Services on Banks Customers Satisfaction in Nigeria. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2984215

Jessah, J. E. (2019). E-Commerce in Nigeria: Liability for Loss or Damage to Goods Supplied by a Seller Pursuant to an Electronic Contract. *IJOCLLEP*, *1*(3), 105–114.

Laven, M., & Bruggink, G. (2016). How FinTech is transforming the way money moves around the world. *Journal of Payments Strategy & Systems*, *10*(1), 6–12.

Majekodunmi, T. A., Akintola, J. O., Aidonojie, P. A., Ikubbanni, O. O., & Oyebade, A. A. (2022). Legal Issues in Combating the Scourge of Terrorism; Its Impact on International Trade and Investment: Nigeria as a Case Study. *KIU Journal of Humanities*, *7*(3), 129–139.

Omoyajowo, K. (2021). Crowdfunding Regulatory Framework in Nigeria: An Appraisal of the Highlights of SEC Crowdfunding Regulation. *SSRN Electronic Journal*.

Sobehart, J. R. (2016). The FinTech revolution: Quantifying earnings uncertainty and credit risk in competitive business environments with disruptive technologies. *Journal of Risk Management in Financial Institutions*, *9*(2), 67–78.

Sokołowska, E. (2015). Innovations in the payment card market: The case of Poland. *Electronic Commerce Research and Applications*, *14*(5), 292–304. https://doi.org/10.1016/j.elerap.2015.07.005

Tasneem, F. (2014). Legal Effect of Electronic Contracts in Australia. *Global Research Journal of Engineering, Technology and Innovation*, *3*(1), 020–026.

Udobi-Owoloja, P. I., Ahigbe, B. E., Ubi, A. E., Gbajumo-Sheriff, M. A., & Umoru, B. (2020). Digital Banking and Bank Profitability in Nigeria. *Nigerian Journal of Management Studies*, *20*(2), 24–34.

Zhaohui, L. (2012). Motivation of Virtual Goods Transactions Based on the Theory of Gaming Motivations. *Journal of Theoretical and Applied Information Technology*, *43*(2), 254–260.

Сведения об авторах

Харуна Исмаила Озовехе – адвокат, бакалавр права, магистр права, аспирант в области педагогики, консультант отдела аспирантуры
Юридический факультет, Университет принца Абубакара Ауду
Адрес: Нигерия, штат Коги, г. Аньигба, P.M.B 1008
E-mail: Ozovehe.ih@ksu.edu.ng
ORCID ID: https://orcid.org/0009-0006-8773-768X
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=8xkClmoAAAAJ

Айдоноджи Пол Атагамен – PhD, заместитель декана по научной работе, Кампальский международный университет
Адрес: Уганда, г. Кампала, район Кансанга, Ггаба роуд, 20000
E-mail: paul.aidonojie@kiu.ac.ug
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Бейда Онивеху Джулиус – PhD, заведующий кафедрой публичного и частного права, юридический факультет, Университет Бингема
Адрес: Нигерия, штат Насарава, г. Кару, P.M.B 005, KM 26 Абуджа-Кеффи
E-mail: beida.onivehu@binghamuni.edu.ng
ORCID ID: https://orcid.org/0000-0002-6089-5059
Google Scholar ID: https://scholar.google.com/citations?user=fxTBqlMAAAAJ

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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 22 сентября 2023 г.
Дата одобрения после рецензирования – 21 октября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:342.727:004.5
EDN: https://elibrary.ru/gbfhor
DOI: https://doi.org/10.21202/jdtl.2024.20

Social and Legal Risks of Sharenting when Forming a Child's Digital Identity in Social Networks

Francisco José Aranda Serna
Catholic University of Murcia, Murcia, Spain

Keywords

children's rights,
digital identity,
digital privacy,
digital technologies,
law,
personal data,
privacy,
sharenting,
social networks,
web platforms

Abstract

Objective: to determine the legal consequences of sharenting as an activity that threatens the fundamental rights of minors, putting their privacy at risk.

Methods: the study is based primarily on the analysis of European and American experience of legislative regulation, which is presented in a comparative-legal aspect, using doctrinal approaches and concepts reflected in scientific publications on the topic. This contributed, among other things, to the critical understanding of the identified risks and helped to describe the existing legal approaches and formulate proposals aimed at protecting the minors' privacy in social networks.

Results: the impact of social networks on the rights of minors was studied, in terms of their negative influence, possible risks and the spread of social conflicts. The main provisions of the legislation of Spain, France and the USA were analyzed in order to identify the key points regarding the activities of minors in social networks and the Internet, the need for them to express their consent to the publication of personal information. The most common conflicts caused by sharenting were described, as well as possible flexible legislative solutions to disputes concerning family relations and social networking activities. Suggestions were formulated for resolving conflict situations and digital identity issues arising in abusive sharenting.

Scientific novelty: the study summarizes various scientific opinions and legal approaches to sharenting as a new phenomenon, which is rapidly developing due to the wide popularity of social networks and Internet activity of children and their parents, generating socio-legal conflicts.

Practical significance: the research shows that minors are particularly vulnerable in the information and telecommunication environment. In many cases, excessive disclosure of their personal data occurs not only because of their own actions, but also because of the actions of their family members, usually parents. A comparative legal study of the adopted legislative measures and their interpretations in the legal doctrine allows characterizing the current legal situation with regard to minors in the digital space as fragmentary and proposing legislative approaches and solutions to avoid or minimize possible conflict situations and risks, such as digital harassment or privacy violation, which may arise in the process of further technological development and the spread of sharenting.

For citation

Aranda Serna, F. J. (2024). Social and Legal Risks of Sharenting when Forming a Child's Digital Identity in Social Networks. *Journal of Digital Technologies and Law, 2*(2), 394–407. https://doi.org/10.21202/jdtl.2024.20

Contents

Introduction

Minors participate in social networks because they see them as potential tools to fulfill a series of interests, whether personal or social. Unlike adults, social networks have a vital consideration in that they are a confirmation of one's own existence; non-participation in this virtual space means marginalization in social relations. However, the Internet is a relatively hostile environment, and although it is also a space for building and consolidating social relationships, it is a place where many socio-legal conflicts arise, such as digital harassment or the violation of the right to privacy (Marcelino Mercedes, 2015; Memedovich et al., 2024; Ahmed et al., 2023; Mola et al., 2023).

One of the keys to these conflicts is that when an Internet user makes his or her image or any relevant personal data public, he or she automatically loses control over it, since it enables other users to access this information, download it later and share it. In many cases, parents themselves ignore the risks of inappropriate use by their children, as all the content that is posted on the network can be turned against them (Durán Alonso, 2022).

To this complexity is added the growing phenomenon of minor «influencers», those who, in addition to uploading content on social networks, receive financial compensation for doing so. This figure has undergone a professionalization in recent years and considers social networks as commercial and advertising platforms, so the content generated is predisposed to attract followers and also commercial brands (Jiménez-Iglesias et al., 2022).

Special attention deserves the issue of «sharenting», this booming phenomenon refers to the exposure on social networks of all kinds of information (especially images and videos) of a minor, but by their parents, who act as digital managers of the former (Ferrara et al., 2023; Kopecky et al., 2020). As in the case of «influencers», by sharing content about their children, the parents receive a financial compensation (García García, 2021).

1. Notion of sharenting and its causes

Sharenting is the activity of disseminating images, videos and comments on social networks that include every day or intimate moments in the lives of underage children by their parents or other close relatives. This phenomenon is linked to the expansion of social networks and, although it apparently offers many benefits to parents such as obtaining validation (through comments or a «like»), this can be a potential danger by transmitting information constantly and excessively, information that should remain in the sphere of privacy (Ordoñez Pineda & Calva Jiménez, 2020; Aydogdu et al., 2023).

The reasons why a parent shows all this content on the network can be very different: Sometimes the goal is simply to make an album of photos and videos to share with family contacts; Given the nature of social networks, one of the motives may be to give a good image as parents or to generate collaborative synergies with other families; In other cases, the objective is economic, since in exchange for the dissemination of content, parents receive monetary or in-kind compensation (in the form of sponsorships, gifts, etc.) (Azurmendi et al., 2021).

This last reason is the one that most concerns the law, since «sharenting», from a psychological point of view, behaves as a digital representation of the concerns and frustrated successes of parents through their children. This behavior is even more pronounced when the content is monetized, because in this case the image of the children is transposed with the professional development of the parents, and even more so when these activities are the only economic source of the family (Ranzini et al., 2020).

Parents on behalf of the family and as co-responsible for the digital identity of their children have the duty to protect these rights, therefore the motivation is quite relevant, firstly, because it will involve a dissemination in a different medium. Thus, it is not the same the dissemination of photographs in a family WhatsApp group than in a digital platform such as Instagram* or YouTube**. It is also not the same that the information is

published in private mode, allowing access to a restricted group (the family) than in public mode, allowing indiscriminate access (Montoro López, 2022).

The dissemination of videos and photos can have serious negative consequences on a child's personal development (Yiseul Choi & Lewallen, 2017).

2. Social networks as a cause of sharenting

Social networks are the most important technological phenomenon of the last twenty years. However, the concept of social networking is not as modern as you might think, although it is true that today it refers to web platforms where users connect with each other, in other times this concept simply referred to communities that were connected in some way, for example, through friendship, work or other values (Oliva Marañón, 2012; Yang et al., 2022; Verswijvel, et al., 2019).

Among all the social networks that exist, a simple classification can be made in terms of their objectives:

– Social networks of a personal nature, such as Facebook*** and Twitter****.

– Professional social networks, such as LinkedIn*****.

– Thematic social networks, such as YouTube and Instagram*.

A priori, one could point to the former as the main networks that have a greater «family» presence and act as a way of propagating «sharenting», however, this classification, although simple in its premise, is complicated because the boundaries in terms of objectives between one social network and another are very blurred.

Thus, YouTube** is a platform that collects channels according to a series of themes (cinema, photography, etc.), but it can also collect «family» channels that include videos of minors in their daily lives, some of which may even be monetized.

The impact that YouTube** has among minors is very high, so many brands and advertising agencies are interested in channels that have a minor in front of the channel. This is for several reasons, one of them because family channels and with minors generate greater confidence in their products, which in turn causes users who are minors tend to consume them if they are displayed on these channels (Durán Alonso 2022).

The same is true for Instagram*, an application that emerged in 2010 with the sole purpose of sharing professional photographs, however, in 2018 it is consolidating as a social network to use because of its features (stories, «hashtags», better circulation of content). It is currently ranked in active profiles above other social networks, especially among young people (Bard Wigdor & Magallanes Udovicih, 2021).

These social networks cannot be viewed as watertight compartments; content is often multi-platform, and it is much more common for users to use two or more social networks at the same time than for them to limit themselves to a single social network. In this area, minors are the most vulnerable group and establishing a balance between technology and privacy is the great challenge that exists.

3. The legal approaches and measures to protect minors in social networks

The protection of fundamental rights is more pronounced in the case of minors, the general rule being that for there to be an intrusion on the right to honor, privacy or self-image there must be validly given consent.

However in Spain, in the case of minors, since they have a limited capacity to act, the Organic Law 1/1996 on the Legal Protection of Minors establishes that this capacity is interpreted restrictively and always in the best interest of the minor. It also differentiates the criterion of sufficient maturity (established at fourteen years of age), by which, if obtained, the minor could exercise his/her rights by him/herself (Durán Alonso, 2022).

The problem lies in the fact that there is no uniform regime in the case of minors, the Organic Law on Data Protection follows a chronological criterion regarding the processing of data, while the Civil Code gives more importance to contractual consent. For example, in the case of minors of sufficient maturity, consent must be given by the minors themselves; however, as we shall see, most cases of «sharenting» take place at a very early age (Toral Lara, 2020).

However, some legal currents understand that regardless of whether or not minors have sufficient maturity, parents, when exercising parental authority, must always protect the personality assets of the minor. The Public Prosecutor's Office may act ex officio if it is considered that their privacy has been exposed and their rights have been violated (De Lama Aymá, 2006).

The United States was the pioneer in the protection of children under thirteen years of age with the 1998 Children's Online Privacy Protection Act (COPPA Act), which established methods for digital platforms to ensure the consent of minors. Thus, with the COPPA Act, the YouTube platform already classifies and identifies content that is directed at minors, and therefore does not collect personal data directed at this audience either. (Durán Alonso, 2022).

The case of France is also a good example aimed at establishing protective laws, in 2020 with Law 2020/1266, on the commercial exploitation of the image of minors under sixteen years of age, establishing limitations in terms of schedules, compatibility with school hours and recording time, and also the regulation of the right to be forgotten, including measures regulating the right to be forgotten of minors, whereby social networks could remove the content of the minor if requested by the latter even against the authorization of their parents (Cremades García, 2021)

In the case of Spain, the publication of images must be consented to by the minor if he/she is over fourteen years of age; if he/she is under fourteen years of age, the consent of both parents must be required. In the case of opening an account in a social network, it will always be a requirement that the minor is over 14 years old, since creating an account implies the formalization of a contract and authorize the processing of data that may interfere with the honor, privacy and self-image (Santos Morón, 2011).

Consent must always be specific and informed, the purpose sought and the actual use of the data must also be assessed. Parents may not interfere with their children's social networks, except in the case of legitimate interference to protect the best interests of the child. In this regard, consent must be obtained, and judicial authorization will only be necessary if it is a serious interference with their fundamental rights (Toral Lara, 2020).

4. The problem of digital identity transposition: abusive sharenting

More and more parents are «sharenting» with a purpose that goes beyond sharing information with a family or friendship circle. The large virtual platforms have made it easier for them to exist and to do business with family-type content, partly because they are more suitable and convenient for advertising sponsors, and also because they allow those who generate such content to make economic profit (García García, 2023).

This form of «sharenting», which is defined by some researchers as «abusive sharenting», involves minors participating as protagonists or co-protagonists with their parents in videos of varying content. Consent in this case is not in doubt in principle, since the vast majority appear under the direction of one of the parents (Azurmendi et al., 2021).

Obtaining business in this modality has a series of objectives that can be varied:

– The monetization of a blog, account on a social network or family YouTube channel.

– The payment for the inclusion of advertising, obtaining sponsorship or sending gifts from advertisers.

– Also, the professional dedication to the only Internet activity (such as a YouTube channel) (Azurmendi et al., 2021).

Unlike other virtual activities in which only adults are involved, a parent's digital identity has an implicit meaning of inescapable connection with that of their children. Therefore, through these activities some parents seek to individualize and transpose their own digital identity through their children, while others adopt the notion of a kind of relational identity in which the parent's and the child's identities converge (Holiday et al., 2020).

When a user participates actively and constantly in social networks, one of the objectives is the search for personal significance and validation by other users, this is no different in the case of parents, however, the problem when using children is that this digital identity is altered. In fact, several examples can be verified in which the personal brand of the parents is imprinted, whether the motivation is economic or not. This happens because even unconsciously parents self-represent themselves through their children on social networks.

This type of activity is detrimental to the children, as it shapes them as if they were an object to obtain validation or simply an extension of the «digital self» of the parents. This self-representation, moreover, does not end with social networks and the digital world, but continues outside the digital world (Blum-Ross & Livingstone, 2017).

In these cases, the children would act as a simple means to achieve the parents' aspirations, recognition and quest for success. This type of harmful behavior can be identified when parents provide information related to children's health, or other personal data such as location, intimate information, or directly acts of promotion and advertising that can be directly qualified as exploitation. (Moser et al., 2017).

Some authors have shown that in cases of overexposure of minors a number of factors come into play that increase or decrease sharenting itself:

– First- and second-degree family unit members, who may act as critical voices to the parents themselves for the commodification of minors, or increase sharenting beyond the parents' involvement, as is the case with other close family members (Jiménez-Iglesias et al., 2022).

– The comments of consumers of this type of content, who are often critical of the commercialization of minors.

The extension over time of «abusive sharenting» suggests that it will have an important influence on the formation of the digital identity of minors, especially when they are protagonists of these family platforms from a very early age.

Currently, even when a minor consents to participate in these videos and is satisfied with the realization of these videos, he/she has no real ability to discern what the long-term consequences are. In fact, the modality of «monetized sharenting» is precisely the one that is generating the most judicial conflicts (Azurmendi et al., 2021).

Even isolated conflicts have value in illustrating the extent to which «abusive sharenting» can be harmful, the current reality is that many parents are in the habit of sharing all kinds of photos and videos almost compulsively, which can negatively affect the parent-child relationship and also the formation of the child's digital identity. In cases where there is monetization for this content, the feeling that is transmitted is an absolute lack of respect for the rights of the child (Azurmendi et al., 2021).

Conclusions

Internet and social networks have been one of the great advances in the development of modern society, however, they also pose one of the greatest dangers with respect to the protection of personal data and some fundamental rights such as privacy. This danger is even more extreme with respect to data protection and digital privacy in the case of minors, as to manage in the digital environment requires a certain maturity and knowledge to treat privacy correctly.

This study has shown that minors are vulnerable to the social networks available to them, and that in many cases the overexposure of their personal data comes not only from their own actions, but also due to the actions of members of their own family, usually their parents.

The current legal situation is somewhat scattered regarding the treatment of minors on the Internet, there are some specific issues that can be deduced from the study of the legal framework. For example, there are two categories: a minor with sufficient maturity and a minor without sufficient maturity. A sufficiently mature minor can manage

his or her own social network and generally has more mechanisms to be heard in a case of abusive sharenting.

The key to solving these conflicts is the need to provide adequate training not only to minors, but also to their parents and guardians, and even to their educators, because in many cases their actions are based on a lack of knowledge of the possible consequences of the indiscriminate uploading of content to the Internet. It is important that both minors and adults are adequately trained and aware of the risks involved in order to be able to use the Internet responsibly and safely.

It is necessary that the legal framework indicates the way forward, first of all in an international manner, which also limits the activities that are considered dangerous and that exceed social uses, especially in cases in which an economic consideration is received and the minor can be instrumentalized.

The laws must incorporate all the protective measures that social agents are advising, and also some that are already present in other legal systems such as the United States, thus establishing a legal regime that provides suitable and sufficient protection for such a vulnerable group as minors.

---

* The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.
** The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.
*** The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.
**** The social network blocked in the territory of the Russian Federation for disseminating unlawful information.
***** The social network blocked in the territory of the Russian Federation.

References

Ahmed, H., Ekman, L., & Lind, N. (2023). Planned Behavior, Social Networks, and Perceived Risks: Understanding Farmers' Behavior toward Precision Dairy Technologies. *Journal of Dairy Science*. https://doi.org/10.3168/jds.2023-23861

Memedovich, A., Orr, T., Hollis, A., Salmon, C., Hu, J., Zinszer, K., Williamson, T., & Beall, R. F. (2024). Social network risk factors and COVID-19 vaccination: A cross-sectional survey study. *Vaccine*, *42*(4), 891–911. https://doi.org/10.1016/j.vaccine.2024.01.012

Aydoğdu, F., Güngör, B. Ş., & Öz, T. A. (2023). Does sharing bring happiness? Understanding the sharenting phenomenon. *Children and Youth Services Review*, *154*, 107122. https://doi.org/10.1016/j.childyouth.2023.107122

Azurmendi, A., Etayo, C. & Torrell, A. (2021). Sharenting y derechos digitales de los niños y adolescentes. *Elprofesional de la información*, *30*(4), 1–10. (In Spanish). https://doi.org/10.3145/epi.2021.jul.07

Bard Widgor, G. & Magallanes Udovicich, M. L. (2021). Instagram*: La búsqueda de la felicidad desde la autopromoción de la imagen. *Culturales*, *9*, 1–29. (In Spanish). https://doi.org/10.22234/recu.20210901.e519

Blum-Ross, A. & Livingstone, S. (2017). "Sharenting", parent blogging, and the boundaries of the digital self. *Popular Communication*, *15*(2), 110–125. https://doi.org/10.1080/15405702.2016.1223300

Cremades García, P. (2021). Futuro profesional de los menores y ejercicio de la patria potestad. *Revista Boliviana de Derecho*, *32*, 252–277. (In Spanish).

De Lama Aymá, A. (2006). *La protección de los derechos de la personalidad del menor de edad*. Valencia: Tirant lo Blanch. (In Spanish)

Durán Alonso, S. (2022). "Mom, I Want to Be a Youtuber": an Unregulated Reality. VISUAL REVIEW. *International Visual Culture Review Revista Internacional De Cultura Visual*, *10*(3), 1–14. (In Spanish). https://doi.org/10.37467/revvisual.v9.3601

Ferrara, P., Cammisa, L., Corsello, G., Giardino, I., Vural, M., Pop, T. L., Pettoello-Mantovani, C., Indrio, F., & Pettoello-Mantovani, M. (2023). Online "Sharenting": The Dangers of Posting Sensitive Information About Children on Social Media. *The Journal of Pediatrics*, *257*. https://doi.org/10.1016/j.jpeds.2023.01.002

García García, A. (2021). La protección digital del menor: el fenómeno del sharenting a examen. *Revista de derecho UNED*, *27*, 455–492. (In Spanish). https://doi.org/10.5944/rduned.27.2021.31094

García García, R. (2023). La responsabilidad social corporativa como herramienta para la consecución de la igualdad de género en cadenas globales de valor. *Temas Laborales: Revista andaluza de trabajo y bienestar social*, *167*, 209–246. (In Spanish).

Holiday, S., Norman, M. S., & Densley, R. L. (2022). Sharenting and the extended self: Self-representation in parents' Instagram* presentations of their children. *Popular Communication*, *20*(1), 1–15. https://doi.org/10.1080/15405702.2020.1744610

Jiménez Iglesias, E., Elorriaga Illera, A., Monge Benito, S. & Olabarri Fernández, E. (2022). Exposición de menores en Instagram*: instamadres, presencia de marcas y vacío legal. *Revista Mediterránea de Comunicación*, *13*(1), 51–63. (In Spanish). https://doi.org/10.14198/medcom.20767

Kopecky, K., Szotkowski, R., Aznar-Díaz, I., & Romero-Rodríguez, J.-M. (2020). The phenomenon of sharenting and its risks in the online environment. Experiences from Czech Republic and Spain. *Children and Youth Services Review*, *110*, 104812. https://doi.org/10.1016/j.childyouth.2020.104812

Marcelino Mercedes, G. V. (2015). Migración de los jóvenes españoles en redes sociales, de Tuenti a Facebook** y de Facebook** a Instagram*. La segunda migración. *Revista de Comunicación y Tecnologías Emergentes*, *13*(2), 48–78. (In Spanish). https://doi.org/10.7195/ri14.v13i2.821

Mola, L., Kaminska, R., Richebé, N., & Carugati, A. (2023). Social strategies for information technology adoption: Social regulation process of mandated enterprise social network systems. *Technological Forecasting and Social Change*, *192*, 122570. (In Spanish). https://doi.org/10.1016/j.techfore.2023.122570

Montoro López, A. (2022). Alcance de la fiscalidad como herramienta de la Política Ambiental de la Unión Europea: Los impuestos ambientales y su eficacia como instrumento de protección ambiental. Human Review. *International Humanities Review*, *2*(14), 1–15. (In Spanish). https://doi.org/10.37467/revhuman.v11.4105

Moser, C., Chen, T., & Schoenebeck, S. Y. (2017). Parents' and children's preferences about parents sharing about children on social media. *Proceedings of the 2017 CHI Conference on Human Factos in Computing Systems*, 5221–5225. https://doi.org/10.1145/3025453.3025587

Oliva Marañon, C. (2012). Redes sociales y jóvenes: una intimidad cuestionada en Internet. *Aposta: Revista de ciencias sociales*, *54*, 1–16. (In Spanish).

Ordoñez Pineda, L. & Calva Jimenez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. *Revista Chilena de Derecho y Tecnología*, *9*(2), 105–130. (In Spanish). https://doi.org/10.5354/0719-2584.2020.55333

Ranzini, G., Newlands, G. & Lutz, C. (2020). Sharenting, Peer Influence, and Privacy Concerns, A Study of Instagram-Sharing Behaviors of Parents in the United Kingdom. *Social Media + Society*, *6*(4), 1–13. https://doi.org/10.1177/2056305120978376

Santos Morón, M. (2011). Menores y derechos de la personalidad. La autonomía del menor. *AFDUAM: Anuario de La Facultad de Derecho de la Universidad Autónoma de Madrid*, *15*, 63–93. (In Spanish). http://hdl.handle.net/10486/662984

Toral Lara, E. (2020). Menores y redes sociales: consentimiento protección y autonomía. *Derecho Privado y Constitución*, *36*, 179–218. (In Spanish). https://doi.org/10.18042/cepc/dpc.36.05

Verswijvel, K., Walrave, M., Hardies, K., & Heirman, W. (2019). Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review*, *104*, 104401. https://doi.org/10.1016/j.childyouth.2019.104401

Yang, M., Chen, H., Long, R., & Yang, J. (2022). The impact of different regulation policies on promoting green consumption behavior based on social network modeling. *Sustainable Production and Consumption*, *32*, 468–478. https://doi.org/10.1016/j.spc.2022.05.007

Yiseul Choi, G. & Lewallen, J. (2017). Say Instagram*, Kids!: examining Sharenting and Children Digital Representations on Instagram. *Howard Journal of Communications*, *29*(2), 144–164. https://doi.org/10.1080/10646175.2017.1327380

---

* The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

** The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

Author information

Francisco José Aranda Serna – PhD (Law), Associate Professor, Department of Law, Catholic University of Murcia
Address: Av. de los Jerónimos, 135, 30107 Guadalupe de Maciascoque, Murcia, Spain
E-mail: fjaranda@ucam.edu
ORCID ID: https://orcid.org/0000-0002-5768-2773
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=58097085200
Google Scholar ID: https://scholar.google.com/citations?user=zrndQAwAAAAJ

Conflict of interest

The author 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 29, 2023
Date of approval – November 25, 2023
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:342.727:004.5
EDN: https://elibrary.ru/gbfhor
DOI: https://doi.org/10.21202/jdtl.2024.20

Социально-правовые риски шерентинга в процессе формирования цифровой идентичности ребенка в социальных сетях

Франциско Хосэ Аранда Серна

Католический университет Мурсии, Мурсия, Испания

Ключевые слова

веб-платформы,
неприкосновенность частной жизни,
персональные данные,
права ребенка,
право,
социальные сети,
цифровая идентичность,
цифровая конфиденциальность,
цифровые технологии,
шерентинг

Аннотация

Цель: определить правовые последствия шерентинга как деятельности, которая ставит под угрозу основные права несовершеннолетних, подвергая риску их частную жизнь.

Методы: проведенное исследование строится прежде всего на анализе европейского и американского опыта законодательного регулирования, который излагается в сравнительно-правовом аспекте с применением доктринальных подходов и концепций, получивших отражение в научных публикациях по данной теме. Это способствовало в том числе критическому осмыслению выявленных рисков, а также представлению существующих правовых подходов и формулированию предложений, направленных на защиту неприкосновенности частной жизни несовершеннолетних в социальных сетях.

Результаты: изучено влияние социальных сетей на права несовершеннолетних в части негативного их воздействия, возможных рисков и распространения социальных конфликтов. Осуществлен анализ основных положений законодательства Испании, Франции и США с целью выявления ключевых моментов относительно деятельности несовершеннолетних в социальных сетях и сети Интернет, необходимости выражения ими согласия на опубликование личной информации. Описаны наиболее распространенные конфликты, обусловленные шерентингом, и возможные гибкие законодательные решения споров, касающихся семейных отношений и связанных с деятельностью в социальных сетях. Сформулированы предложения по разрешению конфликтных ситуаций и проблемы цифровой идентичности, возникающих в процессе шерентинга в случае злоупотребления.

Научная новизна: представленное исследование обобщает различные научные точки зрения и правовые подходы к шерентингу как новому феномену, который быстро развивается в связи с широкой популярностью социальных сетей и интернет-активностью детей и их родителей, порождая социально-правовые конфликты.

Практическая значимость: представленное исследование показывает, что несовершеннолетние особенно уязвимы в информационно-телекоммуникационном пространстве. Во многих случаях чрезмерное раскрытие их личных данных происходит не только из-за их собственных действий, но и из-за действий членов их семей, как правило, родителей. Сравнительно-правовое исследование принятых законодательных мер и их интерпретаций в правовой доктрине позволяет охарактеризовать современную правовую ситуацию в отношении несовершеннолетних в цифровом пространстве как фрагментарную и предложить законодательные подходы и решения, позволяющие избежать или минимизировать возможные конфликтные ситуации и риски, такие как цифровое преследование или нарушение права на неприкосновенность частной жизни, которые могут возникать в процессе дальнейшего развития технологий и распространения шерентинга.

Для цитирования

Аранда Серна, Ф. Х. (2024). Социально-правовые риски шерентинга в процессе формирования цифровой идентичности ребенка в социальных сетях. *Journal of Digital Technologies and Law*, *2*(2), 394–407. https://doi.org/10.21202/jdtl.2024.20

Список литературы

Ahmed, H., Ekman, L., & Lind, N. (2023). Planned Behavior, Social Networks, and Perceived Risks: Understanding Farmers' Behavior toward Precision Dairy Technologies. *Journal of Dairy Science*. https://doi.org/10.3168/jds.2023-23861

Memedovich, A., Orr, T., Hollis, A., Salmon, C., Hu, J., Zinszer, K., Williamson, T., & Beall, R. F. (2024). Social network risk factors and COVID-19 vaccination: A cross-sectional survey study. *Vaccine*, *42*(4), 891–911. https://doi.org/10.1016/j.vaccine.2024.01.012

Aydoğdu, F., Güngör, B. Ş., & Öz, T. A. (2023). Does sharing bring happiness? Understanding the sharenting phenomenon. *Children and Youth Services Review*, *154*, 107122. https://doi.org/10.1016/j.childyouth.2023.107122

Azurmendi, A., Etayo, C. & Torrell, A. (2021). Sharenting y derechos digitales de los niños y adolescentes. *Elprofesional de la información*, *30*(4), 1–10. https://doi.org/10.3145/epi.2021.jul.07

Bard Widgor, G. & Magallanes Udovicich, M. L. (2021). Instagram*: La búsqueda de la felicidad desde la autopromoción de la imagen. *Culturales*, *9*, 1–29. https://doi.org/10.22234/recu.20210901.e519

Blum-Ross, A. & Livingstone, S. (2017). "Sharenting", parent blogging, and the boundaries of the digital self. *Popular Communication*, *15*(2), 110–125. https://doi.org/10.1080/15405702.2016.1223300

Cremades García, P. (2021). Futuro profesional de los menores y ejercicio de la patria potestad. R*evista Boliviana de Derecho*, *32*, 252–277.

De Lama Aymá, A. (2006). *La protección de los derechos de la personalidad del menor de edad*. Valencia: Tirant lo Blanch.

Durán Alonso, S. (2022). "Mom, I Want to Be a Youtuber": an Unregulated Reality. VISUAL REVIEW. *International Visual Culture Review Revista Internacional De Cultura Visual*, *10*(3), 1–14. https://doi.org/10.37467/revvisual.v9.3601

Ferrara, P., Cammisa, L., Corsello, G., Giardino, I., Vural, M., Pop, T. L., Pettoello-Mantovani, C., Indrio, F., & Pettoello-Mantovani, M. (2023). Online "Sharenting": The Dangers of Posting Sensitive Information About Children on Social Media. *The Journal of Pediatrics*, *257*. https://doi.org/10.1016/j.jpeds.2023.01.002

García García, A. (2021). La protección digital del menor: el fenómeno del sharenting a examen. *Revista de derecho UNED*, *27*, 455–492. https://doi.org/10.5944/rduned.27.2021.31094

García García, R. (2023). La responsabilidad social corporativa como herramienta para la consecución de la igualdad de género en cadenas globales de valor. *Temas Laborales: Revista andaluza de trabajo y bienestar social*, *167*, 209–246.

Holiday, S., Norman, M. S., & Densley, R. L. (2022). Sharenting and the extended self: Self-representation in parents' Instagram* presentations of their children. *Popular Communication*, *20*(1), 1–15. https://doi.org/10.1080/15405702.2020.1744610

Jiménez Iglesias, E., Elorriaga Illera, A., Monge Benito, S. & Olabarri Fernández, E. (2022). Exposición de menores en Instagram*: instamadres, presencia de marcas y vacío legal. *Revista Mediterránea de Comunicación*, *13*(1), 51–63. https://doi.org/10.14198/medcom.20767

Kopecky, K., Szotkowski, R., Aznar-Díaz, I., & Romero-Rodríguez, J.-M. (2020). The phenomenon of sharenting and its risks in the online environment. Experiences from Czech Republic and Spain. *Children and Youth Services Review*, *110*, 104812. https://doi.org/10.1016/j.childyouth.2020.104812

Marcelino Mercedes, G. V. (2015). Migración de los jóvenes españoles en redes sociales, de Tuenti a Facebook** y de Facebook** a Instagram*. La segunda migración. *Revista de Comunicación y Tecnologías Emergentes*, *13*(2), 48–78. https://doi.org/10.7195/ri14.v13i2.821

Mola, L., Kaminska, R., Richebé, N., & Carugati, A. (2023). Social strategies for information technology adoption: Social regulation process of mandated enterprise social network systems. *Technological Forecasting and Social Change*, *192*, 122570. https://doi.org/10.1016/j.techfore.2023.122570

Montoro López, A. (2022). Alcance de la fiscalidad como herramienta de la Política Ambiental de la Unión Europea: Los impuestos ambientales y su eficacia como instrumento de protección ambiental. Human Review. *International Humanities Review*, *2*(14), 1–15. https://doi.org/10.37467/revhuman.v11.4105

Moser, C., Chen, T., & Schoenebeck, S. Y. (2017). Parents' and children's preferences about parents sharing about children on social media. *Proceedings of the 2017 CHI Conference on Human Factos in Computing Systems*, 5221–5225. https://doi.org/10.1145/3025453.3025587

Oliva Marañon, C. (2012). Redes sociales y jóvenes: una intimidad cuestionada en Internet. *Aposta: Revista de ciencias sociales*, *54*, 1–16.

Ordoñez Pineda, L. & Calva Jimenez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. *Revista Chilena de Derecho y Tecnología*, *9*(2), 105–130. https://doi.org/10.5354/0719-2584.2020.55333

Ranzini, G., Newlands, G. & Lutz, C. (2020). Sharenting, Peer Influence, and Privacy Concerns, A Study of Instagram-Sharing Behaviors of Parents in the United Kingdom. *Social Media + Society*, *6*(4), 1–13. https://doi.org/10.1177/2056305120978376

Santos Morón, M. (2011). Menores y derechos de la personalidad. La autonomía del menor. *AFDUAM: Anuario de La Facultad de Derecho de la Universidad Autónoma de Madrid*, *15*, 63–93. http://hdl.handle.net/10486/662984

Toral Lara, E. (2020). Menores y redes sociales: consentimiento protección y autonomía. *Derecho Privado y Constitución*, *36*, 179–218. https://doi.org/10.18042/cepc/dpc.36.05

Verswijvel, K., Walrave, M., Hardies, K., & Heirman, W. (2019). Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review*, *104*, 104401. https://doi.org/10.1016/j.childyouth.2019.104401

Yang, M., Chen, H., Long, R., & Yang, J. (2022). The impact of different regulation policies on promoting green consumption behavior based on social network modeling. *Sustainable Production and Consumption*, *32*, 468–478. https://doi.org/10.1016/j.spc.2022.05.007

Yiseul Choi, G. & Lewallen, J. (2017). Say Instagram*, Kids!: examining Sharenting and Children Digital Representations on Instagram. *Howard Journal of Communications*, *29*(2), 144–164. https://doi.org/10.1080/10646175.2017.1327380

---

* Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

** Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Сведения об авторе

Аранда Серна Франциско Хосэ – PhD в области юриспруденции, доцент, факультет права, Католический университет Мурсии
Адрес: 30107, Испания, Мурсия, Гваделупа-де-Макиаскок, авеню де лос Херонимос, 135
E-mail: fjaranda@ucam.edu
ORCID ID: https://orcid.org/0000-0002-5768-2773
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=58097085200
Google Scholar ID: https://scholar.google.com/citations?user=zrndQAwAAAAJ

Конфликт интересов

Автор сообщает 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: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 29 октября 2023 г.
Дата одобрения после рецензирования – 25 ноября 2023 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:34.096:347.211
EDN: https://elibrary.ru/hiqzuj
DOI: https://doi.org/10.21202/jdtl.2024.21

Measures to Prevent the Violation of the Rights of Content Creators in Digital Environment: Case Study of Nigeria

Adetutu Deborah Aina-Pelemo ✉
Redeemer's University, Ede, Nigeria

Ithamar Bassey
Redeemer's University, Ede, Nigeria

Glorious Okeoghene Akpojaro
Redeemer's University, Ede, Nigeria

Keywords

copyright,
Internet,
online content,
intellectual property rights,
legal protection,
prevention of copyright violation,
social network,
digital platform,
digital marketing,
digital technologies

Abstract

Objective: to determine the level of protection of the rights of content creators in social media and to develop measures to prevent offenses in this area.

Methods: to achieve the objective, the sociological and legal cognitive tools were used, including the doctrinal method of researching the subject area, obtaining "first-hand" data and taking into account the factors and circumstances of influence. The main results were obtained through the sociological method used to collect data based on a specially developed questionnaire with four research questions: (1) what are the perceptions and opinions of third parties or users regarding the role of a content creator? (2) are the rights of content creators regarding their works violated? (3) what are the ways to protect the created content from infringement by platforms? and (4) how can the rights of content creators be protected? The empirical findings and generalizations were based on a combination of analyses, including content analysis of primary and secondary legal sources.

Results: In recent years, the content generation in social media has evolved into a complex industry that is transforming both the traditional

✉ Corresponding author

understanding of creative expression and the implementation of intellectual property rights. Using the Nigerian experience as a case study, the authors examine the rights and protection measures provided to digital content creators under intellectual property law. The study shows that there is currently not enough scholarly work in this area or developed legislation to protect the social media content. It is concluded that there is a need for improved legislation on the protection of rights in the sphere of social media content. In the absence of such legislation, creators of online works should resort to more radical methods in enforcing their rights in order to reduce intellectual property misappropriation. Creators of such works are suggested to ensure the protection of their rights based on the fair use doctrine principles.

Scientific novelty: the study is structured around research questions concerning infringements and remedies for content creators. The questions were addressed to respondents from different countries, a large proportion of whom specialize mainly in content creation in various social spheres through several media platforms and social networks.

Practical significance: the article conclusions and recommendations may minimize the risks of infringement of intellectual property rights of content creators, which may arise with the widespread use of social networks, as well as increase the level of protection of rights to works created in the form of online content.

For citation

Aina-Pelemo, A. D., Bassey, I., & Akpojaro, G. O. (2024). Measures to Prevent the Violation of the Rights of Content Creators in Digital Environment: Case Study of Nigeria. *Journal of Digital Technologies and Law*, *2*(2), 408–429. https://doi.org/10.21202/jdtl.2024.21

Contents

Introduction

Intellectual Property is expanding so fast in today's unique and dynamic world. Intellectual property has developed so much in the legal field that conventions have been created around it (Zhang & Xu, 2023). In the same vein, international organizations such as the World Intellectual Property Organization (WIPO) and many others have also contributed to the advancement of intellectual property law by deepening the understanding of people. Artistic works, literary works, performance and broadcasting are also gaining substantial value in the labour market, as such, it will be highly unreasonable to ignore the socio-legal issues that emanates from them.

Over the last couple of years following the COVID-19 pandemic, a lot of people were forced to work remotely because of the lockdown situation, and individual businesses and largely established companies were affected by this shift in the norm (Liu & Zhang, 2024; Aina-Pelemo et al., 2021). Hence, a largely significant increase occurred in the utilization of social media marketing to reach the target audiences. This brought light to a part of intellectual property known as 'content creation' to the public. Although content creation has been in place for as long as intellectual property has been, the new format it has taken via social media platforms is what took the world by surprise. Nowadays, people extend their creative ideas and processes on platforms that are used every day and are primarily audio visual. Since then, the reputation of online content producers and marketers has improved tremendously and the global the influencer marketing sector is predicted to grow (Alvarez-Monzocillo, 2022). Presently, it represents roughly 15% of the overall worldwide advertising income.

Meanwhile, this industry is anticipated to increase by 25% annually, and by the end of 2025, it would have a total market value of more than INR 2,200 crores ($26.84). India had 400 million social media users prior to the pandemic, however this number increased significantly (18%) as a result of the outbreak (Priyanshi, 2022). This currency value will be much higher if it is in United States Dollars.

Content creators and influencers assist brands in reaching out to a wider audience. According to surveys on users of Instagram* and other well-known social media platforms, each user spends, an average, of two hours every day on these platforms (Subair et al., 2019). As a result, social media influencers have proven to be a valuable tool in the marketing sector and contribute significantly to the expansion of companies by enabling them connect with new audiences.

1. Concept of Intellectual Property and Content Creation

Intellectual property (IP) refers to the legal rights granted to individuals or entities over creations of the mind, such as inventions, literary and artistic works, symbols, names, images, and designs (Aina-Pelemo & Akpojaro, 2024; Saha & Bhattacharya, 2011). These rights are crucial for fostering innovation, creativity, and economic growth. In Nigeria, intellectual property laws play a significant role in protecting and promoting innovation and creativity (Owushi, 2020).

Intellectual property is usually regarded as intangible and can only be perceived by sight or hearing. The exclusive uses or ownerships that the creators are granted over these creative works are known as intellectual property rights, (Fatoba, 2019; Lei & Hui, 2023). Typically, the creator is granted an exclusive right to use his or her work, sell or dispose of it as they pleases or even grant usage of these rights to other persons. It is a product of the mind, and the intangible medium of such properties are one of the reasons for its uniqueness. Intellectual property begins in the mind of individuals and then, they are executed into perceivable forms. However, the formation of these ideas is the product of intellect. Every individual's intellectual capacity varies and as a result, ideas even though similar will always have a touch of uniqueness that makes it exceptional.

Content creation is no exception to the above, it is an expression of ideas formed by one's intellect and skill into audio and visual mediums[1]. The process of producing and sharing information through the media to reach a specific audience for specific purpose is known as content creation. Descriptively, content creation could also denote the process of performing research, coming up with strategic ideas, turning those ideas into high-quality collateral, and afterwards promoting those pieces to a target audience. This creation is a product of the intellect of a person known as the creator who has gone through a process of combining his or her knowledge, coupled with creativity to form valuable creations and as such, shows that content creation is a part of intellectual property (Kupers et al., 2019). It is usually aimed at marketing, advertising or information sharing.

According to Kupers et al. (2019), content creation exists mainly through audio visual mediums like videos and photographs. Humans' attention and interest are captivated by the senses of hearing and sight, and audiovisual works have the ability to gain the attention of people a lot faster than any other sensory mechanism. Hence, content creators take advantage of this.

Social media have made potent effect of audio-visual work climb to a whole new dimension. It allows people to connect with one another from all over the world in real time. It breaks the boundaries of time differences and other obstructions. In fact, creators can share their works on the internet and any social media of choice; they also have the ability to reach thousands and millions of people all at once, both in their countries or states and even across countries. Let's take an instance, where an artist has an art exhibition at a gallery and has a total attendance of one hundred (100) people. Analysing the same scenario, imagine a content creator is hired to create a video, giving insight about the art piece displayed in the exhibition and why it would be a great opportunity for artists to attend the exhibit and connect. Such video is then posted on a social media page and is targeted toward artist and art enthusiasts. No doubt, this addition to the promotion and marketing, the video content will reach thousands of people and the total attendance or audience may double or triple. Depending on the scale of the promotion, these results have proven to be remarkable.

[1] Farrington, C. A., McBride, M. R. A., Puller, J., Weiss, E., Maurer, J., Nagaoka, J., Shewfelt, S., & Wright, L. (2019). Arts Education and Social-Emotional Learning Outcomes Among K-12 Students. Developing a theory of Action. UChicago Consortium on School Research.

The rush for the content creation industry is rooted in the above explanation. Companies, organizations and all forms of corporations targeted at profit acquisition thrive on marketing. They look for the best ways to reach their target audience fast and efficiently. They can pay or hire content creators who have influence in a particular market of interest to be marketing the company's product to their vast audience that is, their target audience. Technology has paved the way for content creation to exist in such a large scale as it does. Also, the COVID-19 pandemic forced businesses and corporations to find new innovations to market their products and services and the content creation market filled that gap effortlessly[2]. Premised on these explanations, the authors can rightly say that content creation is the basis of modern digital marketing.

On a daily basis, thousands and millions of contents is shared all over the internet around the world. For a piece of content to make an impact, it needs to be of high value and quality. This indicates that the creator must take particular effort in creating and formulating the content. The intellectual property system is created to accomplish two major goals (Afolayan, 2022). The first is the defense of the rights of creators of works of intellectual property, and the second is the promotion of the interest of the public through granting access to a broad variety of works and inventions in many areas vital to societal well-being. This goal promotes financial support for creative projects that benefit society as a whole.

Copyright law in Nigeria is primarily governed by the Nigerian Copyright Act of 2022 (NCA), which repealed the former 1988 Act. The Act grants exclusive rights to copyright owners, including the rights to reproduce, distribute, perform, and display their works. Copyright protection is automatic upon creation and extends for the lifetime of the author plus 70 years after his or her death[3].

The NCA makes important modifications that will have an effect on creators and significantly enhance the exercise of their rights, particularly in a digital age. The Nigerian Copyright Commission (abbreviated NCC or «the Commission») has been given more authority to effectively administer and enforce compliance of individuals and entities with the Act's provisions (Majekolagbe, 2016). Audiovisual works are now recognized as being eligible for copyright protection. Tenure of moral rights has also been established, and photography and the arts are now subject to licenses.

The Act made it clear that prior to being duplicated, transmitted, or distributed to the public for commercial reasons through sale or other transfers of ownership, the owner of an audiovisual work must provide their approval (Nkwor, 2023). It also broadens the definition of broadcast to include distributing an audiovisual work to the general public via wired or wireless means in a way that allows for general access from a location and at a time of the general public's choosing.

---

2 Smith, K. (2022). How Covid-19 Increased Influencer Marketing. https://clck.ru/3AQeFW

3 Oloruntade, G. (2023). What Does the New Copyright Law Mean for Nigerian Content Creators? Technext. https://clck.ru/3AQeG9

Since the Act defines copy as any kind of reproduction, including a digital copy, it allows for the inclusion of digital information. This implies that owners of any sort of online content, including social media content creators and anyone who produce audio, video, and other types of productions, are protected from copyright infringements since such works cannot be utilized without the owner's or creators' permission (Jerameel, 2021).

However, the artists and influencers on these social media platforms face intellectual property rights risks as a result of the social media market's expansion and their intellectual property rights must be protected because it takes tremendous amount of time, efforts, intelligence to create the original material, and years to build authentic audiences.

In light of this, this paper seeks to examine the rights and protection provided for content creators under Intellectual Property Law with a focus on Nigeria. The study was structured into four (4) research questions and address accordingly.

2. Extent of Creators Rights Over Work Published on the Social Media Platforms

The rights of a creator over their work published on social media platforms are determined by various factors. The general rule is that once a creative work is published in a fixed format, copyright is created (Oriakhogba, 2018). First, the copyright belongs to the influencer when created, except the employer of the creator wishes to solely or partially own the created work based on agreements between the parties or conditions of employment (Garcia, 2022). Additionally, the extent of the creators' right may also be determined by the terms of a contract signed by the creator. In a situation where a content creator enters an agreement with a company, the terms of their agreement may also state the extent of usage rights granted, licensing or shared ownership.

Once a creator uploads their creative work on social media, they still retain ownership of the copyright. The platform neither claims ownership of the material nor is anybody permitted to use it without the creators' consent, but by using any social networking platform, it is considered that the person consents to the terms of service, which frequently provide the platform permission to utilize the creators' works. This does not imply that the website may utilize the creator's work for its own purposes, but it is free to evaluate, remove, or even restrict the content in order to comply with its conditions of use (Reid, 2019). These terms of service may require users to permit the use of their work in order to enhance their services, according to certain terms of service. Neither the users nor web manager, can asserts control over user-generated content or reserves the right to sell it to advertising agents. More significantly, the web manager enables other users of the site to access the work with necessary credit being given to the creators.

The copyright terms of some large social media platforms (e.g Instagram*, Twitter**, YouTube***, LinkedIn****, TikTok, Facebook*****, Snapchat, Pinterest, etc) make it clear that users still have full ownership over their content published and they rather act as

placeholders[4]. Nonetheless, the fact that a work is on public site does not indicate that it is owned by the public or in public domain. In essence, works can be violated and reliefs awarded for any violation of a person's IPRs that happens online or on social media (Fagundes & Perzanowski, 2020).

3. Data Presentation and Analysis

This section presents and analyzes the data obtained by questioning.

3.1. Research sample and methods

In order to implement the adopted comprehensive research methodology, both qualitative and quantitative approaches were used. In this regard, a questionnaire containing several research questions was used for data collection: 1. What are the perceptions and opinions of third parties or users regarding the role of a content creator? 2. Are the rights of content creators regarding their works violated? 3. What are the ways to protect the created content from infringement by platforms? 4. How can the rights of content creators be protected?

The survey was conducted electronically via Instagram* from January through March 2023. More than 50 content creators responded to the survey. The survey used a simple random sampling method to select respondents, which combines well with the use of a hybrid approach to legal research, and has the advantage of reaching the most diverse groups of respondents and is free from bias.

3.2. Data Analysis and Results

The data obtained or generated from the conducted questionnaire are presented in the tables below.

The findings on the social demographics information was presented in Table 1. The gender distributions of the respondents showed that nearly all of them were female. This was such that 94.2 % were female, while 5.8 % were males. The respondents' age distribution revealed that 17.3 % of respondents were within the age ranges of 16 and 20 years, 65.4 % within the age range of 21 and 25 years, and 15.4% aged between 26 and 30 years, while a limited percentage of the respondents (1.9 %) aged above 30 years. In respect to the nationality of the respondents, majority of the respondents (78.9%) were Nigerians, 3.8 % from Ghana and Albania, 1.9 % claimed Kenya, the Republic of Gambia, Trinidad and Brazil for nationality and 5.9 % from Britain.

In a similar trend larger percentage of the respondents (76.9 %) resides in Nigeria, 3.8 % of resides in Ghana, 1.9 % claimed they lives in either Siberia or Trinidad, while 3.8 resides in either Italy or United State of America and 7.7 % lives in the United Kingdom.

[4] Frost, N. (2023). Crediting Sources on Social Media: Why and How to Do It. https://clck.ru/3AQekF

Table 1. Frequency Distribution showing Respondents' Social Demographics

Factors	Options	Frequency	%
Gender	Male	3	5.8
	Female	49	94.2
	Total	52	100.0
Age	16-20 Years	9	17.3
	21-25 Years	34	65.4
	26-30 Years	8	15.4
	Above 30 Years	1	1.9
	Total	52	100.0
Nationality	Nigerian	41	78.9
	Ghanaian	2	3.8
	Kenyan	1	1.9
	British	3	5.9
	Trinidadian	1	1.9
	Albanian	2	3.8
	Gambian	1	1.9
	Brazilian	1	1.9
	Total	52	100.0
Country of Residence	Nigeria	40	76.9
	Ghana	2	3.8
	Russia	1	1.9
	Italy	2	3.8
	Trinidad	1	1.9
	United Kingdom	4	7.7
	USA	2	3.8
	Total	52	100.0
Creative Niche	Beauty	31	59.7
	Lifestyle	3	5.9
	Fashion and education	1	1.9
	Beauty and Food	1	1.9
	2Beauty/lifestyle	2	3.8
	Lifestyle, food	1	1.9
	Fashion and Lifestyle	2	3.8
	Beauty and Fashion	2	3.8
	Lifestyle and Beauty	1	1.9
	Beauty, Fashion & lifestyle	3	5.9
	Lifestyle, beauty and fashion	1	1.9
	Beauty, Lifestyle and Entertainment	2	3.8
	Beauty, lifestyle and Education	1	1.9
	Beauty, Fashion, Health and Lifestyle	1	1.9
	Total	52	100.0

End of Table 1

Creative Platforms	YouTube***	2	3.8
	Instagram*	12	23.1
	TikTok	3	5.9
	WhatsApp, Tiktok	1	1.9
	Instagram* & Tiktok	18	34.6
	Instagram*, Tiktok, Facebook*****	5	9.6
	YouTube***, Instagram* and TikTok	4	7.7
	YouTube***, Facebook*****, Instagram*, Tiktok	2	3.8
	Instagram*, Tiktok, Pinterest and YouTube***	3	5.9
	Instagram*, TikTok, Interest	2	3.8
	Total	52	100.0
How Important is content creation to you?	It is important to me because it takes my time and resources	27	51.9
	It is very important to me because it is my source of livelihood/income	25	48.1
	Total	52	100.0

In respect to the respondents' creative Niche, it was observed that a good number of them (59.7) majored in creating content related to Beauty, 5.9 % centralized it content creation on lifestyles, similar percentage (5.9 %) centralized its content creation on beauty, fashion and lifestyle. It was also reported that 3.8 % centralized their content creativity on beauty and life style, fashion and lifestyle, beauty and fashion, as well as beauty, lifestyle and entertainment. Meanwhile 1.9 % majored their content creation on both fashion and education; beauty and food; lifestyle and food; life style and beauty; beauty with lifestyle and entertainment; or beauty with fashion, and health with lifestyle.

On the creative platform used by the respondents, 3.8 % affirm they use the Youtube***; or both Instagram*, TikTok with Pinterest; or both YouTube***, Facebook***** and Instagram*, Tiktok together, 5.9 % use TikTok, and a similar percentage of (5.9 %) had been using both Instagram*, Tiktok, Pinterest and YouTube*** together, 23.1 % adopted only Instagram as a social media platform for content creation. A few of them (1.9 %) had been using WhatsApp and TikTok for their content creation, 34.6 % also adopted both Instagram and TikTok for their content creativity, 9.6 % adopted both Instagram*, TikTok and Facebook***** for their content creation, while 7.7 % make use of both YouTube***, Instagram and TikTok for their content creation. The last reported socio-demographic information inquired the relevance of content creation to. It indicated that 51.9 % of the respondents affirmed that content creation help use their time and resources productively, while 48.1% consented that content creation is their source of livelihood and means of income generation.

The finding on statements explains perception and attitude towards crediting the source of content creation and presented in Table 2. It revealed that 21.2 % of the respondents had at a time confronted or taken action against someone who appropriated or repurposed their work without their consent, a few (3.8 %) does not bother when anyone appropriated

or repurposed their work without their consent, meanwhile majority had not at any point in time confronted nor took any action against anyone who appropriates or repurposed their work without their consent. It was also reported that 23.1 % of the respondents were of the opinion that they are not sure if they had at any point in time appropriated the creative work of another creator without their consent or giving proper credit when they take inspiration from their work or recreate the same as theirs, however larger number of the respondents (76.9 %) posited they had never appropriated the creative work of another creator without their consent or giving proper credit when they take inspiration from their work or recreate the same as theirs.

Table 2. Frequency Distribution showing perception and attitude towards crediting the source of content ideas

Factors	Options	Frequency	%
I have confronted or taken action against someone who appropriated or repurposed my work without my consent	No	39	75.0
	I don't Care	2	3.8
	Yes	11	21.2
	Total	52	100.0
I have appropriated the creative work of another creator without their consent or giving them proper credit for when I take inspiration from their work or recreate the same	No	40	76.9
	I don't Know	12	23.1
	Yes	0	0
	Total	52	100.0
I always give credit to the original creator of any design or style etc. I take inspiration from my content	No	1	1.9
	I don't Care	12	23.1
	Yes	39	75.0
	Total	52	100.0
I understand what fair content use implies	No	14	26.9
	Yes	38	73.1
	Total	52	100.0

Higher percentage of the respondents (75 %) affirmed that they had always given credit to the original content creator where they got inspiration, 23.1 % do not care to give credit, while a few (1.9 %) does not. Lastly, it indicated that majority of the respondents (73.1 %) affirmed that they do understood what means to engage in fair content use, though 26.9 % report contrary.

The result in Table 3 shows the possibility of infringement on works of content creators. It was observed that a good number of the respondents (55.7 %) were of the believe that a content creators' work can be appropriated on social media without any form of consequences, 21.2 % of were not sure if there is any form of consequences for content appropriation on social media or not, although 23.1 % did not believe that a creators' work can be appropriated on social media without any consequences.

Lastly, it was observed that a good number of the respondents (55.8 %) does not bother whether their works had been appropriated and re-purposed without their consent in time past, however 44.2 % denied the occurrence that their work had been appropriated and re-purposed without their consent in time past.

Table 3. Frequency and percentage summary relating the possibility of infringement on works of content creators

Factors	Options	Frequency	%
Do you believe that a creator work can be appropriated on social media without any consequences	No	12	23.1
	I don't Know	11	21.2
	Yes	29	55.7
	Total	52	100.0
My work has been appropriated and re-purposed without my consent in the past	No	23	44.2
	I do not Care	29	55.8
	Yes	-	-
	Total	52	100.0

The result on the possible ways to protect content creations from media infringement was presented in Table 4. A good number of the respondents (59.6 %) believed that the use of watermarks or the attachment of any other form of personal branding on creative contents been uploaded on social media platforms is sufficient enough to protect content creative rights, however 40.4 % had a contrary impression.

Table 4. Frequency and percentage summary relating possible ways to protect content creations from Media infringement

Factors	Options	Frequency	%
Do you believe that as a creator, watermarking or attaching any form of personal branding on your creative works uploaded on social media platforms is sufficient to protect your creative rights	No	21	40.4
	Yes	31	59.6
	Total	52	100.0
It is not mandatory to register your creative works to enforce copyright as it exists once the work is published to the public in a fixed format. It is however advised that a creator should register their works. Do you believe you can realistically register each piece of your work?	No	21	40.4
	I don't Know	14	26.9
	Yes	17	32.7
	Total	52	100.0
Do you believe that "tagging the original creator" is a sufficient means to credit the creator of a work	No	13	25.0
	Yes	39	75.0
	Total	52	100.0

It was reported that 40.4 % of the respondents were aware of the need to register each piece of the content they create as they have been advised to do so. Therefore it is mandatory for them to register their creative works to enforce copyright as it exists once the work is published to the public in a fixed format. 26.9 % of the respondents were not aware of the need to and the benefit of registering their created contents, meanwhile 32.7 % felt it is not mandatory to register their created contents. Lastly, 75 % of the respondents believed that "tagging the original creator" is a sufficient means to credit the creator of a work, meanwhile 25 % report differently.

The findings on statements relating to the possible steps to protecting the right of content creators were presented in Table 5. The enquiry about the meaning of fair content use to certify the understanding of content creators about their right had shown that 42.3 % of the respondents were of the opinion that fair content use means crediting the original creator of the work, 19.2 % had explained it as using the content created by the creator for its intended purpose, and 3.8 % felt fair content means replicating the same content idea in their own content without credit, while 34.6 % explained fair content as the use of creative work or content without harming the rights of the creator.

Table 5. Frequency Distribution showing the possible steps to protecting the right of content creators

Factors	Options	Frequency	%
What does the principle of fair content use mean to you as a creator?	Crediting the original creator of the work	22	42.3
	Using the content created by the creator for the purpose it was intended for	10	19.2
	Replicating the same idea in my own content without credit	2	3.8
	Using the creative work or content without harming the rights of the creator	18	34.6
	Total	52	100.0
Are you aware of any legal ways to protect your content on social media?	No	18	34.6
	Yes	34	65.4
	Total	52	100.0
If Yes, then through what means?	Friends	1	1.9
	Media (Social media, blogs, videos, articles, etc.)	26	50.0
	Formal Education	7	13.5
	Total	34	100.0
	Note Applicable	18	-
Are you aware that it is wrong for someone to appropriate or repurpose your content without your consent?	No	4	7.7
	Yes	48	92.3
	Total	52	100.0

Reasonable number of the respondents (65.4 %) affirmed that they are aware of legal ways to protect their content on social media, although 34.6% report not to be aware of any form of legal approach to protect their content copyright. A limited percentage of the respondents (1.9 %) express their awareness of legal ways to protect their content creation through their friends as a way to protect their content copyright, and a good number (50 %) has identified the media such as a Blogs, Media videos and articles and other media platforms as a legal way to protect their content copyright, while 13.5 % indicated formal education as means to protecting their content creation copyrights. Lastly, nearly all the respondents (92.3 %) affirmed their awareness that it was a wrong step for someone to appropriate or repurpose their content without their consent, meanwhile 7.7 % did not see content copyright as illegal.

3.3. Discussion of the Results

This study clarified that content creators have adequate knowledge of fair content use, and oftentimes give credit to the creator of any content when they use such or get inspired for their self-created content. Furthermore, content creators are less likely to engage appropriation of other content creators' works without their consent, and in many occasions, they are less bothered about taking actions against those who appropriate their created contents. It is therefore justified that content creators have positive perception and attitude towards crediting the source of their ideas.

The finding of this study is in line with a review conducted by Frost[5], a writer at a Facebook***** advertisement agency who affirmed that it is important to credit the creative work of other creators on social media as this helps build the integrity of a creative work.

The postulation that content creators' works are infringed upon is found true to a reasonable extent, because content creators are aware of the possibility of created contents to be appropriated without any lethal consequence. Creators are also less bothered if their works are been appropriated since they are of the view that there will be no consequences or action taken against the infringers. Therefore, it is clarified that there is certainty of infringement on works of content creators via the social media platforms. This finding is in line with the study conducted by Nicdao et al. (2022) where they found that of the twenty-five content creators that has experienced copyright infringements of their works, only twelve made efforts to challenge the misappropriation, while the remaining thirteen did nothing despite the negative effect of the infringement on their works. This indicates that the likely reason for the abandonment is due to the uncertainty surrounding the implementation of their rights over their works.

The study found that majority of content creators understood the need to always tag an originator of any content when it is used to draw inspiration. Also, adopting watermarks and other form of personal branding is a protective measure for creators to adopt. It is also becoming a necessity to register creative contents that are of high value to avoid misappropriation on social media platforms. Thus, it is ascertained that adopting the identified measures will protect content creations from infringement on the social media platforms.

This study found that majority of the content creators had adequate knowledge of fair content use, and had a withdrawn perception towards the illegality of appropriating a created content without the consent of the originator. It shows that to a reasonable extent, content creators are aware of legal steps that can be adopted to protect their content copyrights. In line with this study, Tobin (2013) found that it is important to understand that users cannot just appropriate a creators work without considering the rights of the creator. Once the moral and economic rights of the creator are being violated, it falls outside the principle of fair use and there will be legal consequences for such violations. Creators must ensure to use other creator's works with caution and always give credit to the origin creator, as well as take appropriate measures to protect their own works.

---

5 Frost, N. (2023). Crediting Sources on Social Media: Why and How to Do It. https://clck.ru/3AQekF

Conclusions

Conclusively, it is an established fact that an author need not register their works before they can claim copyright, because, copyright is deemed created the moment the work is put in an expressive form and publicized, justifying that content creators has a right over their creations or works without any form of registration. Also, the common misconception that creative works of content creators on the internet or any social media platforms are in the public domain for public use without averting their minds to the true meaning of public domain which simply refers to those works and creations that are no longer under the protection of intellectual property laws due to several reasons. Therefore, this new wave of social media usage has resulted into freedom of distribution or circulation of various creative works through the social media platforms, which has grown into a large market for creators and different business minded people needs to be legally protected. Considerably, jobs are being created, new ways of trading and generating economy are springing up and possibility for infringing one another's rights is inevitable.

Millions of individuals interact on these platforms on a daily basis and it has grown at an exponential rate. Hence, attention should be given to the protection of creators' right through the appropriate legislation to eradicate all misconceptions.

Based on the findings of this study, the following recommendations are proposed:

– the use of visible water marks on works published on social media; Creators should explore multiple variants of water marks as will be suitable or compatible with the type of content they make.

– creators who have gathered significant influence in certain fields and are categorized as influencers should be mindful of their works, and register such works to reduce incident of infringement or unfair use.

– creators should also take extra precautions to ensure that their content is not infringing on any other creators work because such infringement would bruise the integrity of their own work.

– there should be proper enforcement of sanctions against intellectual property violators.

– there should be enactments made specifically for the protection of content creations on social media platforms.

– the content creators should be educated about these available legal protections over their works via training, workshops, and seminars.

---

* Instagram – The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.
** Twitter – The social network blocked in the territory of the Russian Federation for disseminating unlawful information.
*** YouTube – The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.
**** LinkedIn – The social network blocked in the territory of the Russian Federation.
***** Facebook – The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

References

Afolayan, O. T. (2022). Intellectual Property Rights Protection in Nigeria: Issues and Perspectives. Information Impact: *Journal of Information and Knowledge Management*, *13*(1), 1–9, https://dx.doi.org/10.4314/iijikm.v13i1.1

Aina-Pelemo, A. D., Ayodeji, J. F., & Alade, I. T. (2021). Implications of Covid-19 on Intellectual Property Rights: Case study of Unfair Competition and Restraint to trade. *Carnelian Journal of Law & Politics*, *2*(2), 1–12.

Aina-Pelemo, A. D., & Akpojaro, G. O. (2024). Understanding Copyright and Fair Use in the Academic World: A Case Study of the Faculty of Law. Redeemer's University Nigeria. *University of Benin Journal of Business Law (UBJBL)*, *4*(2), 1–33.

Alvarez-Monzocillo, J. M. (2022). *The Dynamics of Influencer Marketing.* Routledge Publishers.

Fagundes, D., & Perzanowski, A. K. (2020). Abandoning Copyright. *Faculty Publications*. 2060.

Fatoba, K. (2019). *Intellectual Property Rights – An Overview of Nigerian Legal Framework*. http://dx.doi.org/10.2139/ssrn.3501898

García, K. (2022). The Emperor›s New Copyright. Boston University Law Review, 2023 Forthcoming. *Georgetown University Law Center Research Paper*, 2023/09. http://dx.doi.org/10.2139/ssrn.4048315

Jerameel, K. (2021). *The Law Meets Memes and Says Hello: Rise of Intellectual Property Rights; Kenyan Reflection*. http://dx.doi.org/10.2139/ssrn.3868440

Nicdao, J. D., Fat, A. L. T., Bolo, P. D., & Mactal, J. B. (2022). Context, Engagement and Impact of Copyright Infringement Among Selected Content Creators: A Brief Descriptive Survey Study. *International Journal of Academic and Practical Research*, *1*(1), 33–39. http://dx.doi.org/10.13140/RG.2.2.35834.98240

Kupers, E., Lehmann-Wermser, A., McPherson, G., & van Geert, P. (2019). Children's Creativity: A Theoretical Framework and Systematic Review. *Review of Educational Research*, *89*(1). https://doi.org/10.3102/0034654318815707

Lei, D., & Xue, P. (2023). Incentives or disincentives? Intellectual property protection and FinTech innovation – Evidence from Chinese cities. *Finance Research Letters*, *58*, 104451. https://doi.org/10.1016/j.frl.2023.104451

Liu, S., & Zhong, C. (2024). Green growth: Intellectual property conflicts and prospects in the extraction of natural resources for sustainable development. *Resources Policy*, *89*, 104588. https://doi.org/10.1016/j.resourpol.2023.104588

Majekolagbe, F. (2016). *A Critique of Right Management and Copyright Enforcement by Copyright Society of Nigeria (COSON)*. http://dx.doi.org/10.2139/ssrn.4349522

Nkwor, L. (2023). *Copyright in Audiovisual Works and Performers' Rights in Nigeria: a Clash Rather Than a Connection?* http://dx.doi.org/10.2139/ssrn.4430288

Oriakhogba, D. (2018). The Scope and Standard of Originality and Fixation in Nigerian and South African Copyright Law. *African Journal of Intellectual Property*, *2*(2), 119–135. https://ssrn.com/abstract=3260567

Owushi, E. (2020). Protecting Copyright Owners in Nigeria: A Panacea for Intellectual Development. *International Journal of Knowledge Content Development & Technology*, *10*(1), 21–34. https://doi.org/10.5865/IJKCT.2020.10.1.021

Priyanshi, V. (2022). IP Rights for Social Media Influencers and Content Creators.

Reid, A. (2019). Copyright Policy As Catalyst and Barrier to Innovation and Free Expression. *Catholic University Law Review*, *68*(1). http://dx.doi.org/10.2139/ssrn.3345684

Saha, C. N., & Bhattacharya, S. (2011). Intellectual Property Rights: An Overview and Implications in Pharmaceutical Industry. *Journal of Advanced Pharmaceutical Technology & Research*, *2*(2), 88–93. https://doi.org/10.4103/2231-4040.82952

Subair, S. T., Adebola, S., & Yahya, D. (2019). Social Media: Usage and Influence on Undergraduate Studies in Nigerian Universities. *IJEDICT*, *15*(3), 53–62.

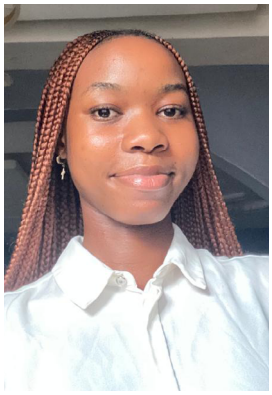
Tobin, J. (2013). *Earn It, Don't Buy It: The CMO's Guide to Social Media Marketing in a Post Facebook World Paperback*. Charles Pinot.

Zhang, C., & Xu, Y. (2023). Institutional innovation essence and knowledge innovation goal of intellectual property law in the big data era. *Journal of Innovation and Knowledge*, *8*(4), 100417. https://doi.org/10.1016/j.jik.2023.100417

Authors information

Adetutu Deborah Aina-Pelemo – PhD, Senior Lecturer (Assistant Professor), Department of Jurisprudence and International Law, Faculty of Law, Redeemer's University
Address: P.M.B 230, Ede, Osun-State, Nigeria
E-mail: aina-pelemoa@run.edu.ng
ORCID ID: https://orcid.org/0000-0002-4063-3983
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57195309994
WoS ResearcherID: https://www.webofscience.com/wos/author/record/2345323
Google Scholar ID: https://scholar.google.com/citations?user=IX160Y8AAAAJ

Ithamar Bassey – LL.B, Law Graduate, Faculty of Law, Redeemer's University
Address: P.M.B 230, Ede, Osun-State, Nigeria
E-mail: bassey7402@run.edu.ng
ORCID ID: https://orcid.org/0009-0004-9491-3392



Glorious Okeoghene Akpojaro– student, Faculty of Law, Redeemer's University
Address: P.M.B 230, Ede, Osun-State, Nigeria
E-mail: akpojaro@run.edu.ng
ORCID ID: https://orcid.org/0009-0007-2918-5431
Google Scholar ID: https://scholar.google.com/citations?user=lu56_usAAAAJ

Authors' contributions

Aina-Pelemo A. D. provided general guidance and set the study objectives; searched and selected scientific literature; critically evaluated the interpretation of the study results; formulated key conclusions, suggestions and recommendations; approved the final version of the article.

Bassey I. analyzed the national legislation; interpreted the study results; organized the sociological survey and drafted the manuscript.

Akpojaro G. O. collected and analyzed literature and legislation; conducted the sociological survey; interpreted the study results; organized the sociological survey and drafted the manuscript.

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 – February 5, 2023
Date of approval – March 3, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:34.096:347.211
EDN: https://elibrary.ru/hiqzuj
DOI: https://doi.org/10.21202/jdtl.2024.21

Меры профилактики нарушений авторских прав на создание контента в цифровой среде: опыт Нигерии

Адетуту Дебора Айна-Пелемо ✉
Университет Искупителя, Эде, Нигерия

Итамар Басси
Университет Искупителя, Эде, Нигерия

Глориос Океоген Акподжаро
Университет Искупителя, Эде, Нигерия

Ключевые слова

авторское право,
интернет,
онлайн-контент,
право интеллектуальной собственности,
правовая защита,
профилактика нарушений авторских прав,
социальная сеть,
цифровая платформа,
цифровой маркетинг,
цифровые технологии

Аннотация

Цель: определить уровень защищенности прав авторов контента в социальных сетях и выработать меры профилактики правонарушений в данной области.

Методы: на достижение поставленной цели был направлен социологический и правовой познавательный инструментарий, включающий доктринальный метод исследования предметной области, с получением данных из «первых уст» с учетом воздействующих факторов и обстоятельств. Основные результаты получены при помощи социологического метода, используемого для сбора данных на основе разработанной анкеты, содержащей четыре исследовательских вопроса: (1) каковы представления и мнения третьих лиц или пользователей относительно роли создателя контента; (2) нарушаются ли права создателей контента на их произведения; (3) каковы способы защиты созданного контента от посягательств со стороны платформ; (4) как можно защитить права создателей контента. В основе полученных эмпирических данных и их обобщений находилась комбинация видов анализа, в том числе контент-анализ первичных и вторичных источников права.

Результаты: в последние годы создаваемый в социальных сетях контент превратился в сложную индустрию, которая меняет как традиционное понимание творческого самовыражения, так и реализацию прав интеллектуальной собственности. На примере опыта Нигерии

✉ Контактное лицо

предпринята попытка изучить права и меры защиты, предоставляемые создателям цифрового контента в соответствии с законодательством об интеллектуальной собственности. Как показало исследование, в настоящее время не существует достаточного количества научных работ в этой области или развитого законодательства по защите произведений в социальных сетях. Делается вывод о необходимости совершенствования законодательных актов по защите прав на контент в социальных сетях, в отсутствие которого авторам онлайн-произведений рекомендуется прибегать к более радикальным методам в обеспечении своих прав, чтобы уменьшить количество случаев незаконного присвоения интеллектуальной собственности. Создателям таких произведений предлагается обеспечивать защиту своих прав, основываясь на принципах доктрины добросовестного использования.

Научная новизна: исследование структурировано по исследовательским вопросам, касающимся нарушений и способов защиты прав создателей контента, адресованным респондентам из разных стран, значительная часть которых специализируется преимущественно на создании контента в разных социальных сферах посредством нескольких медиа-платформ и социальных сетей.

Практическая значимость: выводы и рекомендации позволят минимизировать риски нарушения прав интеллектуальной собственности создателей контента, которые могут возникнуть при широком использовании социальных сетей, а также повысить уровень защиты прав на созданное в виде онлайн-контента произведение.

Для цитирования

Айна-Пелемо, А. Д., Басси, И., Акподжаро, Г. О. (2024). Меры профилактики нарушений авторских прав на создание контента в цифровой среде: опыт Нигерии. *Journal of Digital Technologies and Law*, *2*(2), 408–429. https://doi.org/10.21202/jdtl.2024.21

Список литературы

Afolayan, O. T. (2022). Intellectual Property Rights Protection in Nigeria: Issues and Perspectives. Information Impact: *Journal of Information and Knowledge Management*, *13*(1), 1–9, https://dx.doi.org/10.4314/iijikm.v13i1.1

Aina-Pelemo, A. D., Ayodeji, J. F., & Alade, I. T. (2021). Implications of Covid-19 on Intellectual Property Rights: Case study of Unfair Competition and Restraint to trade. *Carnelian Journal of Law & Politics*, *2*(2), 1–12.

Aina-Pelemo, A. D., & Akpojaro, G. O. (2024). Understanding Copyright and Fair Use in the Academic World: A Case Study of the Faculty of Law. Redeemer's University Nigeria. *University of Benin Journal of Business Law (UBJBL)*, *4*(2), 1–33.

Alvarez-Monzocillo, J. M. (2022). *The Dynamics of Influencer Marketing.* Routledge Publishers.

Fagundes, D., & Perzanowski, A. K. (2020). Abandoning Copyright. *Faculty Publications*. 2060.

Fatoba, K. (2019). *Intellectual Property Rights – An Overview of Nigerian Legal Framework*. http://dx.doi.org/10.2139/ssrn.3501898

García, K. (2022). The Emperor›s New Copyright. Boston University Law Review, 2023 Forthcoming. *Georgetown University Law Center Research Paper*, 2023/09. http://dx.doi.org/10.2139/ssrn.4048315

Jerameel, K. (2021). *The Law Meets Memes and Says Hello: Rise of Intellectual Property Rights; Kenyan Reflection*. http://dx.doi.org/10.2139/ssrn.3868440

Nicdao, J. D., Fat, A. L. T., Bolo, P. D., & Mactal, J. B. (2022). Context, Engagement and Impact of Copyright Infringement Among Selected Content Creators: A Brief Descriptive Survey Study. *International Journal of Academic and Practical Research*, *1*(1), 33–39. http://dx.doi.org/10.13140/RG.2.2.35834.98240

Kupers, E., Lehmann-Wermser, A., McPherson, G., & van Geert, P. (2019). Children's Creativity: A Theoretical Framework and Systematic Review. *Review of Educational Research*, *89*(1). https://doi.org/10.3102/0034654318815707

Lei, D., & Xue, P. (2023). Incentives or disincentives? Intellectual property protection and FinTech innovation – Evidence from Chinese cities. *Finance Research Letters*, *58*, 104451. https://doi.org/10.1016/j.frl.2023.104451

Liu, S., & Zhong, C. (2024). Green growth: Intellectual property conflicts and prospects in the extraction of natural resources for sustainable development. *Resources Policy*, *89*, 104588. https://doi.org/10.1016/j.resourpol.2023.104588

Majekolagbe, F. (2016). *A Critique of Right Management and Copyright Enforcement by Copyright Society of Nigeria (COSON)*. http://dx.doi.org/10.2139/ssrn.4349522

Nkwor, L. (2023). *Copyright in Audiovisual Works and Performers' Rights in Nigeria: a Clash Rather Than a Connection?* http://dx.doi.org/10.2139/ssrn.4430288

Oriakhogba, D. (2018). The Scope and Standard of Originality and Fixation in Nigerian and South African Copyright Law. *African Journal of Intellectual Property*, *2*(2), 119–135. https://ssrn.com/abstract=3260567

Owushi, E. (2020). Protecting Copyright Owners in Nigeria: A Panacea for Intellectual Development. *International Journal of Knowledge Content Development & Technology*, *10*(1), 21–34. https://doi.org/10.5865/IJKCT.2020.10.1.021

Priyanshi, V. (2022). IP Rights for Social Media Influencers and Content Creators.

Reid, A. (2019). Copyright Policy As Catalyst and Barrier to Innovation and Free Expression. *Catholic University Law Review*, *68*(1). http://dx.doi.org/10.2139/ssrn.3345684

Saha, C. N., & Bhattacharya, S. (2011). Intellectual Property Rights: An Overview and Implications in Pharmaceutical Industry. *Journal of Advanced Pharmaceutical Technology & Research*, *2*(2), 88–93. https://doi.org/10.4103/2231-4040.82952

Subair, S. T., Adebola, S., & Yahya, D. (2019). Social Media: Usage and Influence on Undergraduate Studies in Nigerian Universities. *IJEDICT*, *15*(3), 53–62.

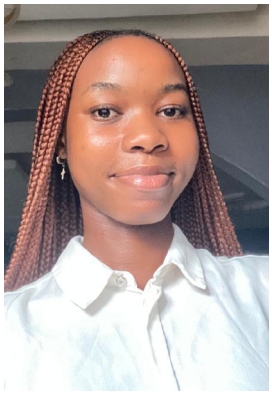
Tobin, J. (2013). *Earn It, Don't Buy It: The CMO's Guide to Social Media Marketing in a Post Facebook World Paperback*. Charles Pinot.

Zhang, C., & Xu, Y. (2023). Institutional innovation essence and knowledge innovation goal of intellectual property law in the big data era. *Journal of Innovation and Knowledge*, *8*(4), 100417. https://doi.org/10.1016/j.jik.2023.100417

Сведения об авторах

Айна-Пелемо Адетуту Дебора – PhD, старший преподаватель (доцент), кафедра юриспруденции и международного права, юридический факультет, Университет Искупителя
Адрес: Нигерия, штат Осун, Эде, P.M.B 230
E-mail: aina-pelemoa@run.edu.ng
ORCID ID: https://orcid.org/0000-0002-4063-3983
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57195309994
WoS ResearcherID: https://www.webofscience.com/wos/author/record/2345323
Google Scholar ID: https://scholar.google.com/citations?user=IX160Y8AAAAJ

Басси Итамар – бакалавр права, юридический факультет, Университет Искупителя
Адрес: Нигерия, штат Осун, Эде, P.M.B 230
E-mail: bassey7402@run.edu.ng
ORCID ID: https://orcid.org/0009-0004-9491-3392



Акподжаро Глориос Океоген – студент, юридический факультет, Университет Искупителя
Адрес: Нигерия, штат Осун, Эде, P.M.B 230
E-mail: akpojaro@run.edu.ng
ORCID ID: https://orcid.org/0009-0007-2918-5431
Google Scholar ID: https://scholar.google.com/citations?user=lu56_usAAAAJ

Вклад авторов

А. Д. Айна-Пелемо осуществляла общее руководство и постановку задач исследования; поиск и подбор научной литературы; критическую оценку интерпретации результатов исследования; формулировку ключевых выводов, предложений и рекомендаций; утверждение окончательного варианта статьи.

И. Басси осуществляла анализ национального законодательства; выполняла интерпретацию результатов исследования; организовала проведение социологического опроса и подготовку черновика рукописи.

Г. О. Акподжаро занималась сбором и анализом литературы и законодательства; проводила социологический опрос; выполняла интерпретацию результатов исследования; осуществляла подготовку чистовика рукописи.

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: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 5 февраля 2024 г.
Дата одобрения после рецензирования – 3 марта 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:347.4:004.4
EDN: https://elibrary.ru/lvpigr
DOI: https://doi.org/10.21202/jdtl.2024.22

Public-Private Partnership Agreement in the Context of the Matrix for Assessing their Legal Parameters and Digitalization

Dominique T. Molintas

PATTS College of Aeronautics, Paranaque, Philippines;
Griffith University, Queensland, Australia

Keywords

agreement,
conflict of interest,
contract,
digital technologies,
digitalization,
law,
legal assessment,
public-private partnership,
restraint of competition,
risk management

Abstract

Objective: by reviewing the legal aspects of public-private partnership agreements, to synthesize their main provisions into a common matrix, which, when digitized, can be used to standardize and simplify the formulation of agreement parameters.

Methods: the author relied on comparative-legal analysis of scientific literature, legislation and Internet sources on public-private partnership, supplemented by a review of public-private partnership agreements in various socio-political spheres, which made it possible to create a science-based and practice-oriented matrix that can serve as a tool for drafting public-private partnership agreements.

Results: national aspects in the legal regulation of the said relations in different countries were highlighted; a number of peculiarities encountered in public-private partnership agreements were described.

Scientific novelty: taking into account the most important legal peculiarities characteristic of different countries, a matrix for drafting public-private partnership agreements is presented, including eight main parameters: 1 – value received, scope, benefits and risks, 2 – route to market, 3 – restraint of competition, 4 – conflict of interest and procurement issues, 5 – powers, approvals, legal assessment, 6 – liabilities, dispute resolution, 7 – ownership structure, governance and level of autonomy, 8 – exit strategies. Depending on the priorities identified, the matrix can be modified, taking into account that priorities define and shape the specific parameters of each individual partnership.

Practical significance: the matrix obtained can become a planning tool used to analyze and understand the relationships between the eight legal parameters necessary for the formation of relations in the sphere of public-private partnership. It may serve as a legal reference point for the formulation of public-private partnership agreements around the world, and will contribute not only to the revitalization of public-private partnerships, but also to a proper understanding of obligations, responsibilities and limitations. The recommendations provided in the study show direction for the evaluation of public-private partnerships, allowing clear conclusions to be drawn about the partnership. Digital accessibility provided, the proposed matrix will be of interest to many organizations that use public-private partnerships in their professional activities.

For citation

Molintas, D. T. (2024). Public-Private Partnership Agreement in the Context of the Matrix for Assessing their Legal Parameters and Digitalization. *Journal of Digital Technologies and Law, 2*(2), 430–449. https://doi.org/10.21202/jdtl.2024.22

Contents

Introduction

Investing in built environment brings forth significant economic progress and social development. Built environment stimulates trade that results in output growth, increased microeconomic efficiency and reduced transaction costs (Jayachandran, 2021). In poor nations where one finds Government budgets already fully allocated, Public Private Partnerships PPP dominate the procurement platform for built environment (Moffatt & Kohler, 2008). Numerous PPP Contracts had been forged as a mechanism to raise risk tolerance and prolong project life[1].

A compilation of critical legal points across regions, are put together in this study to form a matrix to digitalize of the legal features of PPP. A PPP requires a definitive instrument that outlines the understanding between the parties to the intended venture (Leigland, 2018). The contract ought to outline the contributions, expectations, obligations, rights, and duties and responsibilities of the parties. A contract sorts out the key elements such as the mechanism on how profits and liabilities are to be assigned, specifically to avoid disputes (González-Ruiz et al., 2018).

To determine a best fit PPP contract, an appraisal tool is developed using a 4×4 matrix. The argument of function on the vertical axis and horizontal axes are defined below. Noteworthy legal points of different nations are highlighted in this study. These are particularly interesting stipulations that standout among the several Government contracts.

1. Value captured, scope, benefits and risks

1.1. Powers, approvals and due diligence

Chinese Law allows for the flexibility in the determination of both, the composition of board of directors alongside delimit of authority over the operations. Indonesian Law permits Government to enter into PPP Contract with private entities for infrastructure projects[2]. The process for entering into such contracts is governed by PPP laws and regulations, as well as Presidential Regulation No. 38 of 2015 for the co-operation between Government and the business entity for infrastructure development (Rybnicek et al., 2020; Buso et al., 2021).

PPP Contracts in the State of Queensland do not stipulate guarantees of the State over the obligations and performance over the partnership. In the United Kingdom, centralization and formality is a foremost concern over the creation of special purpose vehicles to ensure

1 The World Bank. (2017, April 27). PPP Reference Guide 3.0 (Full version). https://clck.ru/3AgJNx

2 Eddymurthy, I., & Mooduto, N. (2017). Joint ventures in Indonesia: overview. Jakarta: SSEK Indonesian Legal Consultants. https://clck.ru/3AgJS8

its function. Under Australian Law, the PPP is established when significant synergy is demonstrated. Such can be substantiated in increased export earnings or cheaper goods (Jokar et al., 2021). A PPP must substantiate efficiency or reduction in costs by reason of the activity that a project or program is being conducted by the group as a whole rather than by individual members of the group[3].

1.2. Ownership structure, governance and level of autonomy

PPP is not expressly regulated under Japanese law and partnership contracts are regulated under the Civil Code Act No. 89 of 1896 and the Companies Act No. 86 of 2005[4]. A PPP partner under Belgian legislation is expected to contribute 25 percent of the registered capital. The minimum capital share to establish PPP with a public company is €61,500. Indonesian Law[5] stipulates PPPs in a legal entity that has limited liability status, under Company Law (Chen & Hubbard , 2012).

PPP Governance structures with high to activity in policy functions include: The Mission d'appui à la réalisation des partenariats public–privé /MAPPP[6] as the governance institution in France; the Special Secretariat for PPPs Dissemination as the governance institution in Greece; the Unita Tecnicà Finanza di Progetto /UTFP, the technical unit for project financing in Italy[7]; in Portugal by the Commission for PPPs; and The United Kingdom for Infrastructure Local Partnerships (Demirag et al., 2011; Rybnicek et al., 2020; Ito, 2020).

1.3. Liabilities, dispute resolution

Indonesian Law stipulates the aggregate issued and paid-up share capital must be no less than 25 percent of the PPP authorized share capital. An exception for micro, small and medium enterprises, for authorized share capital below IDR50 million, stipulated in Government Regulation No. 29 of 2016, with flexible payment for shares can be made in cash or in kind. Legislation in Brazil[8] stipulates a corporation and sociedades limitadas

---

3 Government of Australia. (2016). National Guidelines for Infrastructure Project Delivery. Canberra: The Department of Infrastructure, Transport, Regional Development, Communications and the Arts. https://goo.su/9k38lH

4 Association of Southeast Asian Nations. (1980). Supplementary Agreement to the Basic Agreement on Asean urea project. Indonesia. Jakarta. https://clck.ru/3AgJbY

5 Government of the Republic of Indonesia. (1979). Agreement between the Government of the Republic of Indonesia and the United Nations High Commissioner for Refugees regarding the Establishment of the Office of the UNHCR representative for Indonesia. Jakarta: Government of the Republic of Indonesia. https://goo.su/kUK0k

6 MAPPP – Mission to support the implementation of public-private partnership contracts. (In French). https://clck.ru/3AgJhn

7 Presidenza del Consiglio dei Ministri. (2010). Unita Tecnica Finanza di Progetto (UTPF). (In Italian). https://clck.ru/3AgJim

8 National Congress. (2004). Brazil's Public-Private Partnership Law. Brasilia: Lei de Licitações e Contratos Administrativos. (In Portuguese). https://goo.su/yOEZc5

is to afford the limited liability protection to shareholders; except for environmental and anti-trust laws, anti-bribery, labour case laws and consumer laws—where a shareholder can become personally liable (Kurniawan et al., 2015; Wang, 2003).

Queensland Courts capacitate the PPP to apply for statutory order for a trust, sale or partition to resolve dispute resolution. At the same time, the parent company Board of Directors is accountable to ensure the guidelines are followed. Specifically for Public Private Partnerships in China, foreign participant is required to pledge no intention to intrude upon China's sovereignty or to exploit its resources (Salem, 1981); Legislation for PPP dispute[9] resolution ought to avoid lengthy lead times before proceedings commence; and better not seek to oust the jurisdiction of the courts to give urgent interlocutory or final relief.

1.4. Exit strategies

A noticeable omission in Thai laws on early termination in the PISU Act, although it is featured in the EEC framework and the New PPP Act. In the event that early termination is not the fault of the private entity, Government is to appropriately compensate what is fair using proper calculation mechanism. This reflects the partnership concept and ensures private participation is carefully qualified. For cases where the early termination is because of acts or deeds by the private entity; the state is entitled to recover its loss arising out of such breach (Garg & Garg, 2016, Wegrich et al., 2017; Hart, 2003).

British Law permits the termination of PPP operations by mutual consent of the parties; otherwise a breach by one of the parties or by force majeure. In Korea, foreign-invested enterprises and assets invested by foreign investors are not subject to nationalization or seizure by the State. A foreign investor is permitted to reinvest a portion of profits, or the all of it within the territory of the DPRK (Lee, 2003).

Chinese Taxation Law encourages the deposit of funds in the Bank of China by permitting a tax refund on the reinvested amount. By so, the whole or part of the income tax already paid on the reinvested portion may be recovered. In the event that the nationalization or seizure by the State of enterprises and assets, fair compensation is to be paid (Jin & Huang, 2021).

[9] US Security Exchange and Commission. (2008). Sino-Foreign Joint Venture Contract by and between Sun Far East Limited and Zibo Bao Kai Trading Company, LTD. for establishing Taixing Zhongneng Far East Silicon Co., LtD. USA: SEC. https://clck.ru/3AgJsr

2. Route to market

2.1. Powers, approvals and due diligence

In Spain, the Unión Temporal de Empresas \UTE, is the temporary consortium in effect for PPP. In the USA, the Special Purpose Vehicle dictates the areas of liability and allocation of exposure such as defense hold harmless provision and indemnification (DoD NASA, 2020; Noring, 2019). In Queensland Territory, when the disposal of a PPP Interest is decided in whole or in part; a Deed of Covenant is executed between existing parties and an incoming participant. AusTrade PPP Grant is a special Public Private Partnership where the Australian Government issues a Grant to SMEs to co-operate to pursue specific export activities. Approval enables the group to be eligible, to access the grant scheme of AU$ 150,000 annually[10] at maximum.

2.2. Ownership structure, governance and level of autonomy

Public Private Partnership units structured under Ministries or institutions, having policy functions that churned out very low to medium activity, or closed down: Austria PPP Kompetenzzentrum; Czech Republic PPP Centrum; Denmark by the PPP knowledge unit; Netherlands by the PPS support; Serbia by the Odbor partnerských projektov; Slovak Republic Sektor za upravljanje javnega premoženja or Division for public property management. Thai law stipulates the Cabinet as final approving authority to the private entity selection and the draft PPP contract during the procurement stage (Hennessey, 2021).

The role of the Cabinet during the procurement stage may be reduced in the upcoming New PPP Act to increase efficiency and flexibility in the PPP process (Mirzaee & Sardroud, 2022). National infrastructure procured through PPP includes the U-Tapao International Airport, High-speed railway connection to three major airports, Map Ta Phut Industrial Port Phase III, Laem Chabang Port Phase III and Digital Park Thailand[11]. Indian Law[12] stipulates that the Government entity intending to enter PPP with the private sector must first explore the possibility of meeting objectives through alternate means, other than PPP (Selim & ElGohary, 2020). In Europe, the structure of the PPP must primarily be compatible with the internal market to promote economic development; particularly in regions where the standard of living is abnormally low or there is underemployment (Yurdakul et al., 2022). The EU regions referred to in Article 349[13], in view of structural, economic and social situation.

---

[10] Austrade Export Market Development Grants Canberra. (2020). https://goo.su/rnYK

[11] Ponte, J. de. (2021). Delivering Thailand's Infrastructure Pipeline – The PPP push. Melbourne: DLA Piper Global Services LLP. https://clck.ru/3AgK8V

[12] Ministry of Finance. (2009). Joint Ventures: a guidance note for public sector bodies forming joint ventures with the private sector. New Delhi: Government of India. https://clck.ru/3AgK9j

[13] Hatton, C., Cardwell, D., & Botts, B. (2020, July 8). European Union: Joint Ventures. Global Competition Review. https://clck.ru/3AgKCF

2.3. Liabilities, dispute resolution

Arbitration is not practiced under Cyprus legislation determined the District Courts as the competent authority to act on dispute resolution[14]. Indians Law determines the Government Directors on the Board of PPP accountable and liable for certain actions and decisions of the PPP; for any lapses or failures (Liu et al., 2016a; Ma et al., 2023; Liu et al., 2016b; Rufín & Rivera-Santos, 2012).

While in Europe, the European Economic Interest Group /EEIG are the established Council. The structure is defined through a contract made between the participants, who have joint liability for the debts and liabilities of the EEIG. Unless defined otherwise, the EEIG appoints the managers of the PPP (Whiteside, 2020).

Specific to Queensland Territory, the PPP contract include the right of access books and accounts of the GOC PPP by the GOC and its auditors. While under Chinese Law, PPP provides significantly greater degree of flexibility in determining the composition of the controlling organ of the joint venture than do a number of other socialist countries (Wang et al., 2019).

2.4. Exit strategies

British Law stipulates the termination of the PPP may be done by mutual agreement of the parties; otherwise by a breach by either one of the parties; or by force majeure.

PPP law in UK permits shareholder exit options through call options over a shareholder share or offering and pre-emptive right. European antitrust or competition laws underscore structure and purpose of the venture. The PPP must consider the market in which it competes, and any restrictions that it imposes on the parties that can generate efficiencies; otherwise encourage anti-competitive restriction, such as price-fixing or market sharing (Owen Liu, Xiong & Zhu, 2007).

PPP prescriptions observed under Emirati Law[15] are presumed restrictive. These dictate confidentiality and non-solicitation clauses, prohibiting shareholders from soliciting for own purpose. The disposition and acquisition of shares that might contain 'piggy-back', 'tag-along' or 'drag-along' rights in the event of a third- party share sale, such as pharmaceuticals industry or the petrochemicals industry among others (Sharma, 2022).

[14] The Private Sector Participation Governing Rules. https://clck.ru/3AgKRH

[15] Mohammed bin Rashid Al Maktoum, Ruler of Dubai (2017). Law No. (22) of 2015 Regulating Partnership between the Public Sector and the Private Sector in the Emirate of Dubai. Dubai: The Supreme Legislation Committee in the Emirate of Dubai. https://clck.ru/3AgKKF

3. Restraint of competition

3.1. Powers, approvals and due diligence

PPP in Europe[16] stipulates incompatibility of aid grants or resources which distort or threaten competition by favoring certain undertakings or the production with the internal market of Europe (Rossi & Civitillo, 2014). The Government of Queensland[17] requires that a PPP must present strategic advantages, particularly for highly regulated sectors. As an example, the PPP with Singapore firms explicitly state for arbitration in Singapore. Under Korean Law[18], specific sectors are identified for PPP, to include industry, agriculture, construction, transport, telecoms, science and technology, tourism and financial services. Investment that encumber the development of the national economy and threaten national security, or technically obsolete and harmful to the environment, shall be prohibited or restricted (Hurk et al., 2016; Soomro & Yuhui, 2023; Liu et al., 2014).

3.2. Ownership structure, governance and level of autonomy

The African Law on PPP prohibits agreement or practice between competitors that results in direct price fixing and allocation of markets; collusive tendering and setting of minimum and resale prices. Under Malaysia law, the landscape of involvement in PPP varies from concessionaire, privatization to partnerships (Biygautane et al., 2020). The collaboration of local practitioners, mostly among Asian nations concerns typical infrastructure developments. Under Australian Law the Competition and Consumer Act 2010 prohibits and criminalizes the cartel conduct in PPP. Under German Law, infringement of the cartel prohibition is criminalized (Outhuijse, 2020).

A PPP that comprises ownership concentration of the independent market players might risk infringement of the cartel prohibition. Otherwise, when both parent companies stay active in the given market, there is a risk that the PPP will be considered to be of a co-operative nature; and the players at risk of infringement of the cartel prohibition. Under German law, PPP can be organized depending on the depth of co-operation the partners elect companies other than partnerships such as the PPP corporation OR Aktiengesellschaft; or the limited liability company, Gesellschaft mit beschränkter Haftung; Silent partnerships or stille Gesellschaft and sub-participations or Unterbeteiligung are also used in German law to organize PPP (Darko et al., 2023).

---

16 Hatton, C., Cardwell, D., & Botts, B. (2020, July 8). European Union: Joint Ventures. Global Competition Review. https://clck.ru/3AgKYR

17 Queensland Treasury and Trade. (2013). Government Owned Corporations Guidelines for Joint Venture Agreements. Queensland Treasury. https://goo.su/v45h3t

18 Standing Committee of the Supreme People's Assembly. (1992). The law of the Democratic People's Republic of Korea on foreign investment. Seoul: Fourth Session of the Ninth Supreme People's.

3.3. Liabilities, dispute resolution

Under Australian Law, one should not avoid the lengthy proceedings of dispute resolution or seek to oust the jurisdiction of the Courts to give urgent interlocutory or final relief[19]. British Venture Law provides for consultation, conciliation, arbitration, and judicial procedure – in that order of preference, for the resolution of disputes arising during the life of the venture (Khallaf et al., 2021). Indonesian law prohibits practices that aim to unfairly restrict competition under the "Prohibition of monopolistic practices and unfair business competition or anti- monopoly law." As an example, a market dominant entity from abusing its position by unfairly restricts its competitors' activities. A non-competition clause may not hold up before the Indonesian Competition Supervisory Body entered into by an industry-dominant business player.

Under Japanese Law[20], restricted industries are industries considered to be affected with great public interest, such as water works, railroads, banking, and maritime transportation (Bradshaw, 1963).

3.4. Exit strategies

Under UAE Law, arbitration is conducted by the Dubai International Arbitration Centre or DIAC or in the DIFC-LCIA or the London Court of International Arbitration and under the DIFC-LCIA rules recommended for adoption that specific place for arbitration is decided at the outset[21]. Under Korean Law, the PPP is subjected to basic governing antitrust and fair competition issues in Korea stipulated in the Monopoly Regulation and Fair-Trade Act[22]. Alternately, PPP via merger and acquisition is caught through the Korean Merger Control Legislation, if a business combination total worldwide assets or turnover is equal or greater KRW300b or UR 257.1 million. Under Australian Laws, the disposal and assignment of PPP interest by a PPP within Government: A Disposal or Assignment should not require the consent of the PPP. Under Indian Law the executing Government entity would have to assess possible recourse to recover investment in case the PPP is unsuccessful.

---

19 Seungwoo Son. (2012). Legal analysis on Public-Private Partnerships regarding Model PPP Rules. https://clck.ru/3AgKta

20 Matsuura, M., Niunoya, M., & Hamasu, Sh. (2023). A structured guide to public private partnerships in Japan. Atsumi & Saka. https://clck.ru/3AgKue

21 HM Treasury. (2010, March). Joint Ventures: a guidance note for public sector bodies forming joint ventures with the private sector. London: Government of UK. https://clck.ru/3AgKva

22 Tae Hee Lee. (2020). International Joint Ventures in Korea. Seoul: Lee & Ko. https://clck.ru/3AgKwa

4. Conflict of interest / procurement issues

4.1. Powers, approvals and due diligence

Under Australian Law, PPP permits unqualified right to disclose confidential information and reversely the right to disclose qualified information. In Cyprus arbitration is not practiced, and the District Courts of Cyprus are the competent authority to act (Caperchione et al., 2017). Under Korean Law, impairments to fair competition include discrimination and abuse of superior bargaining position; false, deceptive, or misleading advertising. Under the Law of Malaysia, measures have been implemented to expedite an overall project approval process for PPP, whereby the approval timeline has been reduced to 8–10 months. These regulations are applicable to investment projects deemed highly important as determined by the EEC Policy Committee, which require submission for consideration prior to approval. Under Chinese law, the four main steps to establish PPP are: Obtaining the assistance of the China International Trust and Investment Corporation; negotiating the legal framework of the joint venture; obtaining the authorization of the Foreign Investment Commission of PROC; and registering with the General Administration for Industry and Commerce (Liyanapathirana et al., 2023).

4.2. Ownership structure, governance and level of autonomy

Public Private Partnership of Democratic People's Republic of Korea permits equity and contractual joint ventures to set up and operate wholly foreign-owned enterprises in the Free Economic and Trade Zone. Under Australian Laws[23] the PPP must permit the unqualified right to disclose confidential information by the Government Owned Corporation PPP; and reversely disclose qualified information (Azarian et al., 2023). In Slovakia[24], Liability is regulated by the commercial code, but among the partners there is a lot of contractual freedom since there is no explicit law on PPP. Under Indian Law[25] a PPP is set up as an autonomous statutory organization and similar guidelines for the organized Group. European Legislation the covenants not to compete are determined upon formation of the joint venture the parties agree not to compete outside of the joint venture[26].

4.3. Liabilities, dispute resolution

In Queensland territory a parent PPP should not provide guarantees or assume any liabilities of the PPP unless specifically approved by shareholding Ministers and consistent Investment

[23] Griffiths, A., & Carney, N. (2023). An introduction to public-private partnerships in Australia. Lexology. https://clck.ru/3AgLab

[24] Ministry of Finance of the Slovak Republic. Public Private Partnership (PPP). https://clck.ru/3AgLbZ

[25] Government of India. Public Private Partnership In India. https://goo.su/qlmvkUI

[26] Giguère, S. (2001). Local governance and partnerships. A summary of the findings of the OECD study on local partnerships. Paris: Organisation for Economic Co-operation and Development. https://goo.su/G5ctv

Guidelines (Ojelabi & Noone, 2020). Under Korean Law any disagreement concerning foreign investment shall be settled through consultation. Disputes shall be examined and settled by a court of law or arbitration body otherwise disagreement may be taken to an arbitration agency in the third countries for settlement[27]. Under New Zealand law, for all kinds of PPP structure; actions subjected laws where a dispute arises and free to agree different dispute resolution place or process; when there is failure of competition when there is only a single interested party remaining (Chou & Lin, 2012).

Under German Law, the material merger control provisions: If the PPP partners can prove that despite the creation or strengthening of a market dominating provisions, the PPP improves the competitive conditions in the same or another market that outweighs the negative impact of market dominance, the FCO may still grant merger clearance a substantive test market dominance is performed and the PPP must be prohibited if it creates a market dominating position. In American law, the PPP dictates liability, the structure of exposure is determined to include defense, indemnification and hold harmless clause.

4.4. Exit strategies

Under British Law, PPP operations may be terminated by mutual agreement of the venture parties, by a breach by one of the parties or by force majeure (Marques, 2021). Under Korean Law[28], the parties are free to resort to any court of competent jurisdiction within or outside Korea to settle the disputes arising under PPP possible legal remedies include monetary compensation for harm or loss, related provisional attachments, and equitable remedies of specific performance, and temporary and permanent injunction (Lemley & McCreary, 2020).

Under New Zealand laws, shareholders in the PPP do not owe fiduciary obligations to one another. Under Indian Law, the typical exit strategies for international projects: sale, trade, and merger, aggregate or liquidate; claim against insurance or guarantee; haul away or walk away; litigate or arbitrate.

Conclusions

Each legal feature of the partnership contract is weighed across four different legal arguments, signifying a well-crafted agreement. The guidelines below provide direction and clarity, and enables crucial thinking. Therefore, it is sufficient to state that the work is excellent.

[27] Mirza & Associates. (2023, May 23). The pros and cons of arbitration vs. litigation: What's the best option for your Business? Mondaq. https://clck.ru/3AgLhv

[28] Standing Committee of the Supreme People's Assembly. (1992). The law of the Democratic People's Republic of Korea on foreign investment. Seoul: Fourth Session of the Ninth Supreme People's. https://clck.ru/3AgLjY

PPP Guidelines

Matrix Of Mechanisms		Powers, Approvals & Due Diligence	Ownership Structure (Governance & Level of Autonomy)	Liabilities, Dispute Resolution	Exit Strategies
	Value Captured (Scope, benefits & risks)	A joint venture is established when significant synergy is forecast to substantiate increase in export earnings, or cheaper consumer services and goods	PPP is compatible with the local market to promote economic development, especially where the standard of living is abnormally low or underemployment	The PPP in the form of a Special Purpose Vehicle can afford the limited liability protection to shareholders; except for environmental and anti-trust laws	Any Agency or GOC should not provide guarantees or assume any liabilities of the PPP unless specifically approved by the Secretary, and consistent with the Investment Guidelines
	Route to Market	The PPP provides for a Deed of Covenant to be executed between existing participants, with reasonable and defined timeframes	PPP Guidelines should restrict industries affected with great public interest: Transport, energy or education. The role of Government is to protect National Infrastructure Assets	Government Secretaries, Directors on the Board of the PPP would be liable and accountable for certain actions and decisions of the PPP for any lapses or failures	Arbitration ought to be put down at the outset such as the London Court of International Arbitration and under whose rules
	Restraints of Competition	The PPP should explicitly prohibit and criminalize the cartel conduct. The role of government is to protect the impact on the economy and NOT the PPP profitability	Government can enter into PPP agreements with private entities for infrastructure projects, provided a step in or takeover can be performed by the sovereignty—no other	A PPP is subjected to basic governing antitrust and fair competition issues: Monopoly and Fair Trade	PPP Agreements must not allow the private sector to take over the undertaking of the projects in its entirety after project completion
	Conflict of Interest (Procurement Issues)	A PPP is not supposed to cause impairments to fair competition: Discrimination, abuse of superior bargaining position; including false, deceptive, or misleading advertising	The Covenants Not to Compete are determined upon formation of the PPP where the parties agree not to compete outside of the joint venture	PPP s or Aid Grants granted or funding resources which distorts or threatens competition by favoring certain undertakings shall be deemed incompatible	

References

Azarian, M., Shiferaw, A. T., Lædre, O., Wondimu, P. A., & Stevik, T. K. (2023). Project ownership in public-private partnership (PPP) projects of Norway. *Procedia Computer Science*, *219*, 1838–1846. https://doi.org/10.1016/j.procs.2023.01.481

Biygautane, Mh., Neesham, C., & Al-Yahya, Kh. O. (2020). Institutional entrepreneurship and infrastructure public-private partnership (PPP): Unpacking the role of social actors in implementing PPP projects. *International Journal of Project Management*, *37*(1), 192–219. https://doi.org/10.1016/j.ijproman.2018.12.005

Bradshaw, C. (1963). Joint Ventures in Japan. *Washington Law Review*, *38*(1), 58–104.

Buso, M., Dosi, C., & Moretto, M. (2021). Do exit options increase the value for money of public–private partnerships? *Journal of Economics & Management Strategy*, *30*(4), 721–742. https://doi.org/10.1111/jems.12440

Caperchione, E., Demirag, I., & Grossi, G. (2017). Public sector reforms and public private partnerships: Overview and research agenda. *Accounting Forum*, *41*(1), 1–7. https://doi.org/10.1016/j.accfor.2017.01.003

Chen, Ch., & Hubbard, M. (2012). Power relations and risk allocation in the governance of public private partnerships: A case study from China. *Policy and Society*, *31*(1), 39–49. https://doi.org/10.1016/j.polsoc.2012.01.003

Chou, J.-Sh., & Lin, Ch. (2012). Predicting disputes in Public-Private Partnership projects: Classification and ensemble models. *Journal of Computing in Civil Engineering*, *27*(1). https://doi.org/10.1061/(ASCE)CP.1943-5487.0000197

Darko, D., Zhu, D., Quayson, M., Hossin, M. A., Omoruyi, O., & Bediako, A. K. (2023). A multicriteria decision framework for governance of PPP projects towards sustainable development. *Socio-Economic Planning Sciences*, *87*(B), 101580. https://doi.org/10.1016/j.seps.2023.101580

Demirag, I., Khadaroo, I., Stapleton, P., & Stevenson, C. (2011). Risks and the financing of PPP: Perspectives from the financiers. *The British Accounting Review*, *43*(4), 294–310. https://doi.org/10.1016/j.bar.2011.08.006

DoD NASA. (2020). *Proposed Rules. Federal Register*, *85*(109), 34561–34569.

Garg, S., & Garg, S. (2016). Rethinking Public-Private Partnerships: An unbundling approach. *Transportation Research Procedia* (Vol. 25, pp. 3789–3807). https://doi.org/10.1016/j.trpro.2017.05.241

González-Ruiz, Ju. D., Botero-Botero, S., & Duque-Grisales, E. (2018). Financial eco-innovation as a mechanism for fostering the development of sustainable infrastructure systems. *Sustainability*, *10*(12), 4463. https://doi.org/10.3390/su10124463

Hart, O. (2003). Incomplete contracts and public ownership: Remarks, and an application to public-private partnerships. *The Economic Journal*, *113*(486), C69–C76. https://doi.org/10.1111/1468-0297.00119

Hennessey, K. (2021). Comment on «When and how to use Public-Private Partnerships in infrastructure: Lessons from the international experience». In E. Glaeser, & J. Poterba (Eds.), *Economic Analysis and Infrastructure Investment* (pp. 365–368). Cambridge: National Bureau of Economic Research.

Hurk, M. van den, Brogaard, L., Lember, V., Petersen, O. H., & Witz, P. (2016). National varieties of Public-Private Partnerships (PPPs): A comparative analysis of PPP-supporting units in 19 European Countries. *Journal of Comparative Policy Analysis: Research and Practice*, *18*(1), 1–20. https://doi.org/10.1080/13876988.2015.1006814

Ito, S. (2020). *Infrastructure Development and Public-Private Partnership.* Singapore: Springer Nature Singapore Pte Ltd.

Jayachandran, S. (2021). *How economic development influences the environment*. Cambridge: National Bureau of Economic Research. https://doi.org/10.3386/w29191

Jin, Zh., & Huang, Ch. (2021). Tax enforcement and corporate donations: evidence from Chinese 'Golden Tax Phase III'. *China Journal of Accounting Studies*, *9*(4), 526–548. https://doi.org/10.1080/21697213.2022.2053375.

Jokar, E., Aminnejad, B., & Lork, A. (2021). Assessing and prioritizing risks in Public-Private Partnership (PPP) projects using the integration of fuzzy multi-criteria decision-making methods. *Operations Research Perspectives*, *8*, 100190. https://doi.org/10.1016/j.orp.2021.100190

Khallaf, R., Naderpajouh, N., & Hastak, M. (2021). Robust decision-making for multiparty renegotiations in Public-Private Partnerships. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *13*(3). https://doi.org/10.1061/(ASCE)LA.1943-4170.0000473

Kurniawan, F., Mudjanarko, S. W., & Ogunlana, S. O. (2015). Best practice for financial models of PPP projects. In *Procedia Engineering* (Vol. 125, pp. 124–132). https://doi.org/10.1016/j.proeng.2015.11.019

Lee, E. Y.-J. (2003). The Special Economic Zones and North Korean economic Reformation with a viewpoint of international law. *Fordham International Law Journal*, *27*(4), 1343–1378.

Leigland, J. (2018). Public-Private partnerships in developing countries: The emerging evidence-based critique. *The World Bank Research Observer*, *33*(1), 103–134. https://doi.org/10.1093/wbro/lkx008

Lemley, M., & McCreary, A. (2019, December 19). Exit strategy. *Stanford Law and Economics Olin Working Paper*, 542.

Liu, J., Gao, R., Cheah, Ch., & Luo, J. (2016). Incentive mechanism for inhibiting investors' opportunistic behavior in PPP projects. *International Journal of Project Management*, *34*(7), 1102–1111. https://doi.org/10.1016/j.ijproman.2016.05.013

Liu, J., Yu, X., & Cheah, Ch. Yu. J. (2014). Evaluation of restrictive competition in PPP projects using real option approach. *International Journal of Project Management*, *32*(3), 473–481. https://doi.org/10.1016/j.ijproman.2013.07.007

Liu, T., Wang, Y., & Wilkinson, S. (2016). Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public-Private Partnerships (PPPs): A comparative analysis of Australia and China. *International Journal of Project Management*, *34*(4), 701–716. https://doi.org/10.1016/j.ijproman.2016.01.004

Liyanapathirana, D., Adeniyi, O., & Rathnasiri, P. (2023). Tactical conflict prevention strategies in Public-Private Partnerships: Lessons from experts. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *16*(1). https://doi.org/10.1061/jladah.ladr-996

Ma, L., Hu, Ya., Zhu, L., & Ke, Y. (2023). Are public-private partnerships still an answer for social infrastructure? A systematic literature review. *Frontiers of Engineering Management*, *10*(3), 467–482. https://doi.org/10.1007/s42524-023-0249-1

Marques, R. C. (2021). Public interest and early termination of PPP contracts. Can fair and reasonable compensations be determined? *Utilities Policy*, *73*, 101301. https://doi.org/10.1016/j.jup.2021.101301

Mirzaee, A. M., & Sardroud, J. M. (2022). Public-private-partnerships /PPP enabled smart city funding and financing. In J. R. Vacca (Ed.), *Smart Cities Policies and Financing. Approaches and Solutions* (Chapter 9, pp. 117–131). https://doi.org/10.1016/B978-0-12-819130-9.00011-5

Moffatt, S., & Kohler, N. (2008). Conceptualizing the built environment as a social–ecological system. *Building Research & Information: Developing theories of the built environment*, *36*(3), 248–268. https://doi.org/10.1080/09613210801928131

Noring, L. (2019). Public asset corporation: A new vehicle for urban regeneration and infrastructure finance. *Cities*, *88*, 125–135. https://doi.org/10.1016/j.cities.2019.01.002

Ojelabi, L. A., & Noone, M. A. (2020). Jurisdictional perspectives on alternative dispute resolution and access to justice: introduction. *International Journal of Law in Context*, *16*(2), 103–107. https://doi.org/10.1017/S1744552320000087

Outhuijse, A. (2020). The effective public enforcement of the prohibition of anti-competitive agreements: Which factors influence the high percentage of annulments of Dutch cartel fines? *Journal of Antitrust Enforcement*, *8*(1), 124–164. https://doi.org/10.1093/jaenfo/jnz020

Owen, B., Sun, S., & Zheng, W. (2007). China's competition policy reforms: The anti-monopoly law and beyond. *Stanford Law and Economics Olin Working Paper*, *339*. https://doi.org/10.2139/ssrn.978810

Rossi, M., & Civitillo, R. (2014). Public Private Partnerships: A general overview in Italy. *Procedia-Social and Behavioral Sciences*, *109*, 140–149. https://doi.org/10.1016/j.sbspro.2013.12.434

Rufín, C., & Rivera-Santos, M. (2012). Between commonweal and competition: Understanding the governance of public-private partnerships. *Journal of Management*, *38*(5), 1634–1654. https://doi.org/10.1177/0149206310373948

Rybnicek, R., Plakolm, Ju., & Baumgartner, L. (2020). Risks in Public-Private Partnerships: A systematic literature review of risk factors, their impact and risk mitigation. *Public Performance & Management Review*, *43*(5), 1174–1208. https://doi.org/10.1080/15309576.2020.1741406

Salem, D. (1981). The Joint Venture Law of the Peoples' Republic of China: Business and Legal Perspective. *Maryland Journal of International Law*, *7*(1), 73–118

Selim, A., & ElGohary, A. S. (2020). Public-private partnerships (PPPs) in smart infrastructure projects: the role of stakeholders. *HBRC Journal*, *16*(1), 317–333. https://doi.org/10.1080/16874048.2020.1825038

Sharma, Ch. (2022). Who does it better and why? Empirical analysis of public-private partnership in infrastructure in Asia-Pacific. *Property Management*, *41*(3), 309–335. https://doi.org/10.1108/PM-07-2022-0050

Soomro, N.-E-H., & Yuhui, W. (2023). Appraisal of existing evidences of competition law and policy: Bilateral legislative developments of Sino-Pak. *Heliyon*, *9*(8). https://doi.org/10.1016/j.heliyon.2023.e18935

Wang, H., Liu, Yu., Xiong, W., & Zhu, D. (2019). Government support programs and private investments in PPP Markets. *International Public Management Journal*, *22*(3), 499–523. https://doi.org/10.1080/10967494.2018.1538025

Wang, Y. (2003). A broken fantasy of Public-Private Partnerships. *Public Administration Review*, *69*(4), 779–782. https://doi.org/10.1111/j.1540-6210.2009.02025.x

Wegrich, K., Kostka, G., & Hammerschmid, G. (Eds.) (2017). *The governance of infrastructure*: Hertie Governance Report. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198787310.001.0001

Whiteside, H. (2020). Public-private partnerships: market development through management reform. *Review of International Political Economy*, *27*(4), 880–902. https://doi.org/10.1080/09692290.2019.1635514

Yurdakul, H., Kamaşak, R., & Öztürk, T. Ya. (2022). Macroeconomic drivers of Public Private Partnership (PPP) projects in low income and developing countries: A panel data analysis. *Borsa Istanbul Review*, *22*(1), 37–46. https://doi.org/10.1016/j.bir.2021.01.002

Author information

Dominique T. Molintas – Researcher, PATTS College of Aeronautics; Graduate Student, Griffith Graduate Research School, Griffith University
Address: Nathan, QLD 4111, Queensland, Australia; Lombos Avenue, San Isidro 1700, Paranaque, Philippines
E-mail: dmolintas@asia.com
ORCID ID: https://orcid.org/0000-0002-4063-3983
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KHE-0949-2024
Google Scholar ID: https://scholar.google.com/citations?user=G8imOMYAAAAJ

Conflict of interest

The author 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 – January 16, 2024
Date of approval – February 12, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:347.4:004.4
EDN: https://elibrary.ru/lvpigr
DOI: https://doi.org/10.21202/jdtl.2024.22

Соглашение о государственно-частном партнерстве в контексте матрицы оценки их юридических параметров и цифровизации

Доминик Т. Молинтас

Колледж аэронавтики PATTS, Параньяк, Филиппины;
Университет Гриффита, Квинсленд, Австралия

Ключевые слова

государственно-частное партнерство,
контракт,
конфликт интересов,
ограничение конкуренции,
право,
соглашение,
управление рисками,
цифровые технологии,
цифровизация,
юридическая оценка

Аннотация

Цель: путем рассмотрения юридических аспектов соглашений о государственно-частном партнерстве синтезировать их основные положения в общую матрицу, которую при переводе в цифровой формат можно использовать в интересах стандартизации и упрощения формулирования параметров соглашения.

Методы: автор опирался на сравнительно-правовой анализ научной литературы, законодательства и интернет-источников по государственно-частному партнерству, дополненный рассмотрением соглашений о государственно-частном партнерстве различной социально-политической направленности, что позволило создать научно-обоснованную и практико-ориентированную матрицу, которая может послужить инструментом при составлении соглашений о государственно-частном партнерстве.

Результаты: выделены национальные аспекты в правовом регулировании обозначенных отношений в различных странах и описан ряд особенностей, встречающихся в соглашениях о государственно-частном партнерстве.

Научная новизна: с учетом важнейших правовых особенностей, характерных для разных стран, представлена матрица для составления соглашений о государственно-частном партнерстве, включающая восемь основных параметров: 1 – полученную стоимость, масштаб, выгоды и риски, 2 – выход на рынок, 3 – ограничение конкуренции, 4 – конфликт интересов/закупки, 5 – полномочия, одобрение, юридическая оценка, 6 – обязательства, разрешение споров, 7 – структуру собственности, управление и уровень автономии, 8 – стратегии выхода. В зависимости от обозначенных приоритетов ее можно модифицировать, учитывая, что приоритеты определяют и формируют конкретные параметры каждого отдельного партнерства.

Практическая значимость: полученная в результате исследования матричная схема может стать инструментом планирования, используемым для анализа и понимания взаимосвязей между восемью юридическими параметрами, необходимыми для формирования отношений в сфере государственно-частного партнерства. Она послужит юридическим ориентиром для формулирования соглашений о государственно-частном партнерстве, используемых во всем мире, и будет способствовать не только активизации государственно-частного партнерства, но и правильному пониманию обязательств, объемов ответственности и ограничений. Приведенные в исследовании рекомендации задают направление для оценки государственно-частного партнерства, позволяя сделать четкие выводы о партнерстве. При условии цифровой доступности предложенная матрица будет представлять определенный интерес для многих организаций, использующих государственно-частное партнерство в своей профессиональной деятельности.

Для цитирования

Молинтас, Д. Т. (2024). Соглашение о государственно-частном партнерстве в контексте матрицы оценки их юридических параметров и цифровизации. *Journal of Digital Technologies and Law*, *2*(2), 430–449. https://doi.org/10.21202/jdtl.2024.22

Список литературы

Azarian, M., Shiferaw, A. T., Lædre, O., Wondimu, P. A., & Stevik, T. K. (2023). Project ownership in public-private partnership (PPP) projects of Norway. *Procedia Computer Science*, *219*, 1838–1846. https://doi.org/10.1016/j.procs.2023.01.481

Biygautane, Mh., Neesham, C., & Al-Yahya, Kh. O. (2020). Institutional entrepreneurship and infrastructure public-private partnership (PPP): Unpacking the role of social actors in implementing PPP projects. *International Journal of Project Management*, *37*(1), 192–219. https://doi.org/10.1016/j.ijproman.2018.12.005

Bradshaw, C. (1963). Joint Ventures in Japan. *Washington Law Review*, *38*(1), 58–104.

Buso, M., Dosi, C., & Moretto, M. (2021). Do exit options increase the value for money of public–private partnerships? *Journal of Economics & Management Strategy*, *30*(4), 721–742. https://doi.org/10.1111/jems.12440

Caperchione, E., Demirag, I., & Grossi, G. (2017). Public sector reforms and public private partnerships: Overview and research agenda. *Accounting Forum*, *41*(1), 1–7. https://doi.org/10.1016/j.accfor.2017.01.003

Chen, Ch., & Hubbard, M. (2012). Power relations and risk allocation in the governance of public private partnerships: A case study from China. *Policy and Society*, *31*(1), 39–49. https://doi.org/10.1016/j.polsoc.2012.01.003

Chou, J.-Sh., & Lin, Ch. (2012). Predicting disputes in Public-Private Partnership projects: Classification and ensemble models. *Journal of Computing in Civil Engineering*, *27*(1). https://doi.org/10.1061/(ASCE)CP.1943-5487.0000197

Darko, D., Zhu, D., Quayson, M., Hossin, M. A., Omoruyi, O., & Bediako, A. K. (2023). A multicriteria decision framework for governance of PPP projects towards sustainable development. *Socio-Economic Planning Sciences*, *87*(B), 101580. https://doi.org/10.1016/j.seps.2023.101580

Demirag, I., Khadaroo, I., Stapleton, P., & Stevenson, C. (2011). Risks and the financing of PPP: Perspectives from the financiers. *The British Accounting Review*, *43*(4), 294–310. https://doi.org/10.1016/j.bar.2011.08.006

DoD NASA. (2020). *Proposed Rules. Federal Register*, *85*(109), 34561–34569.

Garg, S., & Garg, S. (2016). Rethinking Public-Private Partnerships: An unbundling approach. *Transportation Research Procedia* (Vol. 25, pp. 3789–3807). https://doi.org/10.1016/j.trpro.2017.05.241

González-Ruiz, Ju. D., Botero-Botero, S., & Duque-Grisales, E. (2018). Financial eco-innovation as a mechanism for fostering the development of sustainable infrastructure systems. *Sustainability*, *10*(12), 4463. https://doi.org/10.3390/su10124463

Hart, O. (2003). Incomplete contracts and public ownership: Remarks, and an application to public-private partnerships. *The Economic Journal*, *113*(486), C69–C76. https://doi.org/10.1111/1468-0297.00119

Hennessey, K. (2021). Comment on «When and how to use Public-Private Partnerships in infrastructure: Lessons from the international experience». In E. Glaeser, & J. Poterba (Eds.), *Economic Analysis and Infrastructure Investment* (pp. 365–368). Cambridge: National Bureau of Economic Research.

Hurk, M. van den, Brogaard, L., Lember, V., Petersen, O. H., & Witz, P. (2016). National varieties of Public-Private Partnerships (PPPs): A comparative analysis of PPP-supporting units in 19 European Countries. *Journal of Comparative Policy Analysis: Research and Practice*, *18*(1), 1–20. https://doi.org/10.1080/13876988.2015.1006814

Ito, S. (2020). *Infrastructure Development and Public-Private Partnership.* Singapore: Springer Nature Singapore Pte Ltd.

Jayachandran, S. (2021). *How economic development influences the environment*. Cambridge: National Bureau of Economic Research. https://doi.org/10.3386/w29191

Jin, Zh., & Huang, Ch. (2021). Tax enforcement and corporate donations: evidence from Chinese 'Golden Tax Phase III'. *China Journal of Accounting Studies*, *9*(4), 526–548. https://doi.org/10.1080/21697213.2022.2053375.

Jokar, E., Aminnejad, B., & Lork, A. (2021). Assessing and prioritizing risks in Public-Private Partnership (PPP) projects using the integration of fuzzy multi-criteria decision-making methods. *Operations Research Perspectives*, *8*, 100190. https://doi.org/10.1016/j.orp.2021.100190

Khallaf, R., Naderpajouh, N., & Hastak, M. (2021). Robust decision-making for multiparty renegotiations in Public-Private Partnerships. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *13*(3). https://doi.org/10.1061/(ASCE)LA.1943-4170.0000473

Kurniawan, F., Mudjanarko, S. W., & Ogunlana, S. O. (2015). Best practice for financial models of PPP projects. In *Procedia Engineering* (Vol. 125, pp. 124–132). https://doi.org/10.1016/j.proeng.2015.11.019

Lee, E. Y.-J. (2003). The Special Economic Zones and North Korean economic Reformation with a viewpoint of international law. *Fordham International Law Journal*, *27*(4), 1343–1378.

Leigland, J. (2018). Public-Private partnerships in developing countries: The emerging evidence-based critique. *The World Bank Research Observer*, *33*(1), 103–134. https://doi.org/10.1093/wbro/lkx008

Lemley, M., & McCreary, A. (2019, December 19). Exit strategy. *Stanford Law and Economics Olin Working Paper*, 542.

Liu, J., Gao, R., Cheah, Ch., & Luo, J. (2016). Incentive mechanism for inhibiting investors' opportunistic behavior in PPP projects. *International Journal of Project Management*, *34*(7), 1102–1111. https://doi.org/10.1016/j.ijproman.2016.05.013

Liu, J., Yu, X., & Cheah, Ch. Yu. J. (2014). Evaluation of restrictive competition in PPP projects using real option approach. *International Journal of Project Management*, *32*(3), 473–481. https://doi.org/10.1016/j.ijproman.2013.07.007

Liu, T., Wang, Y., & Wilkinson, S. (2016). Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public-Private Partnerships (PPPs): A comparative analysis of Australia and China. *International Journal of Project Management*, *34*(4), 701–716. https://doi.org/10.1016/j.ijproman.2016.01.004

Liyanapathirana, D., Adeniyi, O., & Rathnasiri, P. (2023). Tactical conflict prevention strategies in Public-Private Partnerships: Lessons from experts. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *16*(1). https://doi.org/10.1061/jladah.ladr-996

Ma, L., Hu, Ya., Zhu, L., & Ke, Y. (2023). Are public-private partnerships still an answer for social infrastructure? A systematic literature review. *Frontiers of Engineering Management*, *10*(3), 467–482. https://doi.org/10.1007/s42524-023-0249-1

Marques, R. C. (2021). Public interest and early termination of PPP contracts. Can fair and reasonable compensations be determined? *Utilities Policy*, *73*, 101301. https://doi.org/10.1016/j.jup.2021.101301

Mirzaee, A. M., & Sardroud, J. M. (2022). Public-private-partnerships /PPP enabled smart city funding and financing. In J. R. Vacca (Ed.), *Smart Cities Policies and Financing. Approaches and Solutions* (Chapter 9, pp. 117–131). https://doi.org/10.1016/B978-0-12-819130-9.00011-5

Moffatt, S., & Kohler, N. (2008). Conceptualizing the built environment as a social–ecological system. *Building Research & Information: Developing theories of the built environment*, *36*(3), 248–268. https://doi.org/10.1080/09613210801928131

Noring, L. (2019). Public asset corporation: A new vehicle for urban regeneration and infrastructure finance. *Cities*, *88*, 125–135. https://doi.org/10.1016/j.cities.2019.01.002

Ojelabi, L. A., & Noone, M. A. (2020). Jurisdictional perspectives on alternative dispute resolution and access to justice: introduction. *International Journal of Law in Context*, *16*(2), 103–107. https://doi.org/10.1017/S1744552320000087

Outhuijse, A. (2020). The effective public enforcement of the prohibition of anti-competitive agreements: Which factors influence the high percentage of annulments of Dutch cartel fines? *Journal of Antitrust Enforcement*, *8*(1), 124–164. https://doi.org/10.1093/jaenfo/jnz020

Owen, B., Sun, S., & Zheng, W. (2007). China's competition policy reforms: The anti-monopoly law and beyond. *Stanford Law and Economics Olin Working Paper*, *339*. https://doi.org/10.2139/ssrn.978810

Rossi, M., & Civitillo, R. (2014). Public Private Partnerships: A general overview in Italy. *Procedia-Social and Behavioral Sciences*, *109*, 140–149. https://doi.org/10.1016/j.sbspro.2013.12.434

Rufín, C., & Rivera-Santos, M. (2012). Between commonweal and competition: Understanding the governance of public-private partnerships. *Journal of Management*, *38*(5), 1634–1654. https://doi.org/10.1177/0149206310373948

Rybnicek, R., Plakolm, Ju., & Baumgartner, L. (2020). Risks in Public-Private Partnerships: A systematic literature review of risk factors, their impact and risk mitigation. *Public Performance & Management Review*, *43*(5), 1174–1208. https://doi.org/10.1080/15309576.2020.1741406

Salem, D. (1981). The Joint Venture Law of the Peoples' Republic of China: Business and Legal Perspective. *Maryland Journal of International Law*, *7*(1), 73–118

Selim, A., & ElGohary, A. S. (2020). Public-private partnerships (PPPs) in smart infrastructure projects: the role of stakeholders. *HBRC Journal*, *16*(1), 317–333. https://doi.org/10.1080/16874048.2020.1825038

Sharma, Ch. (2022). Who does it better and why? Empirical analysis of public-private partnership in infrastructure in Asia-Pacific. *Property Management*, *41*(3), 309–335. https://doi.org/10.1108/PM-07-2022-0050

Soomro, N.-E-H., & Yuhui, W. (2023). Appraisal of existing evidences of competition law and policy: Bilateral legislative developments of Sino-Pak. *Heliyon*, *9*(8). https://doi.org/10.1016/j.heliyon.2023.e18935

Wang, H., Liu, Yu., Xiong, W., & Zhu, D. (2019). Government support programs and private investments in PPP Markets. *International Public Management Journal*, *22*(3), 499–523. https://doi.org/10.1080/10967494.2018.1538025

Wang, Y. (2003). A broken fantasy of Public-Private Partnerships. *Public Administration Review*, *69*(4), 779–782. https://doi.org/10.1111/j.1540-6210.2009.02025.x

Wegrich, K., Kostka, G., & Hammerschmid, G. (Eds.) (2017). *The governance of infrastructure*: Hertie Governance Report. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198787310.001.0001

Whiteside, H. (2020). Public-private partnerships: market development through management reform. *Review of International Political Economy*, *27*(4), 880–902. https://doi.org/10.1080/09692290.2019.1635514

Yurdakul, H., Kamaşak, R., & Öztürk, T. Ya. (2022). Macroeconomic drivers of Public Private Partnership (PPP) projects in low income and developing countries: A panel data analysis. *Borsa Istanbul Review*, *22*(1), 37–46. https://doi.org/10.1016/j.bir.2021.01.002

Сведения об авторе

Молинтас Доминик Т. – научный сотрудник, Колледж аэронавтики PATTS; магистр, Университет Гриффита
Адрес: Филиппины, Параньяк, авеню Ломбос, Сан Исидро 1700; Австралия, Квинсленд, Натан, QLD 4111
E-mail: dmolintas@asia.com
ORCID ID: https://orcid.org/0000-0002-4063-3983
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KHE-0949-2024
Google Scholar ID: https://scholar.google.com/citations?user=G8imOMYAAAAJ

Конфликт интересов

Автор сообщает 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: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 16 января 2024 г.
Дата одобрения после рецензирования – 12 февраля 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:17:004.8
EDN: https://elibrary.ru/fsfsnq
DOI: https://doi.org/10.21202/jdtl.2024.23

Ethical and Legal Regulation of Using Artificial Intelligence in Morocco

Hamza Jabir ✉
Ibn Zohr University, Agadir, Morocco

Kamal Lagtati
Ibn Zohr University, Agadir, Morocco

Denis Pohe-Tokpa
University of Bordeaux, Pessac, France

Keywords

"hard law",
Moroccan legislation,
artificial intelligence,
moral values,
"soft law",
principle of technological reality,
legal regulation,
legal risks,
digital technologies,
ethical principle

Abstract

Objective: to explore and identify the issues and opportunities for the ethical and legal regulation of artificial intelligence by the example of digital transformation in Morocco.

Methods: the study was conducted using analytical and comparative approaches to address the emerging legal issues arising from the development of artificial intelligence. The traditional scientific method in law is based on legal analysis, which was applied to the study of legal texts, scientific literature, diagnosis of the condition of the study field at the national and international level. Along with this, the comparative approach in law was used, which made it possible to examine the Moroccan legislation comparison with that of other countries.

Results: the article presents a review of scientific literature on the legal and ethical issues of using artificial intelligence. Legal texts and decrees developed at national and international level, directly or indirectly linked to the use of artificial intelligence, were reviewed. Moroccan legislation was compared with that of other countries. The findings suggest that, in the absence of a specific legal framework for artificial intelligence systems, the adoption of ethical standards in the form of guidelines, best

✉ Corresponding author

practices and ethical charters is preferable. These mechanisms appear to be a viable alternative to legal regulation. In this sense, several initiatives were taken to promote "soft law", which aims to encourage appropriate behavior of technological agents.

Scientific novelty: the analysis of digital transformations in Morocco made it possible to present a comprehensive view on the role of ethical aspects and on the sufficiency of law to respond to the changes in the modern society, transformed by the development of artificial intelligence.

Practical significance: the study allows identifying ways to find a more flexible balance between "soft" and "hard" law in the regulation of relations, taking into account the technological reality. This should encourage the appropriate behavior of technological agents and positively affect the specificity of the current situation. Today, the "hard law" slowly recognizes and addresses the problems associated with the digital technologies' regulation and slowly takes into account the possible risks posed by artificial intelligence and the insufficiency of its regulation.

For citation

Jabir, H., Lagtati, K., & Pohe-Tokpa, D. (2024). Ethical and Legal Regulation of Using Artificial Intelligence in Morocco. *Journal of Digital Technologies and Law, 2*(2), 450–472. https://doi.org/10.21202/jdtl.2024.23

Contents

Introduction

In recent years, artificial intelligence has been at the heart of all concerns because of its intensive and varied use by a growing number of companies. It is a «computer system that works by trying to duplicate or imitate the principles of thinking, intelligence or, more simply, certain movements or gestures of the human being» (Bertrand & André, 2010). With the multiplication of the means of connection, the new capacities of collection and algorithmic

treatment of the data, the emergence of technologies related to Big Data, connected objects, algorithms, blockchain, and artificial intelligence is currently being observed. This multi-faceted digital phenomenon is bringing together different universes by adding the speed, intelligence and simultaneity of digital to the objects associated with these New Information and Communication Technologies (NICTs) (Soulez, 2018).

Indeed, artificial intelligence is developing at an extremely fast pace and companies find themselves more and more in a position where they must on the one hand acquire these technologies to remain competitive, but on the other hand, learn to master them, to avoid the various biases that can be harmful. Artificial intelligence holds great promises, but also strong fears of dangers and risks that need to be corrected, or even limited, in order to guarantee a deployment that complies with the legal framework, moral values and ethical principles and the common good.

According to United Nations Educational, Scientific and Cultural Organization (UNESCO), the risks linked to artificial intelligence are three fold[1]: the scarcity of work, which would be carried out by machines instead of human beings; the consequences for the autonomy of the individual, in particular for his or her freedom and security; the overtaking of humanity, which could disappear, in a dystopian scenario-catastrophic-to the benefit of more intelligent machines (Franchomme & Jazottes, 2021). Moreover, the use of artificial intelligence techniques has already created new challenges). It implies a transformation of society, which creates the need to rethink the ethical aspects, and to ensure that the law is sufficient to react to this change.

The multiple initiatives of regulation of artificial intelligence converge on the importance of ethics in this field, even with its weak impact on the functional perimeter of an artificial intelligence (Merabet, 2018). Ethical issues have only recently been taken into account because the law is slow to grasp the problems linked to digital technology and to legislate on them. It is first necessary to recognize the application of human rights to the digital world, before considering any real regulation. This can be facilitated by the fact that «soft law» ethical issues are considered globally and borders cannot be a real obstacle as is the case when it comes to setting up a «hard law» normative framework (Cath, 2018).

It is therefore becoming essential to integrate in the future ethical critiques around digital projects related to artificial intelligence (Cath, 2018). Several standards, charters and guidelines concerning algorithmic systems, transparency, privacy, confidentiality, impartiality and more generally the elaboration of ethical systems have been elaborated by professional associations, private companies and some international organizations (Bensamoun & Loiseau, 2017a).

Morocco is one of the first countries to align itself with UNESCO's recommendations on the ethics of artificial intelligence (Rochd et al., 2021). This is the first global normative instrument on this subject. This was announced by the Minister of National Education,

[1] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, adopted on the sidelines of the 41st session of the UNESCO General Conference held in November 2021 in Paris.

Preschool and Sport on the sidelines of the signing of an agreement with UNESCO as part of the CONFINTEA VII held in Marrakech in June 2022. The kingdom has officially implemented the recommendation of the United Nations Educational, Scientific and Cultural Organization on the ethics of artificial intelligence adopted on the sidelines of the 41st session of the General Conference of UNESCO held in November 2021 in Paris (Benhanou, 2017).

The functional perimeter of artificial intelligence in company's activity would be difficult to circumscribe in an exhaustive way, so much it widens every day. From now on, AI allows organizations to automate and optimize certain tasks in an increased way, thus playing a major role in the mutations of the activity, by inventing new forms and organization of work (Benhanou, 2017). Artificial intelligence is an integral part of daily life and will become even more integrated in the years to come. It therefore generates several challenges, but also opens new perspectives for individuals, organizations and structures. The use of artificial intelligence in everyday life raises many ethical questions closely linked to the law, as it is the guarantor of the protection of fundamental rights and is the only one able to limit or prohibit certain practices. For example, in terms of environmental damage, to take just one example, it has been estimated that by 2020 digital technologies will account for between 1.8 and 6.3% of global carbon dioxide emissions.

In light of the delicate nature of artificial intelligence, it is crucial to address its legal implications, ensuring accountability for all stakeholders involved and preventing potential abuses. The existence of a legal void regarding artificial intelligence cannot be tolerated. It seems, therefore, essential to reflect on the role of ethics in the establishment of a legal framework for the use of artificial intelligence within companies.

For the elaboration of this study, the standard methods recommended for the realization of a scientific work were adopted: the analysis of legal texts, scientific works, a diagnosis of the sector and its environment at the national and international level. In order to understand and master our field of study, we consulted various books and academic journals dealing with the legal and ethical issues of the use of artificial intelligence. In addition, we have undertaken a review of legal texts and directives planned at the national and international level having a direct or indirect link with the use of artificial intelligence as well as making a comparison between Moroccan legislation and comparative legislations. On the international level, we consulted the various directives and resolutions established by the various organizations or international authorities.

1. The Emergence of Artificial Intelligence: an Opportunity or a Threat?

Artificial intelligence has already started to change almost all areas of everyday life. Based on a process of imitation of human intelligence, which is based on the creation and application of algorithms. Artificial intelligence holds many promises and represents a huge opportunity for countries. On the other hand, the use of this technology has already created new challenges and raises concerns about the risks it poses to the functioning of organizations (1.2), the world of work and fundamental rights and freedoms (1.1).

1.1. Artificial Intelligence and the Protection of Fundamental Rights and Freedoms

It is true that Artificial Intelligence offers a growing opportunity to create new solutions to improve human life, strengthen health guarantees and the well-being of humanity (Soulez, 2018). These intelligent technologies contain risks for the exercise of fundamental rights and freedoms. It is in this sense that the commission of the European Council has stated that «the use of algorithmic systems with automated data collection, decision analysis, optimization or machine learning capabilities, may have negative consequences on the exercise, enjoyment and protection of all human rights and fundamental freedoms»[2].

The truth is that artificial intelligence allows to gather and process a vast set of data. These are collected through the use of applications (badges, geolocation, video surveillance ... etc.) and will be used for the establishment and payment of remuneration, management of employee work and leave, control of performance and discipline[3]. These different technologies used in the workplace are likely to affect the rights and freedoms of employees (Desbarats, 2020) and even the rights of candidates in a recruitment process organized by the company (Desbarats, 2020).

Since artificial intelligence relies on data in order to function, personal data is one of the «stronger» issues in artificial intelligence. The problem is that algorithms need a huge amount of data to process to make a decision. This situation can sometimes conflict with the principles of data collection and use set by Moroccan positive law. These are, in fact, the principles of data minimization and purpose limitation provided for by Law 09-08 on the protection of individuals with regard to the processing of personal data.

It is important to note that, the use of artificial intelligence applications has long been justified by the technological naturalness of these applications, as they allow to avoid any kind of prejudice and unconscious discrimination made by any human being. Artificial intelligence can therefore undermine the human values and principles on which the Universal Declaration of Human Rights is based. It can also lead to violations of fundamental rights and freedoms, such as freedom of expression and assembly, through the filtering and deletion of content: human dignity, discrimination based on gender, racial or ethnic origin, religion or belief and, as the case may be, the protection of personal data, respect for privacy or the right to an effective judicial remedy and a fair trial, as well as consumer protection.

It should also be noted that artificial intelligence has given rise to new issues and challenges in terms of ethics and data protection that normally need to be addressed through policy and careful design of solutions to achieve harmony and compliance with regulatory provisions. The data that will be processed is often personal and behavioral

---

2 Counsil of Europe. (2018, November 12). Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems. https://clck.ru/3B46zf

3 (Michaud, 2021); usages et régulations, conférence de l'université de Toulouse à titre de «l'année universitaire» 2019–2020.

and can be very sensitive data such as health information and biometrics, with potential privacy and ethical implications exacerbating the protection of personal information in a future enabled by artificial intelligence. Indeed, if personal data is the new Eldorado, its exploitation by hyper sophisticated and not ideologically disinterested algorithms risks leading to the constitution of new forms of slavery or at least, of remote control of collective and individual behaviors. (Barraud, 2019). This is a technological regulation that threatens the free will of each individual, the algorithms carry normative effects, formidable although rather imperceptible (Marique & Stronwel, 2017).

By harnessing the power of artificial intelligence, the integration of AI into the legal sphere can serve as a catalyst for social and technical progress, benefiting both legal professionals and litigants alike. «There is no doubt that certain applications of artificial intelligence currently being developed or experimented with, such as those aimed at improving legal research, can be very useful and make judicial work both faster and more efficient. It is necessary to advocate a use of artificial intelligence which is, at the service of the professionals of justice and in phase with their needs and on the other hand, respectful of the individual rights guaranteed by the universal declaration» (Boy, Racine, & Siiriaien, 2009). Far from being a simple instrument for improving the efficiency of judicial systems, artificial intelligence should reinforce and not diminish the guarantees of the rule of law as well as the quality of the public justice service.

1.2. Artificial Intelligence: a Tool for Companies

Technological progress transmits a different and new dynamism to the business environment progressively imposing various challenges to companies. During the industrial revolution, emerging technologies have significantly affected the way companies are organized and managed, resulting in their digital transformation and the optimization of operational models prioritizing IT resources to improve products and services, establish more cooperative next-generation partnerships, and react immediately to real customer expectations.

Indeed, artificial intelligence has made the working world and companies evaluate[4]. It is even evoked the quasi programmed disappearance of certain activities in many sectors (industry, banking, finance, trade... etc.) as well as, in some more or less tangible way, the robots come to «increase» the physical and cognitive potential of the man at work; in order to reduce the tediousness of the task, but also to assist him. With the emergence of artificial intelligence applications, a set of jobs are particularly likely to change and robots are gradually integrating into sensors whose operation uses artificial intelligence. The latter is increasingly enabling «soft» interactions between humans and robots. This revolution is

[4] N. Le Ru. (2016). l'effet de l'automatisation sur l'emploi: ce qu'on sait et ce qu'on ignore, France stratégie. La note d'analyse, n°49 juillet 2016: conseil d'orientations sur l'emploi, Automatisation, numérisation et emploi, t, 1, les impacts sur le volume, la structure et la localisation de l'emploi, janvier 2017.

both favorable for companies and employees, who can now interact in a much simpler way with the machine likely to assist them in difficult tasks (Zouinar, 2020). Collaborative robotics brings benefits to the company, improves productivity and flexibility, but can also participate in the improvement of working conditions by aiming at the reduction of disorders and ensuring a flexible coordination in the execution of tasks within the company[5].

Note that these applications equipped with artificial intelligence are specially designed to support remote and team work via new communication technologies, thus promoting mobility and telecommuting. They also allow a better communication within the company, a better level of professional and human relations by making more accessible the information concerning the life in company. These different tools of artificial intelligence allow new possibilities to blossom, to optimize the working time, to accomplish tasks by reducing the margin of error, as well as to relieve any possible stress (Marique & Stronwel, 2017). Nevertheless, the risk is just as great of witnessing the isolation of the worker, the invasion of his or her private life by omnipresent information flows, and relationships that have become exclusively digital to the detriment of the human being.

In Morocco, as is the case for a whole set of developing countries, the race to Big Data and algorithms is creating new horizons. Indeed, artificial intelligence is already very present in our lives, obviously through our smartphones, GPS, etc. and more and more our cars (Naim et al., 2021). The same is true in companies, where we often use many other tools such as automatic translation or chatbots[6] to respond to consumers on the Internet. As well, speech-to-text technology, which is an interdisciplinary part of artificial intelligence, can transform any audio content into written text. It allows companies to save time by avoiding the need to manually type on the keyboard. Artificial intelligence thus favors the development of a new generation of products and services, with reduced costs.

It is important to note that in Morocco, all sectors do not benefit from the same degree of maturity to accommodate this type of technology. We still cannot talk about artificial intelligence in Morocco, at least for the majority of companies (Ait El Bour & Lebzar, 2020). Today, companies are working on data, trying to collect it, digitize it, facilitate access to it and analyze it (Bouanba et al., 2022; Mohamed-Amine et al., 2024). This is the preliminary step for the implementation of an artificial intelligence system. Now, the sectors that lend themselves best to this technological evolution are banking, the stock market, insurance, telecom operators, and part of industry.

---

5 Atain-Kouadio, J. J., & Sghaier, A. (2017). Les robots et dispositifs d'assistance physique: état des lieux et enjeux pour la prévention. INRS, Note Scientifique et technique, NS 354. (In French).

6 It is a real personal assistant, and provides a quick and consistent response to thousands of tourists seeking information or service. The Chatbot offers a conversation with the customer that respects the culture and the brand image of the company or the person who uses it.

In the public sector, artificial intelligence represents an opportunity to improve public service. It will allow us to provide citizens with practical information, thus making their lives easier, modernizing the administration and public service. Artificial intelligence also improves participation in public life and stimulates economic development through better provision and circulation of information. It also allows the development of information technologies and the establishment of a digital economy, overcoming the reluctance that may exist within the administration and organizing an ecosystem to ensure the harmonious establishment of a knowledge society, where the various actors can make their contribution (Boubker, 2024).

Finally, the adoption of artificial intelligence technologies has a significant impact on the performance of the company, encourages its development and internalization, and improves its effectiveness and economic results. The artificial intelligence technology used is based on the techniques of machine learning, a mathematically modeled tool that allows self-learning algorithms. Management is increasingly investing in artificial intelligence technologies to automate business processes, improve day-to-day decision-making by company managers and make provisions more accurate.

2. Artificial Intelligence Regulation: a Moral and Legal Need

The increased development of artificial intelligence over the last few years and its possible deployment in all sectors and in almost all human activities have led to reflections on its legal framework. However, individuals continue to invent themselves in a deterritorialized world and the protection of digital rights and freedoms must be based on identified and clearly reaffirmed legal principles and on a wide range of regulatory tools.

Aware of its potential in the perspective of a post-covid economy, the States are however just as aware of its dangers. In addition, indeed, in every field of application (as wide as reason can conceive it), the use of artificial intelligence could raise the question, and question its ethical and legal character. Because of the complexity and diversity of the applications of artificial intelligence and their fickle and evolving nature, it is necessary to adopt flexible «soft law» instruments in the form of guidelines, ethical charters, codes of conduct and other ethical standards (2.1), before establishing a legal framework for the use of artificial intelligence (2.2).

2.1. An Ethical Framework for Artificial Intelligence

The relatively anarchic development of artificial intelligence has prompted actors to propose normative frameworks to limit the risks that this technology presents, while aiming to optimize its benefits. However, aware of the importance of norms, as well as of the need not to penalize themselves by establishing a corpus, the actors of artificial intelligence have called upon ethics to set rules for the development and use of artificial intelligence systems based on principles corresponding to specific interests. At the same time, international

public or private actors have become aware of the risks inherent in a standardization that is both disordered and biased, and have engaged in the race for standards at both the national and international levels (Thibout, 2019).

These dynamics have resulted in a multitude of normative and ethical codes, but with the absence of an international consensus on the establishment of common normative tools. The objective of these initiatives is to respond to an obvious and certain concern about the announced rise of artificial intelligence and its real or supposed dangers. The idea is that artificial intelligence should be, from conception to use, «ethically compatible», that is to say, in conformity with the humanistic values that are inherent to society. In other words, it is time to embody in texts in the form of charters, codes of ethics, good practice guides, guidelines, an ethic for the use of artificial intelligence applications (Jobin et al., 2019). In this sense, the implementation of artificial intelligence in society would require the development of flexible rules in the form of a flexible law, which involves the stakeholders in its construction (Bostrom & Yudkowsky, 2018).

Indeed, the idea of an ethics for artificial intelligence, aims that developers must respect human dignity and individual autonomy in the research and development of artificial intelligence systems, for example, they must take the necessary measures not to cause discrimination resulting from prejudices that would have been included in the training data of artificial intelligence systems. In the context of competition to the international stakes and risks of artificial intelligence, the initiatives of regulation of artificial intelligence are multiplying and agreeing on the importance of ethics in this field (Bufflier, 2020).

Ethics applied to artificial intelligence is in the process of being developed; there are certain international standards, but they have a soft law value. Ethics therefore has an original Soft Law logic, but it is progressively being articulated around Compliance.

At the international level, UNESCO adopted a recommendation on the ethics of artificial intelligence at its General Conference. The elaboration of this Recommendation was based on the preliminary study of the World Commission on Scientific Knowledge and Technology (COMEST) of UNESCO. This text constitutes the first international normative instrument on the ethics of AI in the form of a recommendation covering all areas of AI through the elaboration of key principles, and guiding the development and application of AI from a human-centered perspective. The text of the Recommendation states that UNESCO is «Also convinced that globally recognized ethical standards for AI technologies, which fully respect international law, in particular human rights law can play a key role in the development of AI-related norms worldwide[7]».

It is important to note that through this simple recommendation – characterized by a real lack of binding character – UNESCO inscribes Compliance mechanisms called «strategic mechanisms» of ethics where it encourages Member States to set up «strategic frameworks

[7] The Preamble of the UNESCO Recommendation on the Ethics of Artificial Intelligence.

or mechanisms» in order to assess the impact of artificial intelligence on human rights, the rule of law, democracy, ethics as well as due diligence tools by referring to the United Nations Guiding Principles on Business and Human Rights (Bostrom & Yudkowsky, 2018).

At the European level, it is since 2018, that the commission of the European Council has considered in a global way the artificial intelligence. With a desire to ensure an adequate ethical and legal framework in relation to the values of Article 2 of the Treaty on European Union and the Charter of Fundamental Rights of the European Union. To this end, the commission proposed the development of draft ethical guidelines in the field of artificial intelligence. These guidelines were published in 2019, and constitute the foundations of a trustworthy ethics, from which the ethical principles to which the professionals of artificial intelligence must strive to adhere are derived. There are four ethical principles: respect for human autonomy, prevention of harm, fairness and explicability.

In addition, the European Parliament adopted in 2017, a resolution containing «recommendations for civil law rules on robotics»[8] , In the appendix, «a charter on robotics» which is declined according to the addressees, in an ethical «code of conduct» for engineers in robotics, in a «code of ethics» for the committees of ethics and research, a «license» for the designers and another for the users. In this sense, the European Commission has also elaborated a text in the form of «A European ethical charter for the use of artificial intelligence in judicial systems and their environment» (Bensoussan & Bensoussan, 2019). It concerns the automated processing of judicial decisions and judicial data (by machine learning). The charter contains a whole set of principles that aim to address the ethical concerns of artificial intelligence. These principles focus on the respect of certain fundamental values, in particular the principle of non-discrimination and the right to privacy. Particular attention is also paid in the charter to security and transparency[9].

Conscious of the risks that artificial intelligence presents, Morocco, for its part, has taken several initiatives to accompany the digital transition that the world has known today. Morocco has established in 2011, a General Directorate of Information Systems Security (DGSSI), whose mission is to ensure the support and security of digital development. This authority has developed a strategy to accompany the proliferation of communication and information technologies. The strategy in question responds to the new challenges arising from the evolution of digital users and the threats linked to these technologies[10].

---

8 Resolution of February 16, 2017 with recommendations to the Commission on civil law rules on robotics (2015/2103(INL)), Liability, item AF.

9 The European Parliament adopted other resolutions in 2020: European Parliament resolution of October 20, 2020 with recommendations to the commission on a framework for ethical aspects of artificial intelligence and robotics and related technologies; European Parliament resolution of October 20, 2020 with recommendations to the commission on a civil liability regime for artificial intelligence. Voir, Y. Meneceur. (2019). Les enseignements des éthiques européennes de l'intelligence artificielle. JPC, 325, 552, 2.

10 General Directorate for Information Systems Security. Stratégie Nationale en matière de cyber sécurité. https://clck.ru/3B49Gf

The Moroccan authorities have also created in 2017, the Digital Development Agency in order to question the relationship of humans to digital and to structure the debate around this issue. This Agency prepares reports by organizing broad consultations that consist in inviting public and private actors, with a view to contributing to a more creative and innovative society, while building a new balance between economic and societal issues related to digital. Morocco, has also established with the publication of Law 09-08 on the protection of individuals with regard to the processing of personal data, a national commission to monitor the protection of personal data. It is responsible for ensuring the protection of personal data contained in computer files and treatments or paper, both public and private (Jaldi, 2022).

The reports established by these institutions constitute a reference framework for the regulation of the use of technology in Morocco (Ait El Bour & Lebzar, 2020). The latter has also aligned itself with the recommendations of UNESCO on the ethics of artificial intelligence. It remains to establish a commission, which will be responsible for questions of artificial intelligence and its challenges, which will certainly be inspired by the recommendations of UNESCO, and ethical charters and guidelines established by international bodies.

Private initiatives also play a key role in establishing an ethical framework for the use of artificial intelligence. They involve the major players in the digital economy. For example, the «Partnership on AI» collective [11], Founded by the major multinational companies, Google, Microsoft, Facebook[12], Amazon and Apple, to study and formulate best practices on artificial intelligence technologies, to advance public understanding of artificial intelligence, and to serve as an open platform for discussion and engagement around artificial intelligence and its impact on people and society (Bensamoun & Loiseau, 2017a).

The difficulty observed today is that, in practice, ethics applied to artificial intelligence is complex in its implementation. Indeed, a good number of companies, governments, associations, public and private sector actors are setting up good practice guides, recommendations or simply communicating on ethical and responsible artificial intelligence. However, it has been observed that these actors were struggling to implement these principles within their companies. In this sense, self-regulation by operators is a relevant solution, but only if it implies mandatory behaviors upstream, on the model of compliance or accountability (Cath, 2018)

2.2. The Need for a Legal Regime Adapted to Artificial Intelligence

Artificial intelligence has become a strategic issue in that it concerns almost all human activities. From finance to defense, through education, logistics, health and justice. It is gradually becoming essential in certain regions of the world and is tending to spread

[11] Partnership on AI (PAI). www.Partnershiponai.org

[12] The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation

to the entire globe. This has prompted the players involved to propose normative frameworks to limit the risks associated with this technology and optimize the benefits. However, the implementation of a legal framework that would strictly regulate the development and use of artificial intelligence systems poses several problems. First of all, it is not necessarily desired by certain stakeholders insofar as it could go against their interests, thus limiting their margin of action. Secondly, it requires a consensus based on a long diplomatic exercise and complex negotiations with the various public and private actors. The regulation in question must therefore leave as much space as possible for the development and use of algorithmic systems, which offer advantages for individuals and society. Thus, it must guarantee that the use of these systems does not harm the individuals concerned and society as a whole.

Furthermore, should the challenges created by artificial intelligence systems not be governed by a general «law of artificial intelligence» or by a «law of algorithms», a combination of general and sector-specific standards is much more appropriate. Indeed, we can see that it will probably be necessary to adapt the interpretation and application of existing standards in order to be able to meet the new challenges in an appropriate way.

It is particularly necessary to note that there is no specific regulation of artificial intelligence in Moroccan law, as is the case in most advanced countries. However, the use of artificial intelligence systems is associated with data processing. The law on the protection of personal data applies, as it concerns personal data. Thus, it appears in principle possible to solve challenges related to the protection of privacy and data protection with the means – of the existing data protection law (Jaldi, 2022). Then, the law 09-08 relative to the protection of the physical persons with regard to the treatment of the personal data finds its application, every time the systems of artificial intelligence involve the personal data and information.

Nevertheless, the use of artificial intelligence systems also leads to other issues. For example, the implementation of these systems is often not identifiable for the people concerned and their functioning is not understandable. Furthermore, such systems can lead to the discrimination of individuals and the manipulation of their actions. In addition, the implementation of artificial intelligence systems raises new issues of liability law. There is still a need for regulation in all of these areas, and this is the case for guaranteeing the safety of autonomous systems and certain authorization procedures.

It is clear that a legal framework for artificial intelligence systems, which does not disrupt the development of the technology, and which offers guarantees to potential victims, is of considerable importance. In this respect, some authors have gone so far as to propose the creation of an electronic personality, giving artificial intelligence systems a legal status. This concept of electronic personality was very quickly criticized, on the grounds that this solution could break down the boundaries between man and machine (Merabet, 2018). To this effect, we can see that it appears difficult to impute a legal responsibility to a machine, and the solution that would consist in creating a legal personality for the benefit of artificial intelligence systems is extravagant and must be fought. Such a solution could limit the solvency of the «robot debtor» and make its manufacturers less responsible (Bensamoun & Loiseau, 2017b).

On the other hand, it seems reasonable and judicious to impute the effects of the responsibility to the designer, the manufacturer, the owner, and the user of the artificial intelligence, who are hidden behind the machines. Let us note, that one of the difficulties in the field of artificial intelligence, is that many actors are likely to intervene[13]. The responsibilities can thus be found at the level of the choice of the learning data, their collection, their organization, the design of the algorithms, the realization of the software, the interface and even the hardware part (Courtois, 2016). Other actors can disrupt the functioning of the systems, whether it is a malicious user or even a third party acting in bad faith. It seems that several of these actors may have a share of responsibility, or even that the different responsibilities may be jointly and severally committed.

Today, intelligent machines are endowed with the ability to make decisions autonomously and outside the effective control of the person. This makes inapplicable the traditional rules of the responsibility for the things as, it is foreseen in the article 88 of Moroccan code of the obligations and contracts[14]. For even if the human being can keep custody of the thing endowed with artificial intelligence, it can escape from him because of the difficulty to control it effectively. Moreover, in this regime, it is difficult for potential victims to establish whether the custodian was the designer or the user of the artificial intelligence. If, for example, the user has technological skills, he can modify the source code of the artificial intelligence, which will induce a change in its behavior. Moreover, he can choose the parameters of its functioning by altering its behavior. Such a scenario makes it very difficult to identify the person with effective power over the thing. Considering all the aforementioned concerns, establishing whether the harm resulted from the structure or the behavior of artificial intelligence becomes challenging, giving rise to the issue of proof in this hypothesis.

Indeed, the majority of the doctrine has noted that the responsibility for things is not entirely adapted to the autonomous fact of artificial intelligence (Shushanik, 2019). To this end, other no-fault liability regimes can be adapted to the autonomous nature of artificial intelligence. This is the case of product liability, which may appear to be an effective regime for dealing with the most autonomous artificial intelligence systems (Courtois, 2016). The notions of product and defect are compatible with the immaterial and autonomous character of these systems. It constitutes a mechanism of responsibility of full right, as, it is envisaged in article 106 paragraphs 1 of the Moroccan code of the

[13] The plurality of participants in the use or programming of the machine overturns the traditional rules of civil liability: a fault, a damage and the causal link.

[14] Article 88 of the Code of Obligations and Contracts (DOC) stipulates that "individuals are liable for the harm caused by the objects under their control, provided that these objects directly caused the damage, unless they can demonstrate: 1) taking all necessary precautions to prevent the harm, and 2) that the harm resulted from either an unforeseen event, an irresistible force, or the fault of the victim".

obligations and contracts «The producer is responsible for the damage caused by a defect of its product»[15].

In reality, intelligent machines are not ordinary products and it will be necessary to take into account, in particular for the determination of the origin of the defect, the complex character of the good by integrating intangible and, if necessary, tangible elements and whose production involves various participants, from the «manufacturer» of the robot to the designers of algorithms and programs. The broad conception of producer, whether it is the manufacturer of the finished product or the manufacturer of the component part of the system, the joint and several liability of both provide for the treatment of the liability without the need for other rules (Courtois, 2016). The question that arises is in which case the producer can benefit from a cause of exoneration of responsibility. The answer is provided for in Article 106-9 of the Code of Obligations and Contracts: «The producer is not liable if he proves that the defect which caused the damage did not exist at the time the product was put into circulation or that this defect arose afterwards". According to this article, the producer cannot be held liable if, taking into account the circumstances, there is reason to believe that the defect which caused the damage did not exist at the time the product was put into circulation by him or that this defect arose afterwards.

However, artificial intelligence systems can challenge the traditional rules of release. In some cases, the role of the producer is not limited to putting the product into circulation. Sometimes the software is updated to ensure its proper functioning and adaptation to the environment. In addition, the producer may provide new data that will be processed by the stand-alone software. Here, the issue is to know if it is possible to consider the engagement of the producer's responsibility in the presented hypotheses. To this end, we can see that if the producer retains control over the system produced for the subsequent addition of updates, he should be responsible for the defects of this system, even if these defects appear after the release of this product. Finally, it should be noted that this liability regime seems to be adapted to artificial intelligence systems, but its application in this field is still uncertain, in the absence of identified jurisprudence, and the question of the articulation of these different liability regimes may be a real challenge.

Conclusions

Artificial intelligence and the extent of its development has created new economic, social, and ethical challenges. The law is not the exception. However, even if artificial intelligence helps companies to adapt and master an increasingly dynamic business environment, it presents

[15] The term «product» refers to any product made available on the market in the context of a professional, commercial or artisanal activity, whether in return for payment or free of charge, whether new or used, whether or not it has been processed or packaged, even if it is incorporated into another item of furniture or into a building. Electricity is considered a product. See article 106-2 of the Moroccan code of obligations and contracts.

risks to the exercise of fundamental rights and freedoms. It is therefore necessary to find a balance between the use of artificial intelligence for business and human development and the protection of fundamental rights and freedoms.

Technology and the use that is made of it, a fortiori in the XXth century through the Internet, is transborder and calls into question a good number of legal borders, national laws and even international law. However, to remain effective, the law must integrate «the principle of technological reality», which is a factor of differentiation and complexity of the norm and apply it to artificial intelligence. The problem of choosing the regulations applicable to artificial intelligence is a real one, because artificial intelligence is at the crossroads of several so-called advanced sectors.

In the absence of a specific legal framework for artificial intelligence, ethics naturally imposes itself as a palliative solution to the choice, abstruse for the majority, of flexible law, easy to apply to artificial intelligence, non-binding; ethics proves to be a comfortable tool to use instead of law. The legal framework of artificial intelligence systems requires the crossing of many general or special legal disciplines, thus creating new, transversal relationships, so that the law can apprehend the specificity of these new actors and fulfill its normative and regulatory functions.

References

Ait El Bour, D., & Lebzar, B. (2020). L'intelligence artificielle face aux entreprises marocaines, quels défis? *Revue Internationale d'Economie Numérique*, *2*(1). (In French).

Al-Ajmi, F. (2011). *Civil Protection for the Consumer in the Electronic Contract*. (Unpublished Master dissertation). University of the Middle East.

Barraud. (2019). Le droit en datas: comment l'intelligence artificielle redessine le monde juridique. *Revue Lamy droit de l'immatériel*, *164*. (In French).

Benhanou, S. (2017). *Imaginer l'avenir de travail – Quatre types d'organisations à l'horizon 2030*, France Stratégie, Document de travail n°2017-05. (In French).

Bensamoun, A., & Loiseau, G. (2017a). La gestion des risques de l'intelligence artificielle – de l'éthique à la responsabilité. *La Semaine juridique*, *12*. (In French).

Bensamoun, A., & Loiseau, G. (2017b). *L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun: questions de temps*. Dalloz IP/IT, 239. (In French).

Bensoussan, A., &, Bensoussan, J. (2019). *IA, robots et droit*. Bruxelles: Bruylant. (In French).

Bertrand, André R. (2010). C*onditions de la protection par le droit d'auteur. Deux cas particuliers: intelligence artificielle et réalité virtuelle*, Dalloz, 103.27. (In French).

Bostrom, N., & Yudkowsky, E. (2018). The Ethics of Artificial Intelligence. In *Artificial Intelligence Safety and Security* (pp. 57–69). Chapman and Hall/CRC. https://doi.org/10.1201/9781351251389-4

Bouanba, N., Barakat, O., & Bendou, A. (2022). Artificial Intelligence & Agile Innovation: Case of Moroccan Logistics Companies. *Procedia Computer Science*, *203*, 444–449. https://doi.org/10.1016/j.procs.2022.07.059

Boubker, O. (2024). From chatting to self-educating: Can AI tools boost student learning outcomes? Expert *Systems with Applications*, *238*(A), 121820–121820. https://doi.org/10.1016/j.eswa.2023.121820

Boy, L., Racine, J.-B., & Siiriaien, F. (2009). *Droit économique et Droit de l'homme*. Bruxelles, Larcier. (In French).

Bufflier, I. (2020). Intelligence artificielle et éthique d'entreprise. *Cahiers de droit de l'entreprise*, *3*, dossier 19, 45. (In French).

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080.

Courtois, G. (2016). *Robots intelligents et responsabilité : quels régimes, quelles perspectives*. Dalloz IP/IT, 287. (In French).
Desbarats, I. (2020). Quelle protection sociale pour les travailleurs des plateformes? *Revue de droit du travail*, *10*, 592–601. (In French).
Franchomme, M.-P., & Jazottes, G. (2021). Le défi d'une IA inclusive et responsable. *Droit social*, *2*, 100–108. (In French).
Jacquemin, H., & de Streel, A. (2017). *L'Intelligence artificielle et le droit*, Bruxelles, Larcier. (In French).
Jaldi, A. S. (2022). l'intelligence artificielle au Maroc: entre encadrement réglementaire et stratégie économique. *Policy Centre for the New South*, PB-59/22. (In French).
Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature machine intelligence*, *1*(9), 389–399.
Marique, E., & Stronwel, A. (2017). *Gouverner par la loi ou les algorithmes: de la norme générale de comportement au guidage rapproché des conduites*. Dalloz IP/IT, 10, 517. (In French).
Merabet, S. (2018). *Vers un droit de l'intelligence artificielle: thèse pour le doctorat en droit privé*. Université d'Aix-Marseille. (In French).
Michaud, O. (2021). La protection des travailleurs à l'heure de l'intelligence artificielle. *Dossier droit social, 2*, Fév., 124–132. (In French).
Mohamed-Amine, N., Abdellatif, M., & Belaid, B. (2024). Artificial intelligence for forecasting sales of agricultural products: A case study of a moroccan agricultural company. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(1), 100189. https://doi.org/10.1016/j.joitmc.2023.100189
Naim, A., Aaroud, A., Akodadi, K., & El Hachimi, C. (2021). A fully AI-based system to automate water meter data collection in Morocco country. *Array*, *10*, 100056. https://doi.org/10.1016/j.array.2021.100056
Rochd, A., Benazzouz, A., Ait Abdelmoula, I., Raihani, A., Ghennioui, A., Naimi, Z., & Ikken, B. (2021). Design and implementation of an AI-based & IoT-enabled Home Energy Management System: A case study in Benguerir – Morocco. *Energy Reports*, *7*, 699–719. https://doi.org/10.1016/j.egyr.2021.07.084
Shushanik, G. (2019). *Les problèmes de la réparation du dommage pour les produits et services défectueux dans la législation civile: thèse pour le doctorat en droit privé*. l'UEE. (In French).
Soulez, M. (2018). Questions juridiques au sujet de l'IA. *Enjeux numériques*, *1*, 83. (In French).
Thibout, Ch. (2019). La compétition mondiale de l'intelligence artificielle. Pouvoirs – *Revue française d'études constitutionnelles et politiques*, 170, 131–142. (In French).
Vassileva-Hadjitchoneva, J. (2020). L'IA au service de la prise de décisions plus efficace. *Pour une recherche économique efficace: 61° Congrès International AIELF*. Santiago, Chili. (In French).
Zouinar, M. (2020). Evolutions de l'intelligence artificielle: Quels enjeux pour l'activité humaine et la relation humain-machine au travail? *Activités*, 17-1. (In French). https://doi.org/10.4000/activites.4941

Authors information

Hamza Jabir – PhD Student in Private Law, Legal Sciences and Sustainable Development Research Laboratory, Faculty of Law, Economics, and Social Sciences, Ibn Zohr University
E-mail: hamza.jabir@edu.uiz.ac.ma
ORCID ID: https://orcid.org/0000-0003-3534-8982
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HMP-6781-2023
Google Scholar ID: https://scholar.google.com/citations?user=Lka-pbUAAAAJ

Kamal Lagtati – Research Professor, HDR in Private Law, Legal Sciences and Sustainable Development Research Laboratory, Faculty of Law, Economics, and Social Sciences, Ibn Zohr University; Member of the Centre Michel de l'hospital Université de Clermont Auvergne (EA 4232).
Address: BP 32/S, Riad Salam, CP 80000, Agadir, Morocco
E-mail: k.lagtati@uiz.ac.ma
ORCID ID: https://orcid.org/0009-0004-9198-2712
Google Scholar ID: https://scholar.google.com/citations?user=W-X93ewAAAAJ

Denis Pohe-Tokpa – Research Professor, HDR in Private Law, Faculty of Law and Political Science, University of Bordeaux
Address: 16 Avenue Léon Duguit, 33608 Pessac, France
E-mail: denis.pohe-tokpa@u-bordeaux.fr
ORCID ID: https://orcid.org/0009-0007-2678-1430

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 – December 14, 2023
Date of approval – January 12, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:17:004.8
EDN: https://elibrary.ru/fsfsnq
DOI: https://doi.org/10.21202/jdtl.2024.23

Этическое и правовое регулирование использования искусственного интеллекта в Марокко

Хамза Джабир ✉
Университет Ибн Зохр, Агадир, Марокко

Камаль Лагтати
Университет Ибн Зохр, Агадир, Марокко

Денис Поэ-Токпа
Университет Бордо, Пессак, Франция

Ключевые слова

«жесткое право», законодательство Марокко, искусственный интеллект, моральные ценности, «мягкое право», принцип технологической реальности, правовое регулирование, правовые риски, цифровые технологии, этические принципы

Аннотация

Цель: поиск и определение проблем и возможностей этического и правового регулирования искусственного интеллекта на примере опыта цифровых преобразований в Марокко.

Методы: исследование проведено с использованием аналитического и сравнительного подходов к решению возникающих юридических вопросов, обусловленных развитием искусственного интеллекта. За основу традиционного научного метода в праве взят правовой анализ, который применялся к изучению юридических текстов, научной литературы, диагностике состояний и условий изучаемой области на национальном и международном уровне. Наряду с этим использовался сравнительный подход в праве, позволивший рассмотреть законодательство Марокко в сопоставлении с законодательством других стран.

Результаты: осуществлен обзор научной литературы, посвященной правовым и этическим вопросам использования искусственного интеллекта. Проведен обзор юридических текстов и директив, разработанных на национальном и международном уровне и имеющих прямую или косвенную связь с использованием искусственного интеллекта. Приводится сравнение законодательства Марокко с соответствующими правовыми актами других стран. Полученные выводы свидетельствуют о том, что в отсутствие специальной правовой базы для систем искусственного интеллекта предпочтительным является

✉ Контактное лицо

принятие этических стандартов в виде руководящих принципов, руководства по передовой практике и этических хартий. Эти механизмы представляются жизнеспособной альтернативой правовому регулированию. В этом смысле было предпринято несколько инициатив по продвижению «мягкого права», которое направлено на поощрение надлежащего поведения технологических агентов.

Научная новизна: анализ цифровых преобразований в Марокко позволил представить комплексный взгляд на роль этических аспектов и обеспечение достаточности закона для реагирования на изменения современного общества, трансформирующегося в свете развития искусственного интеллекта.

Практическая значимость: проведенное исследование позволяет обозначить пути поиска более гибкого баланса между «мягким» и «жестким» правом в регулировании отношений с учетом технологической реальности, что должно поощрять надлежащее поведение технологических агентов и положительно влиять на специфику современной ситуации, когда «жесткое право» медленно осознает и решает проблемы, связанные с регулированием цифровых технологий, а также медленно учитывает возможные риски, которые несет в себе искусственный интеллект и недостаточность регулирования связанных с ним отношений.

Для цитирования

Джабир, Х., Лагтати, К., Поэ-Токпа, Д. (2024). Этическое и правовое регулирование использования искусственного интеллекта в Марокко. *Journal of Digital Technologies and Law*, *2*(2), 450–472. https://doi.org/10.21202/jdtl.2024.23

Список литературы

Ait El Bour, D., & Lebzar, B. (2020). L'intelligence artificielle face aux entreprises marocaines, quels défis? *Revue Internationale d'Economie Numérique, 2*(1). (In French).

Al-Ajmi, F. (2011). *Civil Protection for the Consumer in the Electronic Contract*. (Unpublished Master dissertation). University of the Middle East.

Barraud. (2019). Le droit en datas: comment l'intelligence artificielle redessine le monde juridique. *Revue Lamy droit de l'immatériel*, *164*. (In French).

Benhanou, S. (2017). *Imaginer l'avenir de travail – Quatre types d'organisations à l'horizon 2030*, France Stratégie, Document de travail n°2017-05. (In French).

Bensamoun, A., & Loiseau, G. (2017a). La gestion des risques de l'intelligence artificielle – de l'éthique à la responsabilité. *La Semaine juridique*, *12*. (In French).

Bensamoun, A., & Loiseau, G. (2017b). *L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun: questions de temps*. Dalloz IP/IT, 239. (In French).

Bensoussan, A., &, Bensoussan, J. (2019). *IA, robots et droit*. Bruxelles: Bruylant. (In French).

Bertrand, André R. (2010). *Conditions de la protection par le droit d'auteur. Deux cas particuliers: intelligence artificielle et réalité virtuelle*, Dalloz, 103.27. (In French).

Bostrom, N., & Yudkowsky, E. (2018). The Ethics of Artificial Intelligence. In *Artificial Intelligence Safety and Security* (pp. 57–69). Chapman and Hall/CRC. https://doi.org/10.1201/9781351251389-4

Bouanba, N., Barakat, O., & Bendou, A. (2022). Artificial Intelligence & Agile Innovation: Case of Moroccan Logistics Companies. *Procedia Computer Science*, *203*, 444–449. https://doi.org/10.1016/j.procs.2022.07.059

Boubker, O. (2024). From chatting to self-educating: Can AI tools boost student learning outcomes? *Expert Systems with Applications*, *238*(A), 121820–121820. https://doi.org/10.1016/j.eswa.2023.121820

Boy, L., Racine, J.-B., & Siiriaien, F. (2009). *Droit économique et Droit de l'homme*. Bruxelles, Larcier. (In French).

Bufflier, I. (2020). Intelligence artificielle et éthique d'entreprise. *Cahiers de droit de l'entreprise*, *3*, dossier 19, 45. (In French).

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080.

Courtois, G. (2016). *Robots intelligents et responsabilité : quels régimes, quelles perspectives*. Dalloz IP/IT, 287. (In French).

Desbarats, I. (2020). Quelle protection sociale pour les travailleurs des plateformes? *Revue de droit du travail*, *10*, 592–601. (In French).

Franchomme, M.-P., & Jazottes, G. (2021). Le défi d'une IA inclusive et responsable. *Droit social*, *2*, 100–108. (In French).

Jacquemin, H., & de Streel, A. (2017). *L'Intelligence artificielle et le droit*, Bruxelles, Larcier. (In French).

Jaldi, A. S. (2022). l'intelligence artificielle au Maroc: entre encadrement réglementaire et stratégie économique. *Policy Centre for the New South*, PB-59/22. (In French).

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature machine intelligence*, 1(9), 389–399.

Marique, E., & Stronwel, A. (2017). *Gouverner par la loi ou les algorithmes: de la norme générale de comportement au guidage rapproché des conduites*. Dalloz IP/IT, 10, 517. (In French).

Merabet, S. (2018). *Vers un droit de l'intelligence artificielle: thèse pour le doctorat en droit privé*. Université d'Aix-Marseille. (In French).

Michaud, O. (2021). La protection des travailleurs à l'heure de l'intelligence artificielle. *Dossier droit social*, *2*, Fév., 124–132. (In French).

Mohamed-Amine, N., Abdellatif, M., & Belaid, B. (2024). Artificial intelligence for forecasting sales of agricultural products: A case study of a moroccan agricultural company. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(1), 100189. https://doi.org/10.1016/j.joitmc.2023.100189

Naim, A., Aaroud, A., Akodadi, K., & El Hachimi, C. (2021). A fully AI-based system to automate water meter data collection in Morocco country. *Array*, *10*, 100056. https://doi.org/10.1016/j.array.2021.100056

Rochd, A., Benazzouz, A., Ait Abdelmoula, I., Raihani, A., Ghennioui, A., Naimi, Z., & Ikken, B. (2021). Design and implementation of an AI-based & IoT-enabled Home Energy Management System: A case study in Benguerir – Morocco. *Energy Reports*, *7*, 699–719. https://doi.org/10.1016/j.egyr.2021.07.084

Shushanik, G. (2019). *Les problèmes de la réparation du dommage pour les produits et services défectueux dans la législation civile: thèse pour le doctorat en droit privé*. l'UEE. (In French).

Soulez, M. (2018). Questions juridiques au sujet de l'IA. *Enjeux numériques*, *1*, 83. (In French).

Thibout, Ch. (2019). La compétition mondiale de l'intelligence artificielle. *Pouvoirs – Revue française d'études constitutionnelles et politiques*, *170*, 131–142. (In French).

Vassileva-Hadjitchoneva, J. (2020). L'IA au service de la prise de décisions plus efficace. *Pour une recherche économique efficace: 61° Congrès International AIELF*. Santiago, Chili. (In French).

Zouinar, M. (2020). Evolutions de l'intelligence artificielle: Quels enjeux pour l'activité humaine et la relation humain-machine au travail? *Activités*, 17-1. (In French). https://doi.org/10.4000/activites.4941

Сведения об авторах

Джабир Хамза – соискатель степени PhD; исследовательская лаборатория частного права, юридических наук и устойчивого развития; факультет права, экономики и общественных наук; Университет Ибн Зохр
Адрес: Марокко, Агадир, BP 32/S, Риад Салам, CP 80000
E-mail: hamza.jabir@edu.uiz.ac.ma
ORCID ID: https://orcid.org/0000-0003-3534-8982
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HMP-6781-2023
Google Scholar ID: https://scholar.google.com/citations?user=Lka-pbUAAAAJ

Лагтати Камаль – профессор-исследователь, почетный доктор, исследовательская лаборатория частного права, юридических наук и устойчивого развития; факультет права, экономики и общественных наук; Университет Ибн Зохр; член Центра Мишель де л'госпиталь, Университет Клермон-Овернь (EA 4232).
Адрес: Марокко, Агадир, BP 32/S, Риад Салам, CP 80000
E-mail: k.lagtati@uiz.ac.ma
ORCID ID: https://orcid.org/0009-0004-9198-2712
Google Scholar ID: https://scholar.google.com/citations?user=W-X93ewAAAAJ

Поэ-Токпа Денис – профессор-исследователь, почетный доктор частного права, факультет права и политологии, Университет Бордо
Адрес: Франция, Пессак, 33608, авеню Леона Дюгуи, 16
E-mail: denis.pohe-tokpa@u-bordeaux.fr
ORCID ID: https://orcid.org/0009-0007-2678-1430

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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 14 декабря 2023 г.
Дата одобрения после рецензирования – 12 января 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:17:004.8
EDN: https://elibrary.ru/fhsfeo
DOI: https://doi.org/10.21202/jdtl.2024.24

From the Theory of the African Origin of Humankind to Modern Social, Legal and Technological Innovations: a Brief Analytical Excursion into Anthroposociogenesis

Djeneba Traore

University of Arts and Humanities of Bamako, Bamako, Mali
West Africa Institute, Praia, Cabo Verde

Keywords

anthropogenesis,
artificial intelligence,
social transformations,
law,
industrial revolution,
social justice,
sociogenesis,
technological revolution,
digital technologies,
evolution of a human being

Abstract

Objective: to trace the evolution of humanity and to identify the role of various social institutions in order to understand the existential role of laws aimed at ensuring the coexistence of society in the context of technological innovations.

Methods: the author used general scientific and special methods of cognition, which allowed tracing the dialectical development of humanity, social transformations and technological innovations.

Results: looking back at the history of humanity, which originated on the African continent (the theory of African descent), the author notes the most important changes in the human way of life and environment, which led to the need to build organized societies and regulate social behavior with the help of legislative norms. Law is seen as part of the evolutionary process that was to emerge in the course of human evolution. The critical importance of law in overcoming the global challenges and existential questions of humanity's continued coexistence arising in the course of evolution is emphasized. In this regard, the historical significance of the Kurukan Fuga Charter of the Malian Empire is emphasized as one of the oldest constitutions in the world, recognized internationally as an important source of legal and political norms for modern societies, regulating the structure of state power and social behaviour, although preserved largely in oral form. It is argued that social and technological change often served as the impetus for the development

of new laws. Humanity has many times intervened in its own biological evolution with the help of technology; now it is an important moment from the viewpoint of law and ethics when technology may interfere in further human evolution. The greatest concern in this regard is the era of rapid development of artificial intelligence, which makes new demands on a human being.

Scientific novelty: the article shows the role of the African continent in the origin and development of humanity and socio-legal institutions in the light of modern transformations and the construction of a new social reality.

Practical significance: the conducted research creates prerequisites for further development of the theory of anthroposociogenesis and in-depth conceptual historical and legal study of the role of the African continent in the development of humanity and its social institutions.

For citation

Traore, D. (2024). From the Theory of the African Origin of Humankind to Modern Social, Legal and Technological Innovations: a Brief Analytical Excursion into Anthroposociogenesis. *Journal of Digital Technologies and Law, 2*(2), 473–486. https://doi.org/10.21202/jdtl.2024.24

Contents

Introduction

From the very beginning, humanity has been governed by oral or written laws. We must go back through history to understand how profound social transformations initially conveyed by progressive ideologies led to changes in lifestyles that were necessary to regulate through legislative texts and regulations.

Since the creation of the planet Earth, mainly three forms of life have appeared: plant life, animal life and human life which detached itself from the animal form through the development of cognitive intelligence, speech, standing and the ability to make tools to domesticate nature.

In prehistorical societies, the human species, which became bipedal, began to communicate. Communication allowed a form of social organization that made it possible to live together and respect certain rules established for this purpose.

It should be noticed that rules also exist in the animal kingdom and, surprisingly as it may seem, in the plant kingdom.

1. Evolution of a human being in the context of technological innovations and social-legal transformations: a historical excursion

According to scientists, there have been seven stages of human evolution[1], notably:

– Dryopithecus (Dryopithecine) ... ;
– Ramapithecus (Syn: Sivapithecus) ... ;
– Australopithecus (Southern Apes) ... ;
– Homo Habilis (Able Man) ... ;
– Homo Erectus (Upright Man) ... ;
– Homo Sapiens Neanderthalensis (New Human Species) ... ;
– Homo Sapiens (Wise Men).

On evidence based archeological discoveries, it is now proved that the African continent issued mankind: "According to the recent African origin of modern human theory, modern humans evolved in Africa possibly from H. heidelbergensis, H. rhodesiensis or H. antecessor and migrated out of the continent some 50,000 to 100,000 years ago, gradually replacing local populations of H. erectus, Denisova hominins, H. floresiensis, ..."[2].

What is the process of evolution of mankind?

"Human evolution is the lengthy process of change by which[3] people originated from apelike ancestors. Scientific evidence shows that the physical and behavioral traits shared by all people originated from apelike ancestors and evolved over a period of approximately six million years"[4].

The different socioeconomic formations that humanity has known are:

– Antiquity or prehistorical societies;
– Slave-owning system;
– Feudalism;
– Capitalism;
– Socialism;
– Communism.

According to historians, states emerged long time after the beginning of mankind: "Early states appeared on the planetary stage between 6,000 and 5,000 years ago, most notably in Egypt, Mesopotamia and along the Pacific coast of South America. Somewhat later states

1 Human evolution. Britannica. https://clck.ru/3BcmeF
2 Google definition acceded on December, 3rd, 2023.
3 National Museum of Natural History. https://clck.ru/3Bcmf8
4 Source: Google

emerged also in the Indus Valley (about 4,500 years ago), China (about 4,000 years ago) and Central America (about 3,500 years ago)"[5].

Hordes, clans and ethnic groups developed laws that have not only allowed them to live together in relative harmony, but also and above all to survive thanks to the rules and later the established laws. These rules and laws defined the sanctity of the individual and protected them from certain forms of violence and abuse against them.

We see that the role of the law is extremely important for the survival of humanity which continually faces changes sometimes leading to the weakening of certain individuals.

According to Edward W. Younkins: "Historically, socially emergent ideas of legal principles, oftentimes in accord with the nature of reality, occurred prior to their adoption by political authorities. Voluntary forms of governance through customary private laws preexisted state law and effectively ordered human affairs. Law arose as a spontaneous order – something to be discovered rather than enacted. Law is an evolutionary systemic process involving the experiences of a vast number of people"[6].

Each of these societies was governed by laws that aimed to consolidate the established order.

At each stage of humanity's evolution, certain laws have been questioned by a minority or majority group of people, have been repealed and replaced by laws perceived as fairer.

With the proclamation of the Charter of Kurukan Fuga in 1236, the Mali Empire was the first Government to legislate on the rights and duties of the human person and of the different socio-professional strata of Mandé.

The Charter has been inscribed in 2009 by UNESCO on the Representative List of the Intangible Cultural Heritage of Humanity.

The UNESCO gives on its website an overview of the Mande Charter, also called the Kurukanfuga Charter: "In the early thirteenth century, following a major military victory, the founder of the Mandingo Empire and the assembly of his wise men proclaimed in Kurukan Fuga the new Manden Charter, named after the territory situated above the upper Niger River basin, between present-day Guinea and Mali. The Charter, one of the oldest constitutions in the world albeit mainly in oral form, contains a preamble of seven chapters advocating social peace in diversity, the inviolability of the human being, education, the integrity of the motherland, food security, the abolition of slavery by razzia (or raid), and freedom of expression and trade. Although the Empire disappeared, the words of the Charter and the rituals associated with it are still transmitted orally from father to son in a codified way within the Malinke clans. To keep the tradition alive, commemorative annual ceremonies of the historic assembly are organized in the village of Kangaba (adjacent to the vast clearing of Kurukan Fuga, which now lies in Mali, (close to the Guinean border). The ceremonies are backed by the local and national authorities of Mali and, in particular, the traditional

5 Source: Google

6 Younkins, E. W. (2000, August 5). Capitalism & Commerce. The evolution of Law. https://clck.ru/3Bcmji

authorities, who see it as a source of law and as promoting a message of love, peace and fraternity, which has survived through the ages. The Manden Charter continues to underlie the basis of the values and identity of the populations concerned"[7].

When the issue of artificial intelligence is discussed, the tendency is to exclude Africa from the advances that have been made in the field of technology (Stiglitz, 2017; Bob-Milliar, 2021).

Now, as Paul E. Lovejoy (2014) states in his monography "African Contributions to Science, Technology and Development": Africa has contributed to a large extent to the development of science and technology and had a real impact on the world thanks to its inventions and innovations. These are inventions and discoveries that have been made on African soil in the fields of medicine, technology, mathematics, astronomy, agriculture and food industry to name but a few areas.

"The Dogon inhabit an area of Mali called the Bandiagara Escarpment, a stretch of sandstone cliffs nearly 100 miles long, reaching up to 1,500 feet high. Taking advantage of the area for its natural protection, the tribe built their homes on the side of the cliffs during the 3rd century B.C. and have remained there since. But it wasn't until the 1930s that French anthropologists discovered their strangely advanced astronomical knowledge, despite maintaining a very primitive lifestyle.

Although the Dogon live in an area more than 2,000 miles from Egypt, they have a history that appears to have some intriguing connections with its famed, ancient lineage that hinted at some connection to the stars.

Upon studying the Dogon tribe, anthropologist Marcel Griaule learned of their obsession with the Sirius star system. While Sirius A is visible to the naked eye, its companion white dwarf, Sirius B, was not discovered until the 1950s with an advanced telescope. The Dogon, however, were well aware of its presence, as well as its orbital period, describing its existence before it was confirmed years later"[8].

In 1983, Ivan Van Sertima published his book "Blacks in Science: Ancient and Modern. Journal of African Civilizations" in which he cites more than one thousand inventions made by Africans and African descends. "From the three-light traffic signal, refrigerated trucks, automatic elevator doors, color monitors for desktop computers, to the shape of the modern ironing board, the clothes wringer, blood banks, laser treatment for cataracts, home security systems and the super-soaker children's toy, many objects and services Americans use every day were invented by Black men and women. These innovators were recognized for their inventions, but countless other inventors of color have gone largely unrecognized. Others are completely lost to history" (Sertima, 1983).

---

7 UNESCO. Manden Charter, proclaimed in Kurukan Fuga. https://clck.ru/3BcmmS

8 (2019, October 13). Was the Sirius Star System Home to the Dogon African Tribe? Gaia. https://www.gaia.com/article/did-this-african-tribe-originate-in-another-star-system

It must be underlines that it was an enslaved man who helped America getting a vaccine against smallpox. In 1706, he was given to the New England Puritan minister Cotton Mather, who renamed him Onesimus. Onesimus introduced Mather to the principle and procedure of the variolation method of inoculation to prevent the disease, which laid the foundation for the development of vaccines.

"The operation Onesimus referred to consisted of rubbing pus from an infected person into an open wound on the arm. This was done in a controlled manner and under the supervision of a physician so the symptoms would be milder but still confer immunity. Once the infected material was introduced into the body, the person who underwent the procedure was inoculated against smallpox. It wasn't a vaccination, which involves exposure to a less dangerous virus to provoke immunity, but it did activate the recipient's immune response and protected against the disease most of the time."[9]

The problem with the inventions made by Africans and the African diaspora is that they have been obscured by slavery and colonization, two systems of oppression and human exploitation, which made black people inferior and having no rights. At these times, a black man could not patent his inventions, because the patent was a contract between the State and a citizen and Blacks were not citizens. This raises the problem of patents and licenses for inventors as well as intellectual property. Many slaves had to put the name of their master on their patent in order to register it.

The trigger for the design of new laws has often been social and technological transformations. When primitive society passed into antiquity, certainly thanks to the discovery of fire, the social situation of individuals changed: weapons began to be manufactured to hunt game and cultivate the land, which meant that relationships forces were changing in favor of the manufacturers and holders of these weapons.

The advent of feudal society led to the omnipotence of a feudal lord who had extremely important powers due to the fact that he had an army, used religion to perpetuate his power and had the right to life and death on his subjects.

Prehistory is one of the periods of history which begins with the appearance of man and goes until the arrival of writing. This marks the beginning of another period in Antiquity. This ended with the fall of the Roman Empire in 476 AD.

Since ancient times, humans have started to tell legends, myths, sagas etc. in which elements of the supernatural and men and women with superpowers appeared.

With the beginning of the industrial age in Europe, it became possible to build machines to replace human power. It is also the technological innovations implemented on a large scale from the 19th century onwards which are at the origin of the end of slavery and the beginning of colonization. Indeed, to access the raw materials that the West needed to operate its machines, the African continent, which was overflowing with these

[9] Blakemore, E. (2021, April, 8). How an Enslaved African Man in Boston Helped Save Generations from Smallpox. https://clck.ru/3BcmrE

raw materials, was colonized and its populations forced to work by the force of extremely deadly firearms. strength.

It has been stated that: "the Industrial Revolution was the transition from creating goods by hand to using machines. Its start and end are widely debated by scholars, but the period generally spanned from about 1760 to 1840"[10].

What are the four steps of the industrial revolution?

"The four industrial revolutions are coal, gas, electronics and nuclear, and the internet and renewable energy. Beginning from 1765 through the present day, we've seen an amazing evolution"[11].

Each revolution led to a new way of life that had to be regulated to allow society to function in line with what the ruling class wanted. However, the European proletariat which was under the ideological domination and economic exploitation of capitalism organized itself and demanded more humane and decent living and working conditions. This marked the birth of unions and the rise of socialism and communism as political systems.

2. Evolution of the humanity and artificial intelligence: modern prospects

The new technological revolution that we have been witnessing since the end of the 20th century and particularly at the start of the 21st century with the appearance of Artificial Intelligence, requires that laws be taken to avoid all forms of abuse that the development of artificial intelligence could generate.

In our understanding, this means that artificial intelligence must first be the subject of in-depth studies to understand all its contours, its opportunities and potential risks.

The results of these studies must then be disseminated to political decision-makers, elected officials and the general public using popularization processes.

The rise of artificial intelligence (AI) continues to grow thanks to technological advances recorded in recent years.

Having emerged around sixty years ago, artificial intelligence has become the major technological revolution of the beginning of the 21st century (Mocanu, 2021; Mulgan, 2019; Pagallo, 2018).

AI is present in all sectors of activity, particularly in industry, transport, health, commerce, economy, agriculture, infrastructure, education, entertainment, etc. It is predicted that it will generate colossal sums of money and will profoundly change our lifestyles thanks to new inventions (Avila Negri, 2021; Bertolini & Episcopo, 2022).

An Internet source give us the definition of artificial intelligence, how it works and why it is important: "Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Specific applications of AI include

[10] The Industrial Revolution. https://clck.ru/3Bcmro

[11] https://clck.ru/3BcmuT

expert systems, natural language processing, speech recognition and machine vision." (Greenstein, 2022; Hacker et al., 2020; Hárs, 2022)[12].

AI programming focuses on cognitive skills that include the following:

Learning. This aspect of AI programming focuses on acquiring data and creating rules for how to turn it into actionable information. The rules, which are called algorithms, provide computing devices with step-by-step instructions for how to complete a specific task.

Reasoning. This aspect of AI programming focuses on choosing the right algorithm to reach a desired outcome.

Self-correction. This aspect of AI programming is designed to continually fine-tune algorithms and ensure they provide the most accurate results possible.

Creativity. This aspect of AI uses neural networks, rules-based systems, statistical methods and other AI techniques to generate new images, new text, new music and new ideas"[13].

Conclusions

AI is important for its potential to change how we live, work and play. It has been effectively used in business to automate tasks done by humans, including customer service work, lead generation, fraud detection and quality control (Bryson et al., 2017; Calo, 2015; Chesterman, 2020). In a number of areas, AI can perform tasks much better than humans"[14].

In order to create the link between artificial intelligence and law, we will look at human evolution, as well as the evolution of different social organizations to understand how laws have been designed and implemented with the aim of to enable living together and the survival of the groups concerned.

To guarantee security and prevent any confusion, it has to be legislated on artificial intelligence (Malgieri & Comandé, 2017; McCarty, 2017; Karnouskos, 2022; Maarten Herbosch, 2024; McNally & Inayatullah, 1988).

In particular, we must prevent artificial intelligence in the military field from falling into civilian hands, so that these inventions which should only be used in the event of war or other security threats do not come into the possession of ill-intentioned people who have nothing to do with the army.

We must develop curricula that make the school and university environment healthy and ethical when it integrates artificial intelligence into teaching programs (Sertima, 1983; Solaiman, 2017; Solum, 1992).

---

12 Gunning, D. (2017). Explainable artificial intelligence (XAI). Defense advanced research projects agency (DARPA). https://clck.ru/3BcmvV

13 Laskowski, N., & Tucci, L. Artificial intelligence (AI). TechTarget. https://clck.ru/3Bcmxj

14 Ibid.

Finally, we must legislate on intellectual property to guarantee the rights of inventors. This is extremely important to ensure social justice and equity among all human beings regardless of their social, cultural and ethnic origin. It is at this price that artificial intelligence will be an instrument of socio-economic development and lasting peace.

References

Avila Negri, S. M. C. (2021). Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. *Frontiers in Robotics and AI*, *8*, Art. 789327. https://doi.org/10.3389/frobt.2021.789327

Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Frontiers in Robotics and AI*, *9*, Art. 842213. https://doi.org/10.3389/frobt.2022.842213

Bob-Milliar, G. M. (2021). Africa's Contributions to World Civilization. In *The Palgrave Handbook of Africa and the Changing Global Order* (pp. 25–42). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-77481-3_2

Bryson, J. J., Diamantis, M. E., & Grant, Th. D. (2017). Of, For, and By the People: The Legal Lacuna of Synthetic Persons. *Artificial Intelligence and Law*, *25*, 273–291. https://doi.org/10.1007/s10506-017-9214-9

Calo, R. (2015). Robotics and the Lessons of Cyberlaw. *California Law Review*, *103*(3), 513–563.

Chesterman, S. (2020). Artificial Intelligence and the Limits of Legal Personality. *International & Comparative Law Quarterly*, *69*, 819–844. https://doi.org/10.1017/s0020589320000366

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

Hárs, A. (2022). AI and international law – Legal personality and avenues for regulation. *Hungarian Journal of Legal Studies*, *62*(4), 320–344. https://doi.org/10.1556/2052.2022.00352

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*, 93–115. https://doi.org/10.1007/s10506-021-09289-1

Lovejoy, P. E. (2014). *African contributions to science, technology and development*. Collective Volume the (Slave Route Project, UNSECO 2012).

Maarten Herbosch. (2024). Fraud by generative AI chatbots: On the thin line between deception and negligence. *Computer Law & Security Review*, *52*, 105941–105941. https://doi.org/10.1016/j.clsr.2024.105941

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

McCarty, L. T. (2017). Finding the Right Balance in Artificial Intelligence and Law. In *Research Handbook on the Law of Artificial Intelligence* (Chapter 3, pp. 55–87). Edward Elgar Publishing. https://doi.org/10.4337/9781786439055.00013

McNally, Ph., & Inayatullah, S. (1988). The Rights of Robots: Technology, Culture and Law in the 21st Century. *Futures*, *20*(2), 119–136. https://doi.org/10.1016/0016-3287(88)90019-5

Mocanu, D. M. (2021). Gradient Legal Personhood for AI Systems – Painting Continental Legal Shapes Made to Fit Analytical Molds. *Frontiers in Robotics and AI*, *8*, Art. 788179. https://doi.org/10.3389/frobt.2021.788179

Mulgan, T. (2019). Corporate Agency and Possible Futures. *Journal of Business Ethics*, *154*, 901–916. https://doi.org/10.1007/s10551-018-3887-1

Pagallo, U. (2018). Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems. *Philosophical Transactions of the Royal Society*, *376*(2133), Art. 20180168. https://doi.org/10.1098/rsta.2018.0168

Sertima, I. V. (Ed.) (1983). Blacks in Science: Ancient and Modern. *Journal of African Civilizations*, *5*(1-2).

Solaiman, S. M. (2017). Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy. *Artificial Intelligence and Law*, *25*(2), 155–179. https://doi.org/10.1007/s10506-016-9192-3

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287.

Stiglitz, J. E. (2017). The coming great transformation. *Journal of Policy Modeling*, *39*(4), 625–638. https://doi.org/10.1016/j.jpolmod.2017.05.009

Author information

Djeneba Traore – PhD, Professor, Former Rector, University of Arts and Humanities of Bamako; Director General for Regional Integration and Social Transformations in West Africa, West Africa Institute
Address: E 3637, Bamako, Mali; 396-A, Praia, Cabo Verde
E-mail: badjenetraore@yahoo.fr
ORCID ID: https://orcid.org/0009-0006-2674-2565
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57202159729

Conflict of interest

The author 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 – December 3, 2023
Date of approval – January 6, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024

Научная статья
УДК 34:004:17:004.8
EDN: https://elibrary.ru/fhsfeo
DOI: https://doi.org/10.21202/jdtl.2024.24

От теории африканского происхождения человечества к современным социальным, правовым и технологическим новациям: краткий аналитический экскурс в антропосоциогенез

Дженеба Траоре

Университет гуманитарных и социальных наук Бамако, Бамако, Мали
Институт Западной Африки, Прая, Кабо-Верде

Ключевые слова

антропогенез,
искусственный интеллект,
общественные трансформации,
право,
промышленная революция,
социальная справедливость,
социогенез,
технологическая революция,
цифровые технологии,
эволюция человека

Аннотация

Цель: проследить эволюцию человечества и выявить роль различных социальных институтов для понимания экзистенциальной роли законов, направленных на обеспечение совместной жизни социума в контексте технологических новаций.

Методы: в процессе исследования использованы общенаучные и специальные методы познания, позволившие проследить диалектическое развитие человечества, социальные трансформации и технологические новации.

Результаты: оглядываясь на историю человечества, зародившегося на Африканском континенте (теория африканского происхождения), автор отмечает наиболее важные изменения в образе жизни человека и его окружающей среде, которые привели к необходимости построения организованных обществ и регулирования социального поведения в нем с помощью законодательных норм. Право рассматривается как часть эволюционного процесса, которое должно было возникнуть в ходе эволюции человечества. Отмечается чрезвычайная важность закона для преодоления возникающих в процессе эволюции глобальных вызовов и экзистенциальных вопросов дальнейшего сосуществования человечества. В этой связи подчеркивается историческое значение Хартии Курукан-Фуга Малийской империи как одной из древнейших конституций в мире, получившей признание на международном уровне как важного источника юридических и политических норм для современных обществ, регламентирующих устройство

государственной власти и социальное поведение, хотя и сохранившейся в основном в устной форме. Утверждается, что толчком к разработке новых законов часто служили социальные и технологические преобразования. Человечество много раз вмешивалось в собственную биологическую эволюцию при помощи технологий, теперь же наступает важный с точки зрения права и этики момент возможного вмешательства технологий в дальнейшую эволюцию человека. Наибольшее опасение в этом плане вызывает эпоха бурного развития искусственного интеллекта, предъявляющая к человеку новые требования.

Научная новизна: показана роль Африканского континента в происхождении и развитии человечества, социально-правовых институтов, находящихся в свете современных трансформаций и конструирования новой социальной реальности.

Практическая значимость: проведенное исследование создает предпосылки для дальнейшего развития теории антропосоциогенеза и углубленного концептуального историко-правового изучения роли Африканского континента в развитии человечества и его социальных институтов.

Для цитирования

Траоре, Д. (2024). От теории африканского происхождения человечества к современным социальным, правовым и технологическим новациям: краткий аналитический экскурс в антропосоциогенез. *Journal of Digital Technologies and Law*, *2*(2), 473–486. https://doi.org/10.21202/jdtl.2024.24

Список литературы

Avila Negri, S. M. C. (2021). Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. *Frontiers in Robotics and AI*, *8*, Art. 789327. https://doi.org/10.3389/frobt.2021.789327

Bertolini, A., & Episcopo, F. (2022). Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Frontiers in Robotics and AI*, *9*, Art. 842213. https://doi.org/10.3389/frobt.2022.842213

Bob-Milliar, G. M. (2021). Africa's Contributions to World Civilization. In *The Palgrave Handbook of Africa and the Changing Global Order* (pp. 25–42). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-77481-3_2

Bryson, J. J., Diamantis, M. E., & Grant, Th. D. (2017). Of, For, and By the People: The Legal Lacuna of Synthetic Persons. *Artificial Intelligence and Law*, *25*, 273–291. https://doi.org/10.1007/s10506-017-9214-9

Calo, R. (2015). Robotics and the Lessons of Cyberlaw. *California Law Review*, *103*(3), 513–563.

Chesterman, S. (2020). Artificial Intelligence and the Limits of Legal Personality. *International & Comparative Law Quarterly*, *69*, 819–844. https://doi.org/10.1017/s0020589320000366

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

Hárs, A. (2022). AI and international law – Legal personality and avenues for regulation. *Hungarian Journal of Legal Studies*, *62*(4), 320–344. https://doi.org/10.1556/2052.2022.00352

Karnouskos, S. (2022). Symbiosis with artificial intelligence via the prism of law, robots, and society. *Artificial Intelligence and Law*, *30*, 93–115. https://doi.org/10.1007/s10506-021-09289-1

Lovejoy, P. E. (2014). *African contributions to science, technology and development*. Collective Volume the (Slave Route Project, UNSECO 2012).

Maarten Herbosch. (2024). Fraud by generative AI chatbots: On the thin line between deception and negligence. *Computer Law & Security Review*, *52*, 105941–105941. https://doi.org/10.1016/j.clsr.2024.105941

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

McCarty, L. T. (2017). Finding the Right Balance in Artificial Intelligence and Law. In *Research Handbook on the Law of Artificial Intelligence* (Chapter 3, pp. 55–87). Edward Elgar Publishing. https://doi.org/10.4337/9781786439055.00013

McNally, Ph., & Inayatullah, S. (1988). The Rights of Robots: Technology, Culture and Law in the 21st Century. *Futures*, *20*(2), 119–136. https://doi.org/10.1016/0016-3287(88)90019-5

Mocanu, D. M. (2021). Gradient Legal Personhood for AI Systems – Painting Continental Legal Shapes Made to Fit Analytical Molds. *Frontiers in Robotics and AI*, *8*, Art. 788179. https://doi.org/10.3389/frobt.2021.788179

Mulgan, T. (2019). Corporate Agency and Possible Futures. *Journal of Business Ethics*, *154*, 901–916. https://doi.org/10.1007/s10551-018-3887-1

Pagallo, U. (2018). Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems. *Philosophical Transactions of the Royal Society*, *376*(2133), Art. 20180168. https://doi.org/10.1098/rsta.2018.0168

Sertima, I. V. (Ed.) (1983). Blacks in Science: Ancient and Modern. *Journal of African Civilizations*, *5*(1-2).

Solaiman, S. M. (2017). Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy. *Artificial Intelligence and Law*, *25*(2), 155–179. https://doi.org/10.1007/s10506-016-9192-3

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287.

Stiglitz, J. E. (2017). The coming great transformation. *Journal of Policy Modeling*, *39*(4), 625–638. https://doi.org/10.1016/j.jpolmod.2017.05.009

Сведения об авторе

Траоре Дженеба – PhD, профессор, ректор в отставке, Университет гуманитарных и социальных наук Бамако; генеральный директор по вопросам региональной интеграции и социальных трансформаций в Западной Африке, Институт Западной Африки
Адрес: Мали, г. Бамако, E 3637; Кабо-Верде, г. Прая, 396-A
E-mail: badjenetraore@yahoo.fr
ORCID ID: https://orcid.org/0009-0006-2674-2565
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57202159729

Конфликт интересов

Автор сообщает 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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 3 декабря 2023 г.
Дата одобрения после рецензирования – 6 января 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.