ISSN 2949-2483

Volume 3 Number 2

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2025

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 3, No. 2
2025
DOI: 10.21202/2949-2483.2025.2
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: 2025, June 20. Hosted on the website https://www.lawjournal.digital: 2025, June 25.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 3, No. 2
2025
DOI: 10.21202/2949-2483.2025.2
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Research article
UDC 34:004:343.9:004.9
EDN: https://elibrary.ru/ypsxqo
DOI: https://doi.org/10.21202/jdtl.2025.8

Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development

Marina A. Efremova ✉

Lebedev Russian State University of Justice, Moscow, Russia

Evgeniy A. Russkevich

Kutafin Moscow State Law University, Moscow, Russia

Keywords

avatar,
crime,
criminal law,
criminal liability,
criminology,
cybercrime,
digital technologies,
law,
metaverse,
virtuality

Abstract

Objective: to conduct a comprehensive analysis of criminal-legal risks arising in the development of the metaverse as a new digital space of social interaction; to define the concept of the metaverse and assess the possibilities of countering criminal activity in this environment by means of criminal law.

Methods: the research methodology consists of the dialectical method of scientific cognition, analysis, synthesis, and a set of specific legal methods. A systematic approach was applied to study legal phenomena in the digital environment; a comparative legal method was used to analyze foreign experience, and a formal legal method – to interpret regulations and doctrinal provisions.

Results: it has been established that the metaverse attractiveness for various forms of criminal activity is largely due to the user anonymity and the lack of a clear legal regime. The study showed that numerous crimes are already being committed on the metaverse platforms. These include socially dangerous acts related to the dissemination of criminogenic and traumatic information, theft of digital property, criminal money laundering, and attacks against the sexual integrity of a person. The authors identify systemic problems of countering crime in the metaverse, including territorial jurisdiction, user identification, and procedural difficulties of proof.

✉ Corresponding author

Scientific novelty: a comprehensive analysis of the criminal-legal aspects of the metaverse functioning was performed. The article formulated theoretical approaches to the qualification of crimes committed in the virtual space. The work substantiates the need to develop special legal structures for regulating relations in the metaverse. The authors proposed a concept of a multidimensional model of legal protection of relations in the metaverse based on public-private partnership.

Practical significance: the study results can be used in improving criminal legislation in terms of regulating responsibility for crimes committed in the digital space. The work may help to develop the concept of legal regulation of the metaverse and to create mechanisms for public-private partnership in the field of countering cybercrime. The findings are relevant for law enforcement practice in the investigation of crimes committed using virtual reality technologies.

For citation

Efremova, M. A., & Russkevich, E. A. (2025). Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development. *Journal of Digital Technologies and Law, 3*(2), 187–202. https://doi.org/10.21202/jdtl.2025.8

Contents

Introduction

With the expansion of Web 3.0, virtual reality began to develop in a new direction. Since 2021, leading IT companies have been developing the metaverse, a new digital space combining physical reality with the augmented reality (AR) and virtual reality (VR) technologies.

It is believed that metaverse technologies can be widely used in such areas as education, culture, trade, etc. (Lewandowsky, 2024). The Singapore government has already announced that most public services will soon be available through virtual representations of relevant structures in the metaverse[1].

In Russia, attention to the metaverse regulation and legal risks was largely due to the speech of the President of the Russian Federation, Vladimir Putin, in which he stated the

[1] Newar, B. (2022, July 29). Marriages and court cases can be held in the Metaverse. Cointelegraph. https://clck.ru/3MGuS6

need to use the opportunities of the metaverse so that people could communicate, work together, study, and implement joint creative and business projects. Also, the head of state noted that this is a real challenge for technology companies, creative industries, as well as for lawyers who are to develop rules for regulating economic and public relations in the fundamentally new world[2].

According to expert estimates, the metaverse market should reach US$74.4 billion in 2025 and 2,633 million users by 2030[3]. Many of the world's leading brands have already established their presence in the metaverse and begun trading and holding virtual presentations, concerts, and exhibitions. For example, in the Decentraland metaverse, Dolce & Gabbana hosted the first Metaverse Fashion Week, featuring a 20-piece collection[4]. Omoda unveiled a new line of vehicles on the metaverse platform. Visitors submitted applications for a test drive of cars, and sales increased after the virtual dealership was opened[5].

We should agree with A.M. Konstantinov that the digital metaverse is currently being formed as an integrated and multilateral public space, some aspects of which are a challenge for many humanities, including legal theory[6].

It is important to realize that the metaverse is not just another multiplayer computer game. The idea of the metaverse is to create a virtual analogue of the real world, although it will not be limited to this, of course (Narasimhan & Kala, 2024). In the criminal law aspect, the metaverse attracts attention as a new space for social interaction, which can (and in fact already does) serve as a space for criminal activity (Saharan et al., 2023). Indeed, for many socially dangerous attacks provided for by criminal law, virtualization makes little difference in achieving the desired result. Moreover, such a virtual world, which does not have a clear law enforcement system, has obvious advantages for intruders (anonymity, wide reach, etc.) (Marshall & Tompsett, 2023).

One could object that the problem of malicious behavior in the metaverse is far-fetched, does not require legal intervention, and should remain completely within the system of relations between a resource owner and a user. We believe that this is a misconception. Such an elimination from public regulation and protection (the "vicious circle" theory) is relatively suitable for computer games, but not for a virtual analogue

2 Minutes of the speeches of participants of Artificial Intelligence Journey 2021. (2021, November 12). https://clck.ru/3MGuU3

3 Metaverse – Worldwide. Statista. https://clck.ru/3MGuW6

4 Metaverse Fashion week. (2022, April 25). NFT Art. https://clck.ru/3MGuYW

5 Is there a demand for events in metaverses in Russia? (2023, July 29). Sostav. https://clck.ru/3MGuau

6 Konstantinov, A. M. (2023). Gaming norms in legal regulation. Cand. Sci. (Law) thesis. Volgograd. P. 145.

of the real world in which government agencies, commercial and non-profit organizations, and real people operate, albeit through their digital counterparts (avatars) (Singh, 2024).

1. Concept of the metaverse

The term "metaverse" is believed to first appear in Neal Stephenson's novel "Snow Crash" in 1992, showing a virtual world as a continuation of people's physical lives, in which they spent most of their time.

The metaverse is a result of convergence of technologies, the blockchain and the Web.3 named as the key ones. Immersion technology is also one of the main components of the metaverse, used to connect users to the virtual world and interact with its objects (Alawadh, 2023). Immersive technologies ensure a realistic representation of virtual content in the metaverse. The Internet of Things (IoT) is necessary to connect the metaverse with the real world. A network is required for communication and data transmission. It allows users around the world to connect to the metaverse (AlMutawa et al., 2024). Cloud and peripheral computing are required for the distributed storage and processing of the vast amount of data generated by the metaverse. It is important to emphasize that the metaverse allows people to interact as if they are not in the virtual, but in the real world.

Although there is no universal definition of the metaverse, in a broad sense it can be defined as a collective virtual space created by a convergence of augmented virtual reality and the physical world.

2. Crime and the metaverse

The metaverse poses the same systemic problem to criminal law as it does to any branch of law (AL-Tkhayneh, 2023). Conventionally, it can be described as follows: if the metaverse is a digital analogue of the physical world where individuals enter into relationships and engage in harmful behavior using their digital images (avatars), is it possible to extend the existing legal frameworks to both these relationships and this harmful behavior?

Modern literature suggests that any crime, including murder, can be committed in the metaverse. This is a bold idea. To agree with it, one must review many fundamental provisions of criminal law, to form completely different understanding of such key categories as victim, life, death, the subject of crime, etc. Is the Russian legal doctrine ready for this? Probably not.

Currently, crimes related to the dissemination of criminogenic and traumatic information are committed on the metaverse platforms (Gómez-Quintero et al, 2023). To a certain extent, this was expected, since digital technologies have always been attractive for criminal activities related to the distribution of prohibited content (Teodorov, 2023).

As for many criminal acts of this group (Articles 110, 110[1], 110[2], 128[1], 137, 205[1], 205[2], 205[3], 242, 242[1], 280, 280[1], 280[3], 280[4], 282 of the Russian Criminal Code), their implementation in the metaverse does not exclude the possibility of bringing a person to criminal responsibility. The metaverse is just one of many digital platforms (messengers, social networks, multi-user virtual games, etc.) used to disseminate prohibited information (Blake, 2023).

Special attention should be paid to the question whether information about a person's activity in the metaverse is a personal secret within the meaning of Art. 137 of the Russian Criminal Code. Today, the virtual world provides a user with almost limitless opportunities for self-identification and self-expression: one can choose an avatar of any gender, determine their race, age and appearance at one's own discretion. The user can enter into a variety of relationships with other avatars and be active in the metaverse, while assessing the information about it as a personal secret. For example, in the metaverse, users can not only be in a relationship (engage in sexual activity without physical contact), but also get married with an NFT certificate, which serves as an alternative to official registration in the real world. We believe that the collection and dissemination of such information about a real person (provided they correspond to the signs of secrecy) fully fall within the Art. 137 of the Russian Criminal Code.

The possibility of bringing a person to criminal liability for violating the right to freedom of conscience and religion committed in the metaverse (Article 148 of the Russian Criminal Code) is debatable. By its nature, this crime can consist both in the public dissemination of certain information offensive to believers and in the commission of specific actions related to interference in worshipping, ritual, etc. In the first case, the application of Art. 148 of the Russian Criminal Code cannot raise objections. However, in case of other actions one has to agree with several assumptions at once, first of all, with the fact that worship or other religious rite can take place in the metaverse. In addition, it should be recognized that the avatar's behavior in the metaverse has signs of interference in the ritual. Indeed, under certain circumstances, a person who is not aware of the intricacies of a particular religious rite can quite conscientiously assess one's actions as permissible and not creating obstacles to its implementation. But, of course, the key issue is recognizing the very possibility of exercising the right to freedom of conscience and religion in the virtual space.

A broadly discussed problem of crime in the metaverse is the possibility of attacks against sexual freedom and sexual integrity of an individual (Wiederhold, 2022). The key point is that it is not the user who is being "sexually abused", but their avatar, of course[7]. Those who had encountered with this phenomenon noted that they had experienced

[7] Smith, I. (2016, October 30). Even in a virtual world, the harsh reality of sexual harassment persists. NPR. https://clck.ru/3MGumo

a strong emotional shock as a result of such actions. A famous example is the case of Nina Jane Patel, whose avatar was sexually assaulted by four male avatars at once on the Horizon Venues platform. According to her, she experienced a psychological shock. It is indeed noted in the literature that, due to immersive technologies, such actions against an avatar can cause emotional experience comparable to the shock of sexual violence in real life (Chawki et al., 2024).

Another example: in the UK, an investigation was initiated into an incident in the metaverse where an avatar (owned by a child) was attacked, involving manipulation similar to sexual violence. This fact caused a mixed reaction from the public. Many criticized, pointing out that law enforcement agencies should be engaged in criminal prosecution of real attacks on sexual freedom[8].

For the same reasons as with murder, the application of criminal law norms on liability for sexual crimes in relation to avatars of the metaverse seems impossible. An avatar is just a digital image of a person in the virtual world and cannot have sexual freedom, as well as sexual inviolability. At least, that is the case at the moment. Of course, one may assume that over time such digital alter-egos will become inseparable from the real person. Then, we will have to review the object of sexual assault and recognize, as part of a person's sexual freedom, also one's right to choose partners and engage in sexual relations, at one's own discretion and without coercion, using one's avatar in the metaverse (Cheong, 2022). However, this is a question of the future and, probably, not the closest future.

It is important to make a reservation that, under the Russian criminal law, it is already possible to initiate criminal proceedings on indecent acts in the metaverse and in some cases on sexual violence against a person under the age of twelve – provided that the perpetrators were aware of the age of the avatar's owner, of course.

The metaverse ecosystem provides opportunities for the acquisition of "digital property", including virtual land plots, buildings and structures. The three most popular platforms include The Sandbox, Decentraland, and SuperWorld. It is known that the cost of land plots can range from hundreds to millions of US dollars. For example, one of the most expensive "digital real estate" transactions was the purchase of 100 private islands on The Sandbox platform for US$4.3 million[9]. The metaverse users place bets on virtual land plots via trading platforms, and purchasing is much like buying real estate in the real

[8] Camber, R. (2024, January 1). British police probe VIRTUAL rape in metaverse: Young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' - sparking first investigation of its kind and questions about extent current laws apply in online world. Mail Online. https://clck.ru/3MejXs

[9] META MONEY Most expensive metaverse properties – including $4.3m purchase of EMPTY virtual land. (2022, March 28).The Sun. https://clck.ru/3MGuu6

world. As soon as the buyer purchases virtual land, the transaction is recorded in the blockchain, which in a sense serves as an analogue of making an entry in the real estate registry when making transactions in the real world. Since many of these virtual worlds have a limited number of land plots, as the popularity of the platform grows, so does their value. Cases of illegal acquisition of digital property in the metaverse are also known. For example, a malware program was used to "steal" a land plot worth £10,000[10] from one of The Sandbox platform users.

According to Russian criminal law, it is impossible to steal virtual property. We can only talk about illegal access to legally protected computer information for mercenary reasons (Part 2 of Article 272 of the Russian Criminal Code). However, one should admit how far such a qualification is from the content and focus of seizing the victim's digital assets. After all, this is not so much about the software and technical means of information protection, but rather about taking possession of items that are marketable and often of significant value.

The debate on this issue in modern jurisprudence (Lin et al., 2023), as a rule, points out the dependence of criminal law protection on the regulation of the relevant objects' turnover in civil law. However, given the current situation, there are more and more arguments that such a relationship does not constitute an absolute dependence of one on the other (Bhardwaj, 2024). Perhaps, the recognized secondary nature of criminal law protection can be overcome by developing special rules for the qualification of encroachments on "digital property", with them forming the subject of specific crimes against property. Similar approach is known to be implemented in the explanations of the Russian Supreme Court's Plenum about legalization. If transactions with cryptocurrencies and other digital assets are possible per se, including for the purposes of criminal legalization, then there are no serious obstacles to considering them as an object with a specific value at the time of the criminal encroachment.

As was noted above, the internal economy of the metaverse serves as an effective tool for money laundering (Wu et al., 2023). Metaverses allow, just as in the physical world but with lower risks, to create the appearance of "profitable" economic activity (provision of virtual services, trading in virtual assets, etc.). This has already been highlighted in the legal literature (Mooji, 2024). In general, the provisions of the Russian criminal law (Articles 174, 174[1] of the Russian Criminal Code) can be applied here on common grounds.

The existence of own economy within the metaverse (Wasswa, 2023) raises the question of the applicability of the traditional criminal law liability provisions to crimes in the field of business and taxation. Suppose a person organizes a platform-based cryptocurrency exchange point. Clients visit it using avatars and make payments with the

[10] LAND GRAB I bought £10,000 worth of digital land in The Sandbox metaverse game but it was stolen and sold for £23,000. (2022, January 11). The U.S. Sun. https://clck.ru/3MGuvq

organizer in one form or another. Clearly, in real life such activities are grounds for bringing the person to criminal liability for illegal banking (if a large amount of income is proven). As is rightly noted in the literature, actions to cash out funds may constitute a crime under Article 172 of the Russian Criminal Code, if large-scale income is extracted, since cashing operations can be considered cash services for individuals and legal entities (Gribunov et al., 2023). However, banking operations cannot be carried out in the metaverse, at least from a formal viewpoint.

It is equally difficult to qualify the actions of a person who, having the status of an economic entity, carries out activities (consulting services, design, etc.) not only in the physical world, but also in the metaverse, receiving significant income from the latter. I.A.Khavanova rightly summarizes that national regulators and tax authorities are still trying to comprehend the problems that arise in the metaverse, including those related to determining the moment of income, evaluating transactions of exchanging virtual goods for virtual or fiat currencies. At the same time, she is right saying that the technical impossibility of accurately calculating the tax base and determining the source of income in a space whose integral component is anonymity should not serve as a basis for non-taxation (Khavanova, 2024). Consequently, it is impossible even to raise the question of applying the rules on tax crimes if a person misleads the tax authorities about the income received from activities in the metaverse.

The above list of criminal-legal risks in the metaverse is, of course, not exhaustive. For example, one could also consider the urgent problem of committing corruption crimes using digital objects of the metaverse. However, further presentation of specific examples will add little to the overall picture. It is more important to pay attention to a number of systemic problems of crime prevention in the metaverse.

As is known, the metaverse has no geographical boundaries. Experts are actively discussing the problem of establishing so-called “cyber boundaries”, or the limits of the powers of states in virtual interaction and compliance with “cyber sovereignty”. It is expected that special procedures will be developed for the metaverse to hold individuals accountable for offenses and crimes based on the legislation of those countries with which the relevant metaverse platforms are affiliated[11]. So far, these problems are under development, which creates additional prerequisites for various forms of criminal activity.

There is much debate about whether the real identity of a user of the metaverse should be disclosed in case of an illegal act. This, anyway, is related to the question

[11] Abraham, A. (2022, April 4). Law & Order in the Metaverse. Finextra. https://clck.ru/3MGv2L

of whether the user's real identity should be combined with only one avatar. Obviously, if a user can have only one avatar, additional identification information will be required. Since the legal guarantees of the right to privacy vary from country to country, it is necessary to reach a consensus on what information about their identity should the users provide.

Until now, when creating avatars, users may imitate other people: celebrities or their friends, colleagues, as well as deceased persons. Over time, this can lead not only to ethical, but also to legal problems (Begishev et al., 2023). For example, law enforcement practice may face numerous disputes about protection of honor and dignity, business reputation and good name against actions committed in the metaverse using the victim's biometric data (for example, a peeved student using the biometric data of a professor in the metaverse to create an image of a prostitute or a drug dealer). A fundamental solution is possible by introducing a registration mechanism in the public registry of avatars, where each person may register only one avatar in the metaverse under a unique identifier (Qin et al., 2025). At the same time, if we are talking about the metaverse as an alternative social space in a virtual environment, the creation of such a registered avatar, supposedly, should be linked to the user's biometric data (technically it is already possible now). In other words, at a certain stage in the metaverse development, today's complete freedom to choose a digital image will probably have to be abandoned.

Finally, all the above said, related to the (greater or lesser) applicability of the substantive criminal law provisions to the users' actions in the metaverse, is only valid if we agree that there are procedural and criminological tools to prove a criminal case. This has already been noticed in Russian science. For example, O. A. Zaitsev rightly stated that we have to improve access to technological integrated platforms that facilitate obtaining the necessary data in the infrastructure of a single information space, as well as to change the very concepts of the criminal procedure, as it contradicts modern methods of obtaining evidentiary information. He also rightly noted that we urgently need an improved legal regulation of electronic evidence in proving the guilt (innocence) of a person in committing a criminal act, as well as a greater range of investigative actions to more productively obtain evidentiary information in electronic format (Zaitsev, 2024).

Conclusions

The most predictable answer to all the problematic issues of legal regulation and protection of relations in the metaverse would be to state that the digital analogue of human physical space requires a digital analogue of real-world law. This involves either applying the provisions of legislation by analogy (where this is permissible), or expanding the limits of existing legal structures through interpretation, or, if necessary,

constructing special "digital twins" of legal norms designed specifically for these relations.

However, the simplicity of the solution is not a guarantee of its correctness. Not everything in the metaverse should be regulated or protected by means of criminal repression. As in the physical world, there are areas in the metaverse that should remain outside the legal regulation. Perhaps, we may argue that there should be significantly more such spheres in the metaverse than in real life.

However, it is also clear that one cannot remain in the paradigm of the real law non-interference in virtual relationships (Duranske, 2008; Fairfield, 2012). According to A. A. Smirnov, in the longer event horizon, as the ontological status of virtual worlds is established as a new environment for human existence, there will be a need to create a full-fledged system of legal regulation of life in virtual worlds (metaverses). Based on these considerations, he justifies the need to develop and adopt a Federal Law "On virtual and augmented reality systems"[12].

At the same time, T. Ya. Khabrieva quite rightly points out the general ineffectiveness of exclusively legislative regulation of relations in cyberspace, compared to other mechanisms (Khabrieva, 2018). In this regard, the model of regulation and protection of relations in the metaverse seems promising mainly through the development of framework rules of user behavior (the so-called "soft law" system) and the selective regulation of legal norms of those relations that cannot be regulated in any other way (beyond the boundaries of the well-known "vicious circle"). In order to prevent and effectively counteract crimes, states and metaverse platforms' owners have yet to find a balance between anonymity and the protection of confidential user data. The metaverse platforms cannot remain just a virtual field for user interaction; they must be involved in their interaction to ensure a balance of interests. Therefore, the model of protecting relations in the metaverse from the most dangerous attacks should be multidimensional and based on close cooperation between the state, the IT sector, business, and users.

References

Alawadhi, I. M. (2023). F*uture Cybercrimes in the Metaverse* (pp. 24–32). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch002

AlMutawa, A., Ikuesan, R. A., & Said, H. (2024). Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model. *Future Internet*, *16*(12), 437. https://doi.org/10.3390/fi16120437

AL-Tkhayneh, K. M., Olowoselu, A., & Alkrisheh, M. A. (2023). *The Crime in Metaverse (the Future Scenarios for Crime Patterns and the Prospective Legal Challenges)*. 1–6. https://doi.org/10.1109/snams60348.2023.10375402

Begishev, I., Denisovich, V. V., Sabitov, R. A., Pass, A. A., & Skorobogatov, A. (2023). *Criminal-legal significance of metaverses: collisions in law*. https://doi.org/10.47475/2311-696x-2023-39-4-58-62

[12] Smirnov, A. A. (2022). Forming the system of legal provision for information and psychological security in the Russian Federation. Dr. Sci (Law) thesis. Moscow.

Bhardwaj, A. (2024). *Cyber Fraud Use Cases in the Metaverse* (pp. 106–130). BENTHAM SCIENCE PUBLISHERS. https://doi.org/10.2174/9789815238457124010007

Billcliff, T. (2023). *Cybercrimes in the Metaverse: Challenges and Solutions*. https://doi.org/10.19107/cybercon.2023.28

Blake, J. (2023). *Online Crime in the Metaverse* (pp. 66–77). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch004

Chawki M., Basu, S., Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, *13*(3), 33. https://doi.org/10.3390/laws13030033

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedie. I*nternational Cybersecurity Law Review*, *3*, 467–494. https://doi.org/10.1365/s43439-022-00056-9

Duranske, B. T. (2008). *Virtual Law. Navigating the Legal Landscape of Virtual Worlds*. Chicago, Illinois: ABA Publishing, American Bar Association.

Fairfield J. A. T. (2012). Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life. *Berkeley Technology Law Journal, 27*.

Gómez-Quintero, J, Johnson, Sh. D., Borrion, H., & Lundrigan, S. (2023). *A scoping study of crime facilitated by the metaverse*. https://doi.org/10.31235/osf.io/x9vbn

Gribunov, O. P., Nikonov, P. V., Parkhomenko, S. V., Rogova, E. V., Shikhanov, V. N. (2023). *Digital currency and digital financial rights as an object and means of committing crimes*. Irkutsk: Irkutsk Law Institute (branch) of the University of the Russian Prosecutor's Office.

Khabrieva, T. Ya. (2018). The law facing the challenges of digital reality. *Journal of Russian Law*, *9*(261), 5–16. https://doi.org/10.12737/art_2018_9_1

Khavanova, I. A. (2024). The metaverse: the problem of adapting tax and legal structures. *Journal of Russian Law*, *7*, 78–93. https://doi.org/10.61205/S160565900029634-1

Lewandowsky, P. (2024). Cybercrime in the Meta-Universe. *Journal of Social Science and Humanities*, *6*(8), 5–8. https://doi.org/10.53469/jssh.2024.06(08).02

Lin, K.-X., Wu, J., Lin, D., & Zheng, Z. (2023). A Survey on Metaverse: Applications, Crimes and Governance. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan* (pp. 541–549). https://doi.org/10.1109/metacom57706.2023.00097

Marshall, A. M., & Tompsett, B. (2023). The metaverse – Not a new frontier for crime. *WIREs Forensic Science*, *6*(1), e1505. https://doi.org/10.1002/wfs2.1505

Mooij A. (2024). *Regulating the Metaverse Economy*. Springer Briefs in Law. Springer.

Narasimhan, P., & Kala, N. (2024). Securing the Metaverse: AI-Driven Solutions for Cyber Security, Privacy, and User Trust. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 1890–1918. https://doi.org/10.32628/cseit241061238

Qin, H. X., Wang, Y. & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanit Soc Sci Commun*, *12*, 194. https://doi.org/10.1057/s41599-024-04266-w

Saharan, S., Singh, S., Bhandari, A. K., & Yadav, B. (2023). The Future of Cyber-Crimes and Cyber War in the Metaverse. In H. N. Elshenraki (Ed.), *The Age of the Metaverse* (pp. 126–148). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch007

Singh, P. P. (2024). Cyber Crimes in Metaverse. *International Journal of Science and Research*, *13*(2). https://doi.org/10.21275/mr24130195237

Teodorov, A.-V. (2023). Cybercrimes in the Metaverse: Challenges and Solutions. In *International Conference on Cybersecurity and Cybercrime*, 10 (pp. 209–215). https://doi.org/10.19107/cybercon.2023.28

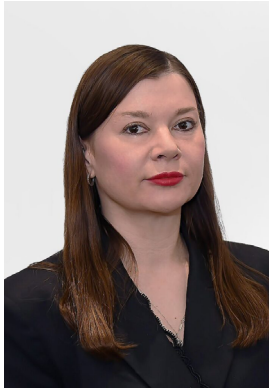
Wasswa, S. (2023). *Predicting Future Cybercrime Trends in the Metaverse Era* (pp. 78–113). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch005

Wiederhold B. K. (2022). Sexual harassment in the metaverse. Cyberpsychology. *Behavior, and Social Networking*, *25*(8), pp. 479–480.

Wu J., Lin K., Lin D., Zheng Z., Huang H .and Zheng Z. (2023). Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *Open Journal of the Computer Society*, *4*, 37–49.

Zaitsev, O. A. (2024). Features of criminal-procedural evidence in the context of digitalization. J*ournal of Russian Law*, *8*, 93–112. https://doi.org/10.61205/S160565900030639-6

Authors information



Marina A. Efremova – Dr. Sci. (Law), Professor, Head of the Department of Criminal-legal Disciplines, Kazan branch of Lebedev Russian State University of Justice
Address: 7a 2nd Azinskaya Str., 420088 Kazan, Russia
E-mail: crimlaw16@gmail.com
ORCID ID: https://orcid.org/0000-0003-1076-2765
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57189299773
WoS Researcher ID: https://www.webofscience.com/wos/author/rid/E-6250-2016
Google Scholar ID: https://scholar.google.com/citations?user=mLPofnMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=630526

Evgeniy A. Russkevich – Dr. Sci. (Law), Associate Professor, Professor of the Department of Criminal Law, Kutafin Moscow State Law University
Address: 9 Sadovaya-Kudrinskaya Str., 125993 Moscow, Russia
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
WoS Researcher ID: https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=539093

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 declare 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 – March 8, 2025
Date of approval – March 26, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:343.9:004.9
EDN: https://elibrary.ru/ypsxqo
DOI: https://doi.org/10.21202/jdtl.2025.8

Уголовно-правовые проблемы противодействия преступности в метавселенной: современное состояние и перспективы развития

Марина Александровна Ефремова ✉

Российский государственный университет правосудия имени В. М. Лебедева, Москва, Россия

Евгений Александрович Русскевич

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Москва, Россия

Ключевые слова

аватар,
виртуальность,
киберпреступность,
криминология,
метавселенная,
право,
преступность,
уголовная ответственность,
уголовное право,
цифровые технологии

Аннотация

Цель: исследование направлено на комплексный анализ уголовно-правовых рисков, возникающих в контексте развития метавселенной как нового цифрового пространства социального взаимодействия, определение понятия метавселенной и оценку возможностей противодействия преступной деятельности в данной среде средствами уголовного права.

Методы: методологию исследования составили диалектический метод научного познания, методы анализа и синтеза, а также совокупность специальных юридических методов. Применялся системный подход к изучению правовых явлений в цифровой среде, сравнительно-правовой метод для анализа зарубежного опыта, формально-юридический – для толкования нормативных актов и доктринальных положений.

Результаты: установлено, что привлекательность метавселенной для различных форм преступной деятельности в значительной степени обусловлена анонимностью пользователей и отсутствием четкого правового режима. Исследование показало, что на платформах метавселенной уже совершаются многочисленные преступления: общественно опасные деяния, связанные с распространением криминогенной и психотравмирующей информации, хищения цифрового имущества, преступная легализация доходов, посягательства против половой неприкосновенности личности. Выявлены системные проблемы противодействия преступности в метавселенной, включая территориальную юрисдикцию, идентификацию пользователей и процессуальные сложности доказывания.

✉ Корреспондирующий автор

Научная новизна: проведен комплексный анализ уголовно-правовых аспектов функционирования метавселенной. Сформулированы теоретические подходы к квалификации преступлений, совершаемых в виртуальном пространстве, обоснована необходимость разработки специальных правовых конструкций для регулирования отношений в метавселенной. Предложена концепция многомерной модели правовой охраны отношений в метавселенной, основанной на государственно-частном партнерстве.

Практическая значимость: результаты исследования могут быть использованы при совершенствовании уголовного законодательства в части регламентации ответственности за преступления, совершаемые в цифровом пространстве, разработке концепции правового регулирования метавселенной, создании механизмов государственно-частного партнерства в сфере противодействия киберпреступности. Полученные выводы актуальны для правоприменительной практики при расследовании преступлений, совершенных с использованием технологий виртуальной реальности.

Для цитирования

Ефремова, М. А., Русскевич, Е. А. (2025). Уголовно-правовые проблемы противодействия преступности в метавселенной: современное состояние и перспективы развития. *Journal of Digital Technologies and Law*, *3*(2), 187–202. https://doi.org/10.21202/jdtl.2025.8

Список литературы

Бегишев, И. Р., Денисович, В. В., Сабитов, Р. А., Пасс, А. А., Скоробогатов, А. В. (2023). Уголовно-правовое значение метавселенных: коллизии в праве. *Правопорядок: История, Теория, Практика*, *4*(39), 58–62. EDN: https://elibrary.ru/hehwgn. DOI: https://doi.org/10.47475/2311-696x-2023-39-4-58-62

Грибунов, О. П., Никонов, П. В., Пархоменко С. В., Рогова, Е. В. Шиханов, В. Н. (2023). *Цифровая валюта и цифровые финансовые права как предмет и средство совершения преступлений*. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации. EDN: https://www.elibrary.ru/ryrwsj

Зайцев, О. А. (2024). Особенности уголовно-процессуального доказывания в условиях цифровизации. *Журнал российского права*, *8*, 93–112. EDN: https://elibrary.ru/bjnfvn. DOI: https://doi.org/10.61205/S160565900030639-6

Хабриева, Т. Я. (2018). Право перед вызовами цифровой реальности. *Журнал российского права*, *9*(261), 5–16. EDN: https://elibrary.ru/ozgiav. DOI: https://doi.org/10.12737/art_2018_9_1

Хаванова, И. А. (2024). Метавселенная: проблема адаптации налогово-правовых конструкций. *Журнал российского права*, *7*, 78–93. EDN: https://elibrary.ru/ejrgxj. DOI: https://doi.org/10.61205/S160565900029634-1

Alawadhi, I. M. (2023). *Future Cybercrimes in the Metaverse: A Comprehensive Forecast*. In H. Elshenraki (Ed.), Forecasting Cyber Crimes in the Age of the Metaverse (pp. 24–32). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-0220-0.ch002

AlMutawa, A., Ikuesan, R. A., & Said, H. (2024). Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model. *Future Internet*, *16*(12), 437. EDN: https://elibrary.ru/yoousp. DOI: https://doi.org/10.3390/fi16120437

AL-Tkhayneh, K. M., Olowoselu, A., & Alkrisheh, M. A. (2023). The Crime in Metaverse (the Future Scenarios for Crime Patterns and the Prospective Legal Challenges). In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, United Arab Emirates* (pp. 1–6). https://doi.org/10.1109/snams60348.2023.10375402

Bhardwaj, A. (2024). *Cyber Fraud Use Cases in the Metaverse. In Beyond the Realms: Navigating the Metaverse* (pp. 106–130). Bentham science publishers. https://doi.org/10.2174/9789815238457124010007

Blake, J. (2024). Online Crime in the Metaverse: A Study on Classification, Prediction, and Mitigation Strategies. In H. N. Elshenraki (Ed.), *Forecasting Cyber Crimes in the Age of the Metaverse* (pp. 66–77). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch004

Chawki, M., Basu, S., & Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, *13*(3), 33. EDN: https://elibrary.ru/ssccdc. DOI: https://doi.org/10.3390/laws13030033

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*, 467–494. EDN: https://elibrary.ru/bvvoth. DOI: https://doi.org/10.1365/s43439-022-00056-9

Duranske, B. T. (2008). *Virtual Law. Navigating the Legal Landscape of Virtual Worlds*. Chicago, Illinois: ABA Publishing, American Bar Association.

Fairfield, J. A. T. (2012). Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life. *Berkeley Technology Law Journal*, *27*, 55.

Gómez-Quintero, J., Johnson, Sh. D., Borrion, H., & Lundrigan, S. (2023). *A scoping study of crime facilitated by the metaverse*. https://doi.org/10.31235/osf.io/x9vbn

Lewandowsky, P. (2024). Cybercrime in the Meta-Universe. *Journal of Social Science and Humanities*, *6*(8), 5–8. EDN: https://elibrary.ru/kbjojn. DOI: https://doi.org/10.53469/jssh.2024.06(08).02

Lin, K.-X., Wu, J., Lin, D., & Zheng, Z. (2023). A Survey on Metaverse: Applications, Crimes and Governance. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan* (pp. 541–549). https://doi.org/10.1109/metacom57706.2023.00097

Marshall, A. M., & Tompsett, B. (2023). The metaverse – Not a new frontier for crime. *WIREs Forensic Science*, *6*(1), e1505. EDN: https://elibrary.ru/eilnzh. DOI: https://doi.org/10.1002/wfs2.1505

Mooij, A. (2024). *Regulating the Metaverse Economy*. Springer. https://doi.org/10.1007/978-3-031-46417-1

Narasimhan, P., & Kala, N. (2024). Securing the Metaverse: AI-Driven Solutions for Cyber Security, Privacy, and User Trust. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 1890–1918. EDN: https://elibrary.ru/vakoem. DOI: https://doi.org/10.32628/cseit241061238

Qin, H. X., Wang, Y. & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanit Soc Sci Commun*, *12*, 194. https://doi.org/10.1057/s41599-024-04266-w

Saharan, S., Singh, S., Bhandari, A. K., & Yadav, B. (2024). The Future of Cyber-Crimes and Cyber War in the Metaverse. In H. N. Elshenraki (Ed.), *The Age of the Metaverse* (pp. 126–148). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch007

Singh, P. P. (2024). Cyber Crimes in Metaverse. *International Journal of Science and Research*, *13*(2). EDN: https://elibrary.ru/ulmpvh. DOI: https://doi.org/10.21275/mr24130195237

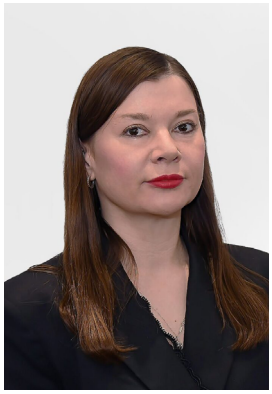
Teodorov, A.-V. (2023). Cybercrimes in the Metaverse: Challenges and Solutions. In *International Conference on Cybersecurity and Cybercrime*, 10 (pp. 209–215). https://doi.org/10.19107/cybercon.2023.28

Wasswa, S. (2023). Predicting Future Cybercrime Trends in the Metaverse Era. In H. N. Elshenraki (Ed.), *Forecasting Cyber Crimes in the Age of the Metaverse* (pp. 78–113). IGI Global. EDN: https://elibrary.ru/swgaya. DOI: https://doi.org/10.4018/979-8-3693-0220-0.ch005

Wiederhold, B. K. (2022). Sexual harassment in the metaverse. Cyberpsychology. *Behavior, and Social Networking, 25*(8), 479–480. EDN: https://elibrary.ru/hocuqv. DOI: https://doi.org/10.1089/cyber.2022.29253.editorial

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *IEEE Open Journal of the Computer Society*, *4*, 37–49. https://doi.org/10.1109/ojcs.2023.3245801

Сведения об авторах



Ефремова Марина Александровна – доктор юридических наук, профессор, заведующий кафедрой уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия имени В. М. Лебедева
Адрес: 420088, Россия, г. Казань, ул. 2-я Азинская, 7а
E-mail: crimlaw16@gmail.com
ORCID ID: https://orcid.org/0000-0003-1076-2765
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57189299773
WoS Researcher ID: https://www.webofscience.com/wos/author/rid/E-6250-2016
Google Scholar ID: https://scholar.google.com/citations?user=mLPofnMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=630526

Русскевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, 9
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
WoS Researcher ID: https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=539093

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 являются членами редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

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: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 8 марта 2025 г.
Дата одобрения после рецензирования – 26 марта 2025 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.

Research article
UDC 34:004:343.9:004.7
EDN: https://elibrary.ru/gvmhzv
DOI: https://doi.org/10.21202/jdtl.2025.9

Judicial Reasoning as a Mechanism for the Legal Protection of Children Against Digital Sexual Abuse and Child Pornography

Yassin Abdalla Abdelkarim

Luxor Elementary Court, Luxor, Egypt
Leeds Beckett University, Leeds, United Kingdom

Keywords

child pornography,
childhood protection,
children's safety,
court decisions,
cyberspace,
digital technologies,
international law,
judicial reasoning,
law,
sexual abuse

Abstract

Objective: to examine the contribution of judicial reasoning to the legislation interpretation, which is aimed at strengthening the legal protection of children against child pornography and digital sexual abuse under the rapid development of cyberspace. The study eliminates the gap in scientific knowledge concerning the possibilities of judicial interpretation as an alternative to the slow process of legislative amendments.

Methods: the main methodological approach is the analysis of court decisions on child pornography and sexual abuse of children from 2018 to 2024. The author used comparative legal analysis and the study of judicial practice in various jurisdictions, including decisions of the European Court of Human Rights, the courts of the USA, Great Britain and Ireland. The research is based on a conceptual analysis of the principle of the child's best interests and its application in judicial practice.

Results: the author proved that judicial reasoning is an effective mechanism for overcoming the limitations of legislative formulations in protecting children from online exploitation. The key areas of judicial reasoning were identified: the expansion of the child pornography concept, the inclusion of contactless forms of sexual abuse, the use of digital technologies to collect evidence, and the priority of the concept of the child's best interests over procedural restrictions. The research confirmed the ability of judicial reasoning to create legal precedents that ensure a more flexible and effective application of existing legislation.

Scientific novelty: for the first time, the article comprehensively investigated the role of judicial reasoning as a tool for the dynamic interpretation of legal norms of protecting children from digital sexual abuse. The author developed a conceptual model of the interaction between judicial reasoning and the principle of the child's best interests. The study reveals mechanisms of overcoming legislative stagnation through judicial interpretation of legal norms related to modern forms of child pornography in cyberspace.

Practical significance: The study results can be used in judicial practice to substantiate decisions in cases of child pornography, in law-making activities to improve childhood protection standards, and in the practice of law enforcement agencies. The conclusions help to form a more effective justice system that takes into account children's interests. The research can serve as a basis to develop methodological recommendations on using judicial reasoning in cases of minors' protection.

For citation

Abdelkarim, Ya. A. (2025). Judicial Reasoning as a Mechanism for the Legal Protection of Children Against Digital Sexual Abuse and Child Pornography. *Journal of Digital Technologies and Law, 3*(2), 203–221. https://doi.org/10.21202/jdtl.2025.9

Contents

Introduction

Being the golden core of society, international and domestic legal rules grant children a particular protection that suits their natural weaknesses and inexperience. This legislative protection is a part and parcel of legal systems and shares similar perspectives universally. Nevertheless, the ongoing evolution of communications created a distinctive sphere of human interaction, which is cyberspace. The easy access to this sphere enabled children to use it as a chief method to contact their society members. The immaturity

of children and their inexperience with Internet dangers lured criminals to exploit them to produce illicit online materials, i.e., child pornography. These vulnerabilities qualified children to be targeted by those criminals to achieve perpetrative purposes. Therefore, due to their stagnation and strict wordiness, existing legislation did not suffice to confront this modernised shape of crime because limiting legal interpretation to the direct understanding of legal rules and texts fell apart from providing children with the appropriate protection. Furthermore, the slowness of the legislation amending process makes legal rules incapable of confronting the daily-evolved child pornography.

Therefore, the effectiveness of child legal protection requires support from a rapidly evolving mechanism of legal rule interpretation. A mechanism that can handle each case per se regardless of the status of the legal code. This mechanism is judicial reasoning, which means the judges' utilisation of their interpretive and logical skills to understand and illustrate a legal text according to the circumstances of a single case. Judicial reasoning enables judges to develop legal notions that exceed the wording of legal texts to apply them appropriately in litigation. It is a multi-dimensional method of interpreting legislation according to the circumstances of each case, maintaining its applicability and preventing its uselessness. Judicial reasoning crystalises the judges' successful merging of their knowledge of the law, logical thinking skills, and their realisation of the litigation factual backgrounds. Hence, it is a unique judicial tool to maintain the integrity of legislation by guaranteeing its applicability in litigation.

Bearing in mind the rapidly evolving online child sexual abuse, the research proves the validity of judicial reasoning to provide a suitably developed legislative interpretation regarding child pornography. By judicial reasoning, judges can determine the best interpretation of legislation and transcend the wording of its text to apply a developed legal notion that suits the litigation object. To achieve to research objective, it reviews several judgments of child pornography and child sexual abuse to conclude the judges' approaches to interpreting existing legal rules according to a single case per se. These legal notions are the results of judicial reasoning, which overcomes the deadlock of the current legislation.

1. Child Pornography as a Phenomenon of Evil

The preamble of the 1989 UN Convention on the Rights of the Child (CRC) clarifies the universal obligation to maintain the dignity and humanitarian life of world children. It grants them a specific protection that suits their natural physical and legal weaknesses. By virtue, the Convention prohibits certain activities damaging children's humanitarian well-being. In particular, the Convention calls on states to prevent engaging minors in sexual abuse activities to defend their natural purity which goes against the exploitative feature of those acts (CRC, art. 19). Emphasising the severity of these acts, General

Comment No. 25 (2021, para. 3) points out the primary of providing children with a safe digital environment. The Comment mentions the State Parties' obligations to prevent child sexual abuse glaringly to protect their existence in cyberspace (ibid, paras. 112–113). Thus, these international legal instruments are obvious concerning the prohibition of child sexual abuse, of which child pornography is the major sort.

2. Literature Analysis

The gravity of child pornography drove scholars to analyse and review it from criminal and psychological perspectives. It is referred to as sexual acts including exploitation of a child for the interest of the abuser or another person (Kirk-Provencher & Jeglic, 2023). This conception reflects the core pillars of child pornography:

– acts of a sexual nature, which means engaging minors in sexual contact, regardless of their consent or physical grooming,

– the abused child, who are minors below 18 years old,

– the abuser, who owns power over the victim that enables him to lead the sexual exploitation of the victim,

– and the benefitted, who makes use of child pornography either financially or morally.

It is noted that the rapid evolution of cyberspace communications has increased the ratio of child pornography because its openness facilitated the offenders' reachability to their victims. The offenders manage to exploit innovative technologies, such as avatars and AI software, to catch children online and drive them deep into the darkness of sexual abuse (Noll & Roitman, 2023). Online exploitation jeopardises providing children with a safe environment in cyberspace. Furthermore, the anonymity of internet users grants offenders a powerful camouflage which enables them to broaden their activity sphere universally (Noll & Roitman, 2023). In this case, the child's curiosity to meet strangers is the abusers' golden key to trapping the victims. Nevertheless, cyberspace facilitates legal proceedings against those offenders as it permits law authorities to operate for gathering digital evidence on sexual abuses of children (KletečkaPulker et al., 2023), which enhances prosecutions of the perpetrators and the victims' access to justice. Judicial authorities have succeeded in integrating technologies into legal proceedings, enabling police officers, prosecutors, and judges to search various digital environments for evidence of illegal child sexual abuse to establish the perpetrators' accountability for their deeds and limit their impunity.

Acts including sexual usings of a child are a solid category of child abuse because they contradict the childhood inreadiness for sexual relations (Brunton, 2023). In addition, engaging minors in sexual activities violates society's standards of these activities, which elevates them to be considered child abuse. Brunton (2023) argues that an abused

child usually does not understand the illicit core of the activity and cannot express full obvious consent about it. He notably mentions that 20,4 % of North American children, 28.8 % of Australian children, 18.9 % of African children and 22.4 % of South American children were sexually abused in 2021 (Brunton, 2023). These figures reflect the universal widespread of this evil act against children, which inflicts physical and psychological harm on them. Sexual abuse could have traumatic impacts on a child's mentality and personality because it jeopardises children's conceptions of mortality and appropriate sexual behaviour (Brunton, 2023). Sexualization of childhood deprives the victims of their trust in the protection provided by law and society and taints their purity and innocence. This represents the brutal impact of pornography on children. Needless to say, engaging minors by force in sexual content inflicts severe damage on their physical and mental health; immediate death is a common consequence of this activity (Ali et al., 2024). Notable impacts on the psychological growth of the child's personality and social behaviour as a result of the heinous fear and anxiety the victims endure during the abuse. Moreover, the severity of the abuse consequences is affected by its manner, duration, and broadcast publicly or remains secret (Hébert & Langevin, 2023). All these factors formulate the futural portrait of the victims's social personality and mentality.

3. Contradiction to the Child's Best Interest Concept

Article 3 of the CRC obliges state parties to prioritise the child's best interest when organising their issues. Furthermore, Article 9 permits separating the child from his parents under the requirement of his best interest. This conventional conception of the child's best interest reflects the prominence of this concept regarding society's interactions with the child. This interest is the fundamental core of domestic and international child-relevant policies. Furthermore, General Comment No. 14 (2013) notes that this norm manifests the core values of the CRC because of its obligatory nature on state parties. De facto, granting the child's best interest a primary consideration establishes a legal and logical shield against violations of children's rights. In the same context, The European Commission clarifies that the concept of the best interest of the child (BIC) should be assessed as the primary consideration concerning international, regional, and domestic policies and strategies.[1] Article 24(2) of the Charter of Fundamental Rights of the European Union incorporates BIC to ensure the dignity and prosperity of the EU children. Affirming this concept, the Egyptian Child Law No. 12/1996 grants BIC the same primacy as the CRC (art 3c). Those legal instruments highlight BIC as a determinant of the validity and efficiency of governmental policies that affect children. By virtue, BIC occupies the same order concerning individuals' interactions with children. The legality of one's interaction with a child depends on the interactor's compliance with BIC; violating BIC criminalises the interaction.

[1] Best interests of the child (BIC) (European Commission: Migration and Home Affairs). https://clck.ru/3MGoCV

BIC manifests the deliberations taken into account when introducing services or products that concern children (Levesque, 2023). They are controlled by several determinants, e.g., the safety and well-being of the child. BIC serves to guarantee the maximum ratio of the child's favour versus other interests of the society members. To enhance this concept, jurisprudence developed the child's dynamic self-determinism to figure out a decision's compliance with BIC (Eekelaar, 2017; Levesque, 2023). Therefore, children are possessors of rights who are able to determine their best interests and represent their views to society. The purpose of this strategy is to enable abused children to speak out against their perpetrators, particularly in domestic abuse cases. BIC should have a broad legal conception that exceeds the mere maintenance of the child's life to guarantee its quality (Sorbie, 2021). Thus, BIC includes providing children with essential life needs, physical and psychological, through efficient mechanisms that enhance the appropriate quality of those needs.

The previous review of BIC explains how child pornography contradicts this concept. Engaging children in illicit activities, either by force or deception, does not accord with the pure nature of childhood because most of the victims might be unaware of the immorality of the content they have been exploited to produce. Child pornography transfers the victims to illicit productions to be offered solely in dark inhumane markets. According to the affirmed conception of BIC, children have no interest in such activities as they deprive children of the required emotional and social protection. Furthermore, the severe physical and psychological impacts of sexual interactions on children frustrate their normal social and mental growth and deprive them of engaging society as ordinary members. Child pornography introduces distorted personalities to society. Therefore, this evil deed jeopardises the child's well-being and safety which are fundamental values of the inner society. BIC, from a practical perspective, reflects a chief interest of the whole society because children are the core blocks of the society establishment. Consequently, BIC should be the primary legal interest of the whole society when confronting child pornography.

4. Enhancing the Protective Feature of Legal Rules Through the Judicial Reasoning

In general, judicial reasoning is the process by which judges arrive at a decision or judgment in a legal case through the analysis and interpretation of legal rules and the consideration of the case factual background. Judicial reasoning includes confrontation between judges and laws by creative rule-making to formulate a rule of decision or faithful adherence to the existing rules by rule-following approaches. Thus, judicial reasoning encompasses both creative rule-making and faithful rule-following. Judges play a crucial role in shaping legal principles while respecting existing authority. Their decisions impact individual cases and contribute to the evolution of legal doctrine. Judicial reasoning is

the art of balancing between antagonistic interests of litigation parties (Mańko, 2022) seeking the appropriate application of legal rules on the dispute. The judicial balancing between antagonists achieves social, legal, and political objectives since it promotes the trustworthiness of the national judiciary (Mańko, 2022). Therefore, judicial reasoning is the pulsing heart of the judicial process, which crystalizes the judges' knowledge of the law, efficient analytical skills, and capabilities to deliver the best interpretation of legislation.

5. Judicial Reasoning Supports the Best Interpretation of Legal Rules

Judicial reasoning is an effective shield for judges to defend the legitimacy of their rulings; it prevents arbitrary deciding of judgments because judges review the case facts through an analytical perspective under a well-established set of judicial decision-making mechanisms, which proves the judges' efficient knowledge of law and legal facts (Ravarani, 2019). A qualified judgment should be established on efficient reasoning. Furthermore, the judge's interpretation of the law according to each case's circumstances supports their endeavours to reveal the accurate legislative intentions behind the legal rules (Leszczyński, 2020). Those intentions are the true national motivation for the legislation which judges should consider when interpreting them within a specific case context. This approach prevents opportunities for judicial arbitralization or personalisation of their judgements, granting the judicial process an effective impartiality guarantee.

The European Court of Human Rights (ECHR) adopts the proportionality standard to establish the judges' reasoning in several cases. According to the ECHR, proportionality implies maintaining the balance between the individuals' protected legal interests and society's legitimate objectives[2]. Furthermore, proportionality in judicial reasoning strengthens the quality of justice introduced by the judgment (Jaeger, 2019) as it manifests a core pillar of legal certainty and enhances the fairness of the court's rulings. It also portrays the judges' logical analysis strength while interpreting legal rules and contextualising them within the case's factual background in a case-by-case manner.

A golden outcome of judicial reasoning is its support for curing legislative deficiencies through developing a case-by-case interpretation (Małolepszy & Głuchowski, 2023). Activating the judges' analytical and interpretive skills to contextualize a legal rule within litigation enhances overcoming linguistic and applicability difficulties and melts down the rigidity of legislative instruments. Therefore, judicial interpretation of legislation assigns a legislative job to the judges because of their contribution to creating an appropriate

[2] ECHR Annual Report. (2014). https://clck.ru/3MGoLh

and applicable understanding of the legislator's intent. It is a realistic judicial law-making process crystalising the judges' efforts to the accurate application of legal rules (Małolepszy & Głuchowski, 2023). Judicial reasoning and interpretation facilitate this judicial-legislative mission.

Mańko (2022) explains that judicial reasoning is a formulation of legal and logical stages. It begins with the identification of conflicting interests of the dispute parties and then analyzing them to determine the applicable legal rules. Afterwards, the judge should utilize his evaluation skills to find out the most appropriate interpretation of legal rules. Interpretation is the reason for the variety in legislation applications because it depends on the judge's understanding of them within the dispute context. The judge's analysis of the dispute entries contributes chiefly to this interpretation. Then, the judge determines the appropriate interpretive norm generated by this legal and logical judicial thinking mechanism to settle the litigation.

From this model, it is needless to say that judicial reasoning constitutes the generator of legislation interpretation; courts' judgements elaborate on the concepts texted within the legislation, legislative intentions, and their application mechanisms. Thus, judicial reasoning is the illustration of legal concepts. Accordingly, the legal concept of BIC finds its efficient interpretation within judgments on child litigations because those judgments considered BIC a primary when balancing the disputing interests. They constructed a shield of judicial protection for children against perpetrating abuse activities.

6. BIC Through a Judicial Lens

The research in this section reviews a handful of judgements on child pornography and other sexual abuse sorts. These case laws were selected under a criterion that guarantees their suitability to the study objective. The studied case laws are judgments on child pornography-related disputes. They are chronically limited to the period 2018 to 2024 to ensure the modernity of the research results in this rapidly developing area of concern. The analysis and process of scrutiny will determine the objects of these case laws. In addition, an analysis of the rulings will examine the grounds for the decision and the legal norms they entailed.

In AG v Williams (2023, paras. 6, 12), a case concerning child sexual abuse, the court discussed the principle of open justice. The judgment decided that the fundamental principle to administer justice in public is not absolute; the court can cast it away according to the plaintiff's interest. BIC implies that sexual abuse hearings should not be in public for the proper application of justice. Thus, it is the ultimate authority of the court to exclude public hearings in those cases[3]. Furthermore, the court preserved the power to limit publication in this case without prejudice to its authority to conduct private

[3] Crown Prosecution Service (CPS). (2019, 17 January). Hearings in Private ('In Camera'). https://clck.ru/3MGoSg

hearings (ibid, para. 20). both are management powers intended to provide the child with effective judicial protection. The fundamentality of the courts' protection for children authorizes granting them broad authority to conduct hearings in private (Forde, 2022). This authority is a procedural guarantee of child-friendly justice as it enshrouds the victim with a peaceful tranquil judicial environment that suits the child's psychological needs. The principle of children's private court hearings is a direct application of General Comment 24/2019 objective to provide them with effective justice.

Enhancing the protection of the child's psychology and reputation, the England and Wales Court of Appeal anonymised the names of the offender and the victim since they both were children. In Bai, R. v (2022) the judgment did not include the litigation parties' names but it referred to them with separate capitalised letters. Moreover, the court indicated that the severity of the child's crime should not deprive him of the specific legal protection concerning detention and other non-custodial measures (ibid. para. 17). it is a primary guideline of a paramount consideration. Thus, upon assuring the 1st instance court's compliance with the guideline, the appellate circuit dismissed the defendant's appeal. The same principle was adopted in Barker, R. v (2023). Thus, considering the child's detention guidelines is a chief pillar of children's judicial protection.

In State v Hunt (2020), the court reshaped the traditional understanding of the scope of the defendant's digital device search warrants. While detectives extracted child pornography materials from his laptop according to a search warrant, the defendant urged the court to dismiss this evidence because of the detectives' excess of the warrant scope. Specifically, he claimed that the warrant authorized the detectives to search "for" electronic devices, not search "of" them, which implies finding them and sending them to the ad hoc judicial body without exploring their contents. Consequently, the detectives' exploration and seizure of digital materials stored on the laptop is null and void and, with that, the court should not convict the defendant (ibid, p. 28). The invalidity of evidence-gathering procedures implies the defendant's acquittal according to fundamental legal logic. The court expressed a prima facie agreement with the defendant's argument since the traditional rules governing search warrants require ultimate compliance with their wording. Nonetheless, it refuted this argument as it decided that previous US judicial precedents indicated the fruitlessness of this argument; they authorised child pornography evidence revealed by detectives even though the warrant limited its scope to search "for" devices (ibid. p. 32). the severity of engaging minors in this illicit activity justified the court's excessive interpretation of the search warrant. BIC implies overcoming prima facie wording odds to enhance children's judicial protection.

Furthermore, the Alabama Court of Criminal Appeals in this case authorized tracking the suspect's IP address to gather evidence of child pornography (ibid, p.19). It could be understood that the court's reasoning contributed to evolving a suitable interpretation

of legislation to BIC, which reflects the prominence of this judgment. Judicial reasoning can recontextualise legal notions to achieve the objectives of BIC. This conclusion accords with the humanitarian mission of the judges. Similarly, a US court permitted using IP addresses to disclose the identity of child pornography perpetrators and reveal their locations for prosecution purposes (United States v Tagg, 2018, p. 3). Notwithstanding the judicial affirmation of the personal theme of the defendant's IP address (Sokol et al., 2020) because it represents its owner's personal data. Therefore, the utilisation of this technique at courts discloses judicial prioritisation of BIC by bypassing the offender's shallow interest in protecting his privacy, represented in the IP address, to reveal his identity and location, favouring the victim's BIC. The courts' attitude indicates the success of judicial reasoning in merging law and technology to achieve justice and the true concept of BIC. Judicial interpretation cures the failure of domestic legal systems to protect individuals' privacy on the Internet, regardless of the existing legislation (Gilman, 2021) because it contextualises privacy legal rules within a single litigation considering the unique perspectives of each case per se. the Court of Justice of the European Communities affirmed this notion in SpaceNet (Judgment) (2022, para. 100) as it transcended the legal protection of IP address entailed in Articles 7 and 8 of the EU Charter and permitted tracking the suspect's IP address in cases of the acquisition, dissemination, transmission or making available online of child pornography to combat sexual abuse of children.

Moreover, in United States v Tagg, the court considered that the mere possession of child pornography content reflects the defendant's intent to view and suffices to convict him (ibid, p.12; United States v Miltier, 2018, para. 85) under 18 U.S.C. § 2252 4(B).

In the same context, the court decided in United States v. Fall (2020) that using an intermediary device, owned by another person with bona fida, to temporarily store child pornography content constitutes illegal transportation of this content under 18 U.S.C. § 2252 (ibid, para. 396). Furthermore, the court concluded that possessing illicit content of minors on one hard drive and other materials on a separate drive does not constitute multiplicity; the judgment can punish the defendant for each actus reus per se (ibid, para. 374) as there was no overlapping between accusations. The court's conclusion accords with the US Supreme Court's explanation of criminal multiplicity in Rheuben Johnson v State of Kansas (2019, p. 10).

The judicial utilisation of technology against child pornography has rocketed glaringly. The 5th Circuit of the US Court of Appeals permitted using hash values coinciding as evidence (United States v. Reddick, 2018, para.639). The court indicated that matching online distributed child pornography hash values with those found on the defendant's devices suffices to conclude accountability. Hash values comparisons permit concluding the defendant's possession of child pornography with absolute certainty, which is the fruit of incorporating technologies into judicial interpretation.

The Court of Appeal in Northern Ireland Decisions, in Pacyno, R. v (2024), concluded that the gravity of creating online child pornography content aggravates the defendants' accountability (ibid, para. 13). The reason for this gravity is the exploitive feature of this activity, which inflicts an inherent harm on the victim. Accordingly, the accusation passes the custody threshold, justifying sentencing the defendants to three years in jail (ibid, para. 15). Considering the psychological harm, upon deciding the punishment, manifests an appropriate moral remedy for victims. Moreover, the anonymity of victims does not prevent the defendants' conviction. Because several child pornography materials image unknown victims, who might be unable to reach justice, the court permitted punishing the perpetrators regardless of the non-identification of victims (ibid, para. 19). Thus, the court's broad interpretation blocked a road to impunity based on the anonymity of online child pornography victims. This broad approach is represented in the court's affirmation of the criminalisation of the mere possession of minors' illicit materials victims (ibid, para. 40). The dependence of judicial reasoning on logic promotes the judges' utilisation of broad interpretive skills to strengthen judicial child protection.

In Director of Public Prosecutions v M. O'D (2022), the Irish Court of Appeal considered showing child pornography an aggravating condition of the rape offence that preceded committed by the victim's father (ibid, paras. 22, 33). The defendant's violation of parental responsibility duties justified the court's opinion because of the severe psychological harm he inflicted on the victim. This was a direct interpretation of the obligation included in Article 18 of the CRC on both parents to comply their endeavours in bringing up the child with BIC. Correspondingly, the court resentenced the defendant to 10-15 years imprisonment.

The US Court of Appeals 4th Circuit affirmed the mere criminalisation of engaging minors in sexual activities, including child pornography, disregarding the victim's consent or the offender's purpose (United States v. McCauley, 2020, para. 694). It is established that child consent does not prevent the offender's punishment; the child's protection considerations justify neglecting the minor's expression of consent (Featherstone, 2021). England and Wales Court of Appeal disregarded the child's consent because of the victim's immaturity and lack of life experience (R v BHL, 2023, para. 10). Thus, the court does not mitigate the original sentence on the basis of the victim's responsive reaction to the sexual abuse; expressing no resistance by the minor does not constitute a legal consent on the sexual activity. Furthermore, requiring the offender's purpose to convict him restricts attributability in child pornography crimes, which frustrates justice. Thus, the appellate court broadened the interpretation of the specific intent stipulated in 18 U.S.C. § 2251. This intent is found in any moment of the deliberate imaging the child sexual abuse. Then, the prosecution authority is not required to establish evidence of the

offender's intent to produce and distribute illicit child materials (ibid, para. 697). The broad interpretation of this legal text is necessary to enhance the child's judicial protection as it enables judges to overcome legislative wording deadlocks; the supportive effect of the latter for the perpetrators' impunity is needless to say.

Child pornography might not include direct engagement of minors in sexual activities; it might occur without physical contact with the victim (O (Description of Sexual Abuse), 2024, para. 20). Consequently, exposing children to adult pornographic content, even though unintentionally, constitutes sexual abuse under the UK Children Act 1989 (Section 31 (9)) that drove the court to replace the victim's care from her parents to her grandparents. The carers' behaviour violated childcare basics as they did not take proper measures to prevent the victim's exposure to adult pornography (O (Description of Sexual Abuse), 2024, paras. 33, 36). The judgment, through this interpretation, developed the NSPCC Guidance (§ 26)[4] about children's sexual abuse by adding non-contact activities to this category. According to the court, the Guidance wording does not include newly created sorts of children's sexual abuse which compelled the court to overcome the Guidance direct illustration to cover acts that did not contain direct contact with the victim (O (Description of Sexual Abuse), 2024, paras. 43, 45). The ECHR confirmed the illegality of distributing pornography to children and the urgent need to limit online porn products to adults (PRYANISHNIKOV v. RUSSIA, 2019, para. 61). Thus, physical contact is no longer required to prove child sexual abuse, which enhances children's judicial protection.

In R.B. v. Estonia (2021), the ECHR decided the insufficiency of civil child protection proceedings to defend the victim against sexual abuse (ibid, para. 61). Child sexual abuse is a heinous crime that requires urgent proceedings of criminal law nature. Therefore, in custody litigation, states should provoke criminal investigation proceedings about child sexual abuse allegations. Ancillary investigations by the civil court are not enough against this criminal act. The court vividly indicated that BIC requirements imply this decision under CRC (ibid, paras. 69, 71); an approach to effective child-friendly justice (ibid, para. 88). Thus, BIC is judicially considered the cornerstone of child-friendly justice.

To sum up, the identified judgments enhanced the concept of BIC through judicial reasoning. They merged technical tools and interpretive skills with the existing legal rules to overcome the evolving nature of child pornography and the stagnation of domestic legislation. Therefore, they established a unique mechanism to protect children online, based on judicial reasoning. This mechanism has a flexible theme that adapted the national judiciaries to the technical nature of child pornography and enhanced the national

[4] National Society for the Prevention of Cruelty to Children. https://goo.su/bwhWVsv

courts' ability to prioritise BIC. Consequently, cyberspace has become safer and more secure for children because of overcoming the shortcomings of the relevant legislation. Furthermore, judicial reasoning proves that the prominent theme of the judges' contribution to confronting child pornography is innovation, which enabled them to overcome the legislation stagnation concerning this activity by developing an appropriate understanding of legislation according to each case circumstance. This is the core of judicial reasoning that manifests its contribution to contextualising BIC in legal practice.

Conclusion

In conclusion, the research points out the gravity of online child sexual abuse by engaging innocent minors in child pornography. It is an illicit criminal act violating the purity and innocence of childhood. Because it degrades children's well-being, international legal instruments and national laws prohibit child pornography, ensuring that preventing child sexual abuse is a BIC. This concept is the determinant factor of all policies and decisions that concern the child; its enhancement is the chief objective of judicial and legislative policies.

The research concludes that an ongoing legislation amending process to confront child pornography is not required because judicial reasoning bridges practical gaps caused by legal rules shortcomings. Reasoning delivers the most suitable interpretation of legislation to the judge. Thus, they can contextualise this interpretation within each case according to the concept of BIC. Judicial reasoning is the golden key to overcoming legislation stagnation concerning evolving child pornography. The previewed judgments are evidence of this conclusion because they crystalised the judges' endeavours to reach the perfect application of legal rules in light of the BIC concept.

References

Ali, S., Anwar Pasha, S., Cox, A., & Youssef, E. (2024). Examining the short and long-term impacts of child sexual abuse: a review study. *SN Social Sciences*. https://doi.org/10.1007/s43545-024-00852-6

Brunton, R. (2023). Child Abuse: Definitions, Prevalence, and Considerations in Assessment and. In R. Brunton, & R. Dryer (Eds.), *Perinatal Care and Considerations for Survivors of Child Abuse*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-33639-3_2

Eekelaar, J. (2017). The interests of the child and the child's wishes: The role of dynamic self-determinism. In U. Kilkelly, *Children's rights* (1st ed., pp. 129–148). London: Routledge. https://doi.org/10.4324/9781315095769-8

Featherstone, L. (2021). *Sexual Violence in Australia, 1970s–1980s: Rape and Child Sexual Abuse*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-73310-0

Forde, L. (2022). The role of the courts in protecting children's rights in the context of police questioning in Ireland and New Zealand. *The Howard Journal of Crime and Justice*, *61*, 240–260. https://doi.org/10.1111/hojo.12472

Gilman, M. E. (2021). Feminism, Privacy, and Law in Cyberspace. In D. L. Brake et al. *The Oxford Handbook of Feminism and Law in the United States*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197519998.013.36

Hébert, M., & Langevin, R. (2023). Child Sexual Abuse. In R. J. R. Levesque (Ed.). *Encyclopedia of Adolescence*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-32132-5_235-3

Jaeger, M. (2019). The EU Judiciary in a New Era of Accountability. In G. Selvik et al. (Eds.). *The Art of Judicial Reasoning*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-02553-3_8

Kirk-Provencher, K. T., & Jeglic, E. L. (2023). Child Maltreatment: Child Sexual Abuse. In T. K. Shackelford (Ed.). *Encyclopedia of Domestic Violence*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-85493-5_1871-1

KletečkaPulker, M., Doppler, K., VölklKernstock, S., Fischer, L., Eitenberger, M., Mussner, M., Klomfar, S., MoraTheuer, E. A., Grylli, C., Atanasov, A. G., & GreberPlatzer, S. (2023). Influence of various factors on the legal outcome of cases of child abuse – experiences gathered at an interdisciplinary forensic examination centre in Vienna, Austria. *International Journal of Legal Medicine*, 138, 3–14. https://doi.org/10.1007/s00414-023-03094-y

Leszczyński, L. (2020). ExtraLegal Values in Judicial Interpretation of Law: A Model Reasoning and Few Examples. *International Journal for the Semiotics of Law*, 33, 1073–1087. https://doi.org/10.1007/s11196-020-09773-y

Levesque, R. J. R. (2023). Best Interests of the Child. In *Encyclopedia of Adolescence*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-32132-5_666-2

Małolepszy, M., & Głuchowski, M. (2023). Judicial LawMaking in the Criminal Decisions of the Polish Supreme Court and the German Federal Court of Justice: A Comparative View. *International Journal for the Semiotics of Law*, *36*, 1147–1184. https://doi.org/10.1007/s11196-023-09969-y

Mańko, R. (2022). Judicial DecisionMaking, Ideology and the Political: Towards an Agonistic Theory of Adjudication. *Law and Critique*, *33*, 175–194. https://doi.org/10.1007/s10978-021-09288-w

Noll, J. G., & Roitman, M. (2023). Applying Innovative Methods to Advance the Study of Youth At-Risk for Internet-Initiated Victimization. In C. E. Shenk (Ed.), *Innovative Methods in Child Maltreatment Research and Practice, Child Maltreatment Solutions Network*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-33739-0_3

Ravarani, G. (2019). Some Reflections on the Legitimacy of the Strasbourg Judge. In G. Selvik et al. (Eds.). *The Art of Judicial Reasoning*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-02553-3_10

Sokol, P., Rozenfeldov, L., Lucivjanska, K., & Harasta, J. (2020). IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic. *Forensic Science International: Digital Investigation*, *32*, 300918. https://doi.org/10.1016/j.fsidi.2020.300918

Sorbie, A. (2021). Children's best interests and parents' views: Challenges from medical law. *Journal of Social Welfare and Family Law*, *43*(1), 23–41. https://doi.org/10.1080/09649069.2021.1876306

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice; LLM Master of Laws, Leeds Law School, Leeds Beckett University
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt; LS1 3HE, City Campus, Leeds, United Kingdom
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

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 – April 8, 2025
Date of approval – April 24, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:343.9:004.7
EDN: https://elibrary.ru/gvmhzv
DOI: https://doi.org/10.21202/jdtl.2025.9

Судебная аргументация как механизм правовой защиты детей от цифрового сексуального насилия и детской порнографии

Яссин Абдалла Абделькарим

суд общей юрисдикции в Луксоре, г. Луксор, Египет
Лидский университет Беккета, г. Лидс, Великобритания

Ключевые слова

безопасность детей,
детская порнография,
защита детей,
киберпространство,
международное право,
право,
сексуальное насилие,
судебная аргументация,
судебные решения,
цифровые технологии

Аннотация

Цель: исследование направлено на изучение вклада судебной аргументации в толкование законодательства для усиления правовой защиты детей от детской порнографии и цифрового сексуального насилия в условиях быстрого развития киберпространства, устраняя тем самым пробел в научном знании о возможностях судебного толкования как альтернативы медленному процессу внесения законодательных поправок.

Методы: в качестве основного методологического подхода применен анализ судебных решений по делам о детской порнографии и сексуальном насилии над детьми за период с 2018 по 2024 г. Использованы методы сравнительно-правового анализа, изучения судебной практики различных юрисдикций, включая решения Европейского суда по правам человека, судов США, Великобритании и Ирландии. Исследование основывается на концептуальном анализе принципа наилучших интересов ребенка и его применения в судебной практике.

Результаты: установлено, что судебная аргументация представляет собой эффективный механизм преодоления ограниченности законодательных формулировок при защите детей от онлайн-эксплуатации. Выявлены ключевые направления судебного толкования: расширение понятия детской порнографии, включение бесконтактных форм сексуального насилия, применение цифровых технологий для сбора доказательств, приоритет концепции наилучших интересов ребенка над процедурными ограничениями. Доказана способность судебной аргументации создавать правовые прецеденты, обеспечивающие более гибкое и эффективное применение существующего законодательства.

Научная новизна: впервые комплексно исследована роль судебной аргументации как инструмента динамического толкования правовых норм в сфере защиты детей от цифрового сексуального насилия. Разработана концептуальная модель взаимодействия судебного толкования с принципом наилучших интересов ребенка. Выявлены механизмы преодоления законодательного застоя через судебную интерпретацию правовых норм применительно к современным формам детской порнографии в киберпространстве.

Практическая значимость: результаты исследования могут быть использованы в судебной практике для обоснования решений по делам о детской порнографии, в законотворческой деятельности при совершенствовании норм защиты детей, в правоприменительной практике правоохранительных органов. Выводы работы способствуют формированию более эффективной системы правосудия, учитывающей интересы детей, и могут служить основой для разработки методических рекомендаций по применению судебной аргументации в делах о защите несовершеннолетних.

Для цитирования

Абделькарим, Я. А. (2025). Судебная аргументация как механизм правовой защиты детей от цифрового сексуального насилия и детской порнографии. *Journal of Digital Technologies and Law*, *3*(2), 203–221. https://doi.org/10.21202/jdtl.2025.9

Список литературы

Ali, S., Anwar Pasha, S., Cox, A., & Youssef, E. (2024). Examining the short and long-term impacts of child sexual abuse: a review study. *SN Social Sciences*. https://doi.org/10.1007/s43545-024-00852-6

Brunton, R. (2023). Child Abuse: Definitions, Prevalence, and Considerations in Assessment and. In R. Brunton, & R. Dryer (Eds.), *Perinatal Care and Considerations for Survivors of Child Abuse*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-33639-3_2

Eekelaar, J. (2017). The interests of the child and the child's wishes: The role of dynamic self-determinism. In U. Kilkelly, *Children's rights* (1st ed., pp. 129–148). London: Routledge. https://doi.org/10.4324/9781315095769-8

Featherstone, L. (2021). *Sexual Violence in Australia, 1970s–1980s: Rape and Child Sexual Abuse*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-73310-0

Forde, L. (2022). The role of the courts in protecting children's rights in the context of police questioning in Ireland and New Zealand. *The Howard Journal of Crime and Justice*, *61*, 240–260. https://doi.org/10.1111/hojo.12472

Gilman, M. E. (2021). Feminism, Privacy, and Law in Cyberspace. In D. L. Brake et al. *The Oxford Handbook of Feminism and Law in the United States*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197519998.013.36

Hébert, M., & Langevin, R. (2023). Child Sexual Abuse. In R. J. R. Levesque (Ed.). *Encyclopedia of Adolescence*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-32132-5_235-3

Jaeger, M. (2019). The EU Judiciary in a New Era of Accountability. In G. Selvik et al. (Eds.). *The Art of Judicial Reasoning*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-02553-3_8

Kirk-Provencher, K. T., & Jeglic, E. L. (2023). Child Maltreatment: Child Sexual Abuse. In T. K. Shackelford (Ed.). *Encyclopedia of Domestic Violence*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-85493-5_1871-1

KletečkaPulker, M., Doppler, K., VölklKernstock, S., Fischer, L., Eitenberger, M., Mussner, M., Klomfar, S., MoraTheuer, E. A., Grylli, C., Atanasov, A. G., & GreberPlatzer, S. (2023). Influence of various factors on the legal outcome of cases of child abuse – experiences gathered at an interdisciplinary forensic examination centre in Vienna, Austria. *International Journal of Legal Medicine*, 138, 3–14. https://doi.org/10.1007/s00414-023-03094-y

Leszczyński, L. (2020). ExtraLegal Values in Judicial Interpretation of Law: A Model Reasoning and Few Examples. *International Journal for the Semiotics of Law*, 33, 1073–1087. https://doi.org/10.1007/s11196-020-09773-y

Levesque, R. J. R. (2023). Best Interests of the Child. In *Encyclopedia of Adolescence*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-32132-5_666-2

Małolepszy, M., & Głuchowski, M. (2023). Judicial LawMaking in the Criminal Decisions of the Polish Supreme Court and the German Federal Court of Justice: A Comparative View. *International Journal for the Semiotics of Law*, *36*, 1147–1184. https://doi.org/10.1007/s11196-023-09969-y

Mańko, R. (2022). Judicial DecisionMaking, Ideology and the Political: Towards an Agonistic Theory of Adjudication. *Law and Critique*, *33*, 175–194. https://doi.org/10.1007/s10978-021-09288-w

Noll, J. G., & Roitman, M. (2023). Applying Innovative Methods to Advance the Study of Youth At-Risk for Internet-Initiated Victimization. In C. E. Shenk (Ed.), *Innovative Methods in Child Maltreatment Research and Practice, Child Maltreatment Solutions Network*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-33739-0_3

Ravarani, G. (2019). Some Reflections on the Legitimacy of the Strasbourg Judge. In G. Selvik et al. (Eds.). *The Art of Judicial Reasoning*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-02553-3_10

Sokol, P., Rozenfeldov, L., Lucivjanska, K., & Harasta, J. (2020). IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic. *Forensic Science International: Digital Investigation*, *32*, 300918. https://doi.org/10.1016/j.fsidi.2020.300918

Sorbie, A. (2021). Children's best interests and parents' views: Challenges from medical law. *Journal of Social Welfare and Family Law*, *43*(1), 23–41. https://doi.org/10.1080/09649069.2021.1876306

Сведения об авторе

Абделькарим Яссин Абдалла – судья, Суд общей юрисдикции в Луксоре, Министерство юстиции Республики Египет; магистр права, Школа права в Лидсе, Лидский университет Беккета
Адрес: Египет, Сохаг, 82516, Мадинат Насер, ул. Ахмим Сохаг, ул. Нью Касалови Отель; Великобритания, Лидс, городской кампус, LS1 3HE
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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 8 апреля 2024 г.
Дата одобрения после рецензирования – 24 апреля 2024 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.

Research article
UDC 34:004:341.3:004.8
EDN: https://elibrary.ru/ifibfo
DOI: https://doi.org/10.21202/jdtl.2025.10

Technology Transfer in the Era of Military Conflict: Legal Challenges for International Trade and International Humanitarian Law

Nisha Bhaskar
West Bengal National University of Juridical Sciences, Kolkata, India

Jackson Simango Magoge
National Institute of Transport, Dar es Salaam, Tanzania

Sayed Qudrat Hashimy
University of Mysore, Mysore, India

Keywords

artificial intelligence,
digital technologies,
Geneva Conventions,
Hague Conventions,
international humanitarian law,
international trade,
law,
military law,
technology transfer,
warfare means

Abstract

Objective: to identify the complex relations between international trade and military law in the context of technology transfer; to analyze the legal implications of technology transfers for international humanitarian law in order to clarify the impact of technology transfer in international trade on the warfare means regulation and identify legal gaps in existing international conventions.

Methods: the study uses a comprehensive legal analysis of international documents, including the Geneva Conventions and their Additional Protocols, the Hague Conventions, and modern international agreements in the field of trade and technology. The authors used comparative legal method to study the national legislations of various states and a systematic approach to analyze the interaction of international humanitarian law and international trade law.

Results: the study revealed significant legal gaps in regulating the transfer of dual-use technologies during wartime. It was established that modern technologies, including artificial intelligence, autonomous weapons

Corresponding author

systems and cybernetic means, create a regulatory vacuum that undermines the effectiveness of existing international conventions. A significant technological gap between the Global North and South was demonstrated.

Scientific novelty: the work is the first comprehensive study of technology evolution in the context of international humanitarian law, with an emphasis on the need to develop special regulatory mechanisms. The authors present a conceptual model for the integration of technology transfer norms into the system of international disarmament treaties, taking into account the principles of proportionality and distinction.

Practical significance: the study proposes specific amendments to the articles of the Geneva Conventions, including the modification of Article 35(2) of Additional Protocol I to include new technologies and extend the requirements of Article 36 regarding legal reviews of technological transfers. The recommendations developed can serve as a basis for creating international monitoring mechanisms and increasing transparency in the field of military technology transfer.

For citation

Bhaskar, N., Magoge, J. S., & Hashimy, S. Q. (2025). Technology Transfer in the Era of Military Conflict: Legal Challenges for International Trade and International Humanitarian Law. *Journal of Digital Technologies and Law, 3*(2), 222–258. https://doi.org/10.21202/jdtl.2025.10

Contents

Introduction

Resource! It has always been the clash over the resources. Since the advent of the civilization, it has been the clash over the resources that has regulated its course. In the contemporary as it is the clash over the resource that is causing the wars and the uproars and all the disagreements. Whether it is the land resource as is the reason for fight between majority of the countries or the resources over the same such as water, minerals or biodegradable resources such as petroleum, the causation for the disagreement has been the resources per se. In the contemporary the bi-products of these resources have also caused the discourses and resultantly there have been conferences and conventions to provide a middle ground for their dispersal and usage (Kaldor, 1986). The production of weapons is one of the most resource consuming task. Every country invests a major chunk of their GDP for their military and defence expenditure and ironically the developing countries spend more of their share in military expenditure than the developed countries (Azam, 2020; Saeed, 2025). The major factors behind this investment are the conditions of the developing countries. They not only have to control and maintain their internal security and conditions but also have to cope with the developed countries and rapidly advancing technology. Also, they are more prone to be administered by the ICRC and the tenets of IHL as compared to the developed countries considering the lack of IHL's understanding by the military and the defence junta. However, with the advancement of the world trade and the strengthening of the multilateralism, the deals between the developed and the developing has increased. This can be elucidated by the fact that

the USA has made defence deals in the month of March 2023 with countries ranging from Taipei and Romania to Japan and Australia and also to Greece, Poland Kuwait and Bahrain. Thus, the mighty USA has defence deals countries from around the world. Both the major developing economies of the east, India and China have also signed defence and strategic agreements with majority of the countries with India being the largest weapon importer in the world it has increased its export by 334 % in the last 5 years (Li, 2008). These deals are comprehended and facilitated as per the Draft ToT Agreement and other international standards and state practices and opinion juris (Chinkin, 1989). Also, the IHL has regulations for transfer of certain technologies specified in its conventions and thus, it regulated the transfer of defence and military specific technology. However, with the advancement and the liquefying of the borders due to the preponderance of technology and capitalism in the form of profit making, defence deals are at the forefront. In light of this IHL has become crucial than ever and it needs to encompass all the upcoming at the pace that it is upcoming. The law needs to be more pragmatic and prudent than ever. IHL needs to understand the consequences of the deals and also needs to be a representative and if not party an observer in these (Ratner, 2011). However, the question would again arise who would be representing the IHL and what would accept such a representation.

International Humanitarian Law is known by a couple of other names in the contemporary. It has been called the Law of War and the Law of Armed Conflict (Alexander, 2015). However, it serves only one purpose that is the regulation of the inevitable, i.e. the war. It regulates the war and helps us understand the principle of Just War (McKinnon, 2008). The author has called the war inevitable considering the persisting wars between the various countries and nations of the world in the modern times. After the World War-II and with the Détente and the conclusion of the Cold War, the countries have collaborated at least on the sharing of technologies in order to advance their warfare purely on the monetary lines. It has been an ancient story whence the West negated the sharing of its technology to the east and to the second world and the third world purely due to conflict of ideologies. With the development of the capitalist model and the rapid exchange and sharing of technology pertaining to warfare the International Humanitarian Law has a crucial role to play. The Geneva Conventions which hold the privilege of having almost all the State's as it's signatories ought to provide the anvil on which this transfer of technology could be moulded. The United Nations has formulated the United Nations Convention on Trade and Development Transfer of Technology with the purpose of providing impetus to the transfer of technology to the developing nations (Pandey et al., 2022) international efforts around technology to support sustainable development transitions in developing countries have failed to yield results congruent with the needs. This review paper aims to contribute to, and help change, the conversation on international technology transfer (ITT. This Draft Code on Transfer of Technology (hereinafter referred to as Draft TOT) discusses the implication of technology transfer whether it be patented or non-patented. The paper analyses the Draft ToT's impact on

Article 36 of the Additional Protocol I to the Geneva Conventions of 12 August 1949 (McClelland, 2003). Further Part III of the Additional Protocol I (hereinafter referred to as AP I) enumerates the Methods and Means of Warfare Combatant and Prisoner-of-War Status (hereinafter referred to as POW) (Goodman, 2013). API dig into the means and methods of warfare that are permitted under the International Humanitarian Law (hereinafter referred as IHL). However, it does not mention the parameters for manufacturing or for TOT and thus, creates a major loophole in the status quo. The paper tries to analyse the lacunae and proposes certain strategies and viable solutions however, the latter shall remain secondary as it is outside the purview of the paper. Further the approach adopted here is purely doctrinal and the latter shall require empirical approach. Thus, the instant paper shall be restricted towards analysing the lacunae in relation to the transfer of technology for the modern warfare vis a vis the Geneva Conventions and shall analyse the same in light of the International Conventions, Treaties, Deals of all, Bi-lateral, multi-lateral and international character (Nedeski, 2022a).

1. International Trade and Transfer of Technology and Laws of War

This section explores the interconnected domain of international trade and War by delving into the doctrine of Transfer of Technology (ToT) by understanding the manufacture of tools of warfare. The transfer of technology refers to the process by which knowledge, skills, technologies, and manufacturing methods are shared between governments, organisations, or individuals (Gottwald et al., 2013). Historically, ToT has driven economic development and industrialisation, enabling countries to bridge technological gaps and enhance their productive capacities (Qi & Chu, 2022). However, in the context of armed conflict, ToT often involves the dissemination of military technologies, including weapons systems, surveillance tools, and cyber capabilities. The post-World War II era witnessed a significant increase in the global transfer of military technology, driven by geopolitical rivalries and the arms race during the Cold War. During this period, states actively engaged in the export and import of weapons, often using technology transfer as a tool of diplomacy and strategic influence. In recent decades, the nature of ToT has evolved significantly with the proliferation of dual-use technologies, those that have both civilian and military applications complicating the regulatory landscape. For example, drones designed initially for agricultural monitoring or disaster response have been repurposed for military surveillance and targeted killings in conflict zones (Ayamga et al., 2021). Correspondingly, Anderson and Waxman highlight the ethical and legal dilemmas posed by the use of armed drones in targeted killings. They argue that while drones may enhance precision in theory, their use in practice has often resulted in significant civilian casualties, raising questions about compliance with the Geneva Conventions (Winter, 2022). For instance, the United States drone strikes in Pakistan and Yemen have been criticised for violating the principles of distinction and proportionality

(Gunaratne, 2013), as well as for operating outside the framework of international law (Byrne, 2016). Similarly, advancements in artificial intelligence (AI) and robotics have led to the development of autonomous weapons systems, which operate without direct human intervention (Osimen et al., 2024). This raises ethical and legal questions about their use in warfare (Rid, 2012). The increasing involvement of private companies in the development and transfer of military technologies has further exacerbated these challenges, as these entities often operate outside the scope of traditional IHL frameworks (Hashimy, 2024).

1.1. International Trade, UNCITRAL and UNCTAD and War

The United Nations regulates and facilitates international trade through its two forums the United Nations Conference on Trade and Development (UNCTAD) and the United Nations Commission on International Trade Law (UNCITRAL). These along with the Hague Conference on Private International Law, OECD, WTO and others ensure that international trade has the impetus it requires (Baltag et al., 2023). All these however, are developed under the aegis of the Western and the Western Legal Traditions and therefore, the functioning of these multilateral agencies and treaties is rather unilateral. The feasibility of international trade along with the developments in technology have propelled the need for market. In this market-dominated State system the power is being accumulated by the sale and purchase of weapons. The deterrent theorists might affirm and rationalise the same and the neo-liberalists would assert the need of the market. And the realists might adhere to lex loci and Westphalia. Irrespective of the explanation for the dominance of trade, the established fact remains that arms trade deal marks a significant portion of the global trade and the western legal tradition setups in the international law have been supporting this. Further, the distinction between the categories of transfer of technology has created the divide between the arms producers and arms purchasers such that the necessary evil of sale and purchase need has been concretised.

1.2. Transfer of Technology

“Technology transfer” is the process by which commercial technology is disseminated. This takes the form of a technology transfer transaction, which may or may not be covered by a legally binding contract” (Van Norman & Eisenkot, 2017). Transfer of Technology of Technology Transfer is one of the agendas of UNCTAD which aims at dissipating and correcting the asymmetry between the Trans National Companies (TNCs) and the Countries importing them. Further it also aims towards making the availability of these military and defence related arms and armistice to the developing nations. The main issues that it deals with are:

a. Treatment of proprietary knowledge
b. Regulation of technology transfers
c. Competition issues
d. Technology related host country measures (Kim et al., 2024).

The United Nations Conference on Trade and Development on Transfer of Technology, 2001 (UNCTAD TOT Convention 2002) emphasises on the free market transfer of technology with the consideration for the Intellectual Property. It is the model law regulating the transfer of technology[1].

As the need for weapons increased the advancement was brought and recognised in the modern weapons. The four primary technologies that have led to these advancements are, Use of the effects of nuclear fission and fusion; Launching and controlling the actions of objects released in nearby outer space; Semiconductors and the development of technology in micro-electronics and Coherent light beams (lasers) and their many technological applications. All these still remain within the development terrains of the West and the developed countries. However, there are small but not steady steps being taken through the aegis of UN bodies. Some of these steps could be witnessed in the niche treaties. The Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons under its Article 11 talks about "Technologies Co-operation and assistance".The provision of Article 11 Section 1 however, only regulates the transfer of technology pertaining to the implementation of this protocol. This however, does not limit the scope of this Convention and it covers a vast number of means of warfare and also regulates their usage thus, regulating the methods of warfare. Further, the knowledge pertaining to land mines, booby traps, anti-personnel mines, non-detectable fragments form the basis as these are the weapons still being used rampantly and their proper technological transfer shall be beneficial in their proper dissemination. Technology Transfer is also crucial from the lens of Intellectual property (Maskus, 2022). According to the World Intellectual Property Organisation (WIPO) the different types of technology transfer agreements are (Muchlinski, 2021):

a. Technology Transfer Licensing Agreement
b. Assignments of Intellectual Property Rights (Stoll, 2022)
c. Confidentiality Agreements
d. Collaborative Research Agreements
e. Consultancy Agreements Sponsored Research Agreements
f. Material Transfer Agreements
g. Contract Research Agreements
h. Academic spin-off Agreements
i. University Research based Start-up Agreements
j. Joint Venture Agreements

Along with this analysis the paper adds a few other factors that have augmented or rather propelled the development of modern weapons:

1. Development in information technologies, particularly cyber technology and resultant development of Autonomous Vehicles and Mobile Robot Navigation (Raslan, 2024).

2. Development of Semi-autonomous Weapons and autonomous weapon systems.

[1] UNCTAD. (2001). Transfer of technology. UN. https://clck.ru/3Mdppn

3. Developments in communication technology and resultant missiles with minimal ricochet effect, air to air missiles, high-power microwaves, long-range stand-off weapons and such others. Also, with the advancement of 5G communication techniques the weapons and armistice have been able to advance with more efficacy in deplorable conditions as well (Gkagkas et al., 2024).

4. Advancement of Artificial Intelligence (Soori et al., 2023).

1.3. Laws of War

The etymology of international humanitarian law is perverse of the notions of Western Legal tradition and therefore the author has been using the terminology of laws of war instead (Kiss & Lammers, 2021). The same has been discussed in and again by the academicians and the authors keeping in mind the third world narratives. Further the terminology of international humanitarian law keeps in abeyance the aspirations of the sovereign by sticking to the set tenets.

2. Geneva Conventions and Additional Protocols

This section discusses the available provisions under the international law for regulating the production of means of warfare. Therefore, this section highlights the lacunae in the available Treaties and Instruments.

2.1. International Legislations

The part tries to locates the provisions pertaining to regulation on the means of production enumerated in the positive international law through the help of treaties and customary provisions. IHL has developed a long list of protocols for sieving the means and methods of warfare. Some of these Conventions, Treaties and Declarations are enumerated below:

a. Declaration Renouncing the Use, in Time of War, of Certain Projectiles, St. Petersburg, (Certain Explosives Projectiles), 1868 (Schindler & Toman, 2004a).

b. Declaration (IV, 1) to Prohibit for the Term of Five Years, the Launching of projectiles and Explosives from Balloons, The Hague, (1899 Hague Balloon declaration), 1899; Declaration (IV, 2) Concerning Asphyxiating Gases, The Hague, (Hague Gas Declaration), 1899; Declaration (IV, 3) Concerning Expanding Bullets, The Hague, (Hague Dum-dum Bullet Declaration), 1899 (Traven, 2021).

c. Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons, The Hague (1907 Hague Balloon Declaration), 1907 (Schindler & Toman, 2004b).

d. Convention (VIII) Relative to the Laying of Automatic Submarines Contact Mines, The Hague (1907 Hague Sea Mines Convention), 1907 (Haines, 2014).

e. Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or other gases, and Bacteriological Methods of Warfare, Geneva (1925 Geneva protocol), 1925 (McElroy, 1991).

f. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and toxin Weapons and Their Destruction, London (Biological Weapons Convention), 1972 (Dando & Pearson, 1997).

g. UN Convention on the Prohibition of Military or Any Other Hostile use of Environmental Modification Techniques (ENMOD), 1976 (Jarose, 2024).

h. Convention on the Prohibition or Restrictions on the Use of Certain Conventional Weapons Which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects, Geneva (CCW), 1980; CCW Protocol I; CCW Protocol II and CCW Protocol III (Dunworth, 2020).

i. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Paris[2], 1993 (Tabassi, 2007).

j. Arms Trade Treaty, 2013 (D'Ascanio, 2017; Lustgarten, 2015).

These treaties and conventions provide reprimands in the form bans and regulations on certain types of weapons. It is crucial to understand that these treaties have not been ratified in majority of the States who are parties to the same. The advancements in the usage of chemical weapon systems stands outside the purview of the Chemical Weapons Convention, 1993 in light of its Article II Section 9 which enlists the purposes which are not prohibited under the convention and is inclusive of peaceful purposes (Lak, 2009), which has not been defined further under the convention[3]. This opens the portal for development of chemical weapons in the garb of protective purposes, military purposes and law enforcement purposes. Thus, it indirectly permits the States to use the Chemical Weapons. Further, with the advancement of technology the developments in the Anti-ballistic air to air missiles, the challenges for administering the attack specifically on target in light of the IHL principle of Distinction has become many folds.

2.2. Geneva Conventions and the Additional Protocols

The Geneva Conventions ensure the availability of law by providing for its application in times of war irrespective of the declaration and recognition of war (Daniele, 2024). The Conventions I-IV along with the Protocols I, II and III ensure jus in bello (Stahn, 2006). The Additional Protocol I primarily discusses the means and methods of warfare.

2.3. The Principle of Distinction and Technology Transfer

Article 48 of Additional Protocol I to the Geneva Conventions enshrines the principle of distinction, which requires parties to a conflict to distinguish between civilians and combatants at all times (Melzer, 2008). However, the transfer of technologies such as armed drones and autonomous weapons systems complicates the application of this

[2] Chemical Weapons Convention. (n.d.). OPCW. https://clck.ru/3Mdq58

[3] Ibid.

principle. For instance, armed drones, while touted for their precision, have been used in ways that blur the line between civilian and military targets. The United States' transfer of armed drones to allies like Pakistan has resulted in significant civilian casualties in counterterrorism operations, raising questions about compliance with Article 48 (Boyle, 2013). Correspondingly, autonomous weapons systems, which operate without human intervention, challenge the principle of distinction. These systems rely on algorithms to identify and engage targets, but they lack the ability to make context-specific judgments. For example, the use of autonomous drones in Libya by non-state actors resulted in indiscriminate attacks on civilian infrastructure, violating the principle of distinction (Schmitt, 2008). The Geneva Conventions do not explicitly address the transfer of such technologies, leaving a regulatory gap that undermines their effectiveness.

2.4. The Principle of Proportionality and Dual-Use Technologies

Article 51(5)(b) of Additional Protocol I prohibits attacks that may cause excessive civilian harm relative to the anticipated military advantage (Beard, 2019). This principle of proportionality is particularly relevant to the transfer of dual-use technologies, which have both civilian and military applications (van den Boogaard, 2023). For example, surveillance technologies originally designed for civilian purposes have been repurposed by authoritarian regimes to target civilian populations. In Yemen, surveillance equipment supplied by Western countries was used by the Saudi-led coalition to identify and attack civilian infrastructure, resulting in disproportionate harm to civilians (Pomson, 2023). The transfer of cyber capabilities also raises concerns about proportionality. The Stuxnet virus, allegedly developed by the United States and Israel, was used to sabotage Iran's nuclear program (Rid, 2012). While the operation targeted a military facility, the virus spread to civilian systems, causing unintended harm. The Geneva Conventions do not provide clear guidelines on the transfer of cyber technologies, leaving states to exploit legal loopholes.

2.5. Prohibition of Weapons Causing Unnecessary Suffering

Article 35(2) of Additional Protocol I prohibits using weapons that cause superfluous injury or unnecessary suffering (Cassese, 2008). However, the transfer of technologies such as cluster munitions and incendiary weapons has resulted in widespread civilian harm. For example, the transfer of cluster munitions by the United States to Saudi Arabia was linked to civilian casualties in Yemen, as these weapons often fail to detonate on impact, posing long-term risks to civilians. The Geneva Conventions do not explicitly regulate the transfer of such weapons, allowing states to circumvent their obligations under IHL. Similarly, the transfer of autonomous weapons systems raises concerns about unnecessary suffering.

These systems, which operate without human judgment, may cause prolonged suffering by targeting individuals in ways that violate the principles of humanity. For instance, the use of autonomous drones in targeted killings has been criticized for causing unnecessary harm to civilians and violating the spirit of Article 35(2) (Liivoja, 2024). Furthermore, Article 36 of Additional Protocol I requires states to review new weapons, means, and methods of warfare to ensure compliance with IHL. This article provides a potential framework for regulating technology transfer but lacks enforcement mechanisms. For Example, Countries developing cyber warfare tools should theoretically conduct legal reviews to assess compliance with IHL, yet many do not due to the absence of binding regulations (McClean, 2002).

Articles 57 and 58 of Additional Protocol I mandate precautions in attacks to minimize civilian harm[4]. The transfer of drone technologies with autonomous targeting capabilities could challenge these obligations if not strictly regulated. For example, Autonomous drones used in conflict zones may lead to civilian casualties due to flawed targeting algorithms, contradicting the precautionary principles outlined in these articles (Al Karawi, 2024).

3. Hague Conventions

While the Geneva Conventions focused on the regulation of war, the Hague Conventions of 1907 developed parallel developing with the regulations on the means of warfare (Ní Shúilleabháin & Trimmings, 2024). The Hague Conventions of 1899 and 1907 have been instrumental in regulating warfare, including provisions on the transfer of military technology. The 1907 Hague Convention VIII on the Laying of Automatic Submarine Contact Mines and Hague Convention IX on Bombardment by Naval Forces highlight early efforts to control the spread and use of emerging military technologies. Article 1 of Hague Convention VIII restricts the use of contact mines unless they become harmless after a short period, ensuring that technology does not lead to indiscriminate destruction (Webster, 2011). Similarly, Hague Convention XIII on Neutral Powers in Naval War prohibits the transfer of warships or munitions from neutral states to belligerents (Articles 6 and 8), aiming to prevent technological proliferation in conflicts. These provisions laid the foundation for modern arms control treaties by addressing the ethical and legal implications of transferring warfare technologies, anticipating later agreements like the Missile Technology Control Regime (MTCR) and the Arms Trade Treaty (ATT).

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. (n.d.). https://clck.ru/3MLAFT

4. Principles and Customary IHL

One of the major principles of IHL is the principle of distinction. This is the crux of the IHL and thus, segregates the combatant from the civilian. Every IHL doctrine is based on the principle that those persons who are civilians and also those who are hors de combat and protected shall not be attacked. This is based on the principle of humanity and intrinsic right to life attached and encumbered by every individual by their very birth. This is also done with the purpose of facilitating the mundane affairs to the utmost possible extent in the time of war. However, the weapons and the weapon systems used cause destruction more than requisite and thus, damaging the civilian objects and the population as well. Today we are investing in the R&D and have been able to proceed towards the actualisation of such armistice that can identify the individual and attack them thus, mitigating the causation of superfluous injury or of harming the civilian population. However, reliance on AI and such modern warfare has not been beneficial. Even before their advent countries have come together and have signed treaties against their usage and production. Companies have started banning the usage of AI in their regular work. This is happening parallel to the vast number of monetary resources being invested on their production. At the same time, we have been unable to eradicate poverty from the world. Today we are still proceeding with the Sustainable Development Goals of clean water and education. Thus, IHL needs to cater to the same with its legal provisions and needs to codify legislation pertaining to the regulation of the investment of resources towards the development of arms and armistice.

5. Other Treaties

The Arms Trade Treaty (ATT) complements the Geneva Conventions by regulating arms transfers that contribute to human rights abuses (da Silva & Wood, 2021). Article 7 of the ATT requires exporting states to assess whether the transferred technology could be used in war crimes (Clapham et al., 2016). While this provision applies to conventional arms, its effectiveness in addressing emerging dual-use technologies remains limited. Scholars argue that integrating dual-use regulations within IHL frameworks could strengthen legal accountability.

5.1. Regional Agreements

European Union has been actively developing policies and guidelines for regulation of war and warfare (Kelemen & McNamara, 2022). However, there are no instruments or documents that have been adopted in the form of treaty (Lupu & Wallace, 2024) 2024. Though USA dominates the SIPRI arms producing military services company list, Europe with the countries of Germany and Italy remains the next top contender. The positive sign remains that the sale percentage in the arms trade has decreased for the year 2022 but

this is too little too late when the arms trade deals are gaining momentum (Larik, 2023). Further, the regions of Asia and the Pacific have not discussed the regulation on arms trade deal or transfer of technology in any of their agreements and rounds. However, what these regional agreements discuss qua the ToT is the standard setting instruments within the framework of TRIPS. The regional level standard setting instruments have been concluded by the regional organisations of NAFTA (Bethlehem et al., 2009), Andean Group and ASEAN along with EU (Ansari & Babu, 2018). The EU Commission regulation of 2014 discusses technology transfer qua competition and therefore includes the licensing of technology rights (Anderman & Kallaugher, 2006). While these standard setting instruments are not discussed much and there remains the unhindered reluctance in the developed countries to share the same with the developing and the LDCs, the second category of instruments are being discussed and agreed upon readily compared to the former category. This second category of ToT focuses more on direct measures aiming at capacity building and can be said to be in tandem with the sustainable development needs. This has been taken up by the regional organisations of ASEAN, ESCOWAS and other sub-groups (Strachan, 2020). Thus, the regional regulations appear and act as mere auxiliary for the UNCTAD endeavours.

There are however, regional disarmament treaties and these treaties do not discuss the option of ToT on the apprehension and assumption that disarmament could be conceded sans ToT. However, this very approach impedes the evolution and development of technology in the developing and the LDCs. This disturbs the balance of power and leads to the divide between the core and the periphery (Vidigal, 2013). Thus, perpetuating the rift between the developing and the developed.

5.2. Bilateral and Multi-lateral Treaties and Agreements

The Treaty law is governed by the Vienna Convention on the Law of the Treaties, 1969 (Villiger, 2008). Between the period of 2015 to 2018, India has signed Defence and Military related Memorandum of Understandings and Agreements with 29 other Countries and most of these pertain to transfer of technology (Sinha, 2023). During the 12th Defence Expo, in October, 2022, a total of 451 MoUs (Nedeski, 2022b), Transfer of Technology Agreements and Product launches were executed. Of these the number of ToTs were eighteen. It is crucial from the perspective of IHL as India is also the largest exporter of the military and defence equipment and its involvement in any war in near future shall be detrimental for the Humanitarian Laws. India however, has not only acclimatised itself in accordance with the ToT but has brought the tenets of the same in its defence agreements and releases. Defence Research and Development Organisation (DRDO) has released its own Policy and Procedure of Transfer of Technology Manual which categorises the items and provides regulation on their imports and exports. Also, the Indian Government has released its Defence Acquisition Procedure, 2020 which elucidates the procedures and policies adopted by the Government with the motive of facilitating the ease of doing business and strengthening the concept of Atmanirbharta

(Jain & Gill, 2022) or self-reliance being propounded by the Indian Government. Thus, the importers are in the process of becoming the exporters. This shall not only provide equilibrium to the balance of power but shall also provide impetus to the development and better advancement of the safeguard mechanisms in light of the increased competition.

Between the period of March 2022 to March 2033 the USA has signed 74 bi-lateral defence deals ("Chapter Seven", 2025). Japan has also been signing ToT agreements and has defence co-operation with the USA, the UK, France, Germany, Italy, India, Australia, Philippines, Vietnam, Indonesia and Malaysia. Japan under its Defence Budget for the year 2023 provides for transfer of technology under the heading "Expanding the Sales Channels of the Defence Industry, etc." and states for cross-border transfer of defence equipment. Further Japan has adopted "Measure on Defence Equipment and Technology Co-operation" (Szenes, 2023).

The United Kingdom has agreed over mutual security deals with both Finland and Sweden. Though this pact does not include transfer of technology, however, it opens the portal for the same. The UK has agreed to come to the aid of these nations in case either of these nations come under attack. Thus, the defence deals and military trade has become far more accessible with all the treaties in existence and those being processed behind the closed doors and yet again IHL's task is made difficult and hectic. These defence deals and treaties are not executed from the lens of the IHL. These arrangements and agreements are not considered within the ambit of methods of warfare as they are being executed in the name of national and international security. However, them being detrimental for the world is just a stick away and the same has to be taken care by the IHL. The AP-I and the Geneva Conventions do prohibit such means and methods of warfare which are against the IHL principles however, these do start analysing the activities in the time of war or when they are categorically specified to be used for war. Thus, these weapons garner the advantage and thus, the deals and agreements thrive at the pretext of national security and international peace. It shall be the duty of the global organisations such as UN, the multi-lateral organisations such the BRICS, ASEAN, NATO, QUAD and such others in association with the ICRC and other IHL bodies to analyse these agreements and ToT in light of IHL and such related protocols and laws.

6. Exploring the Entangled Relationships

The transfer of technology intersects with the Geneva Conventions in several critical ways. First, the principles of distinction and proportionality, which are central to IHL, are increasingly difficult to apply in the context of advanced military technologies. For example, the use of armed drones in targeted killings raises questions about compliance with the principle of distinction, as these technologies often result in civilian casualties[5]. Similarly, deploying autonomous weapons systems challenges the principle of proportionality, as

[5] Boyle, M. (2013). The Costs and Consequences of Drone Warfare. International Affairs, 89, 1.

these systems operate without human judgment and may cause disproportionate harm to civilians. Second, the transfer of dual-use technologies complicates the application of the Geneva Conventions. States often exploit legal loopholes to transfer technologies that can be used for both civilian and military purposes, making it difficult to hold them accountable for violations of IHL. For instance, the transfer of surveillance technologies to authoritarian regimes has been used to suppress dissent and violate human rights. Yet, these actions often fall outside the scope of the Geneva Conventions[6]. Human Rights Watch (2020) has documented numerous cases where dual-use technologies have been used to perpetrate human rights abuses. In Yemen, for instance, surveillance technologies supplied by Western countries have been used by the Saudiled coalition to target civilian infrastructure, resulting in widespread suffering and displacement. These cases underscore the urgent need for stricter regulations on the transfer of dual-use technologies and greater accountability for states and private actors involved in their dissemination. Finally, the increasing role of private actors in developing and transferring military technologies poses a significant challenge to the enforcement of IHL. Companies such as Palantir and Raytheon are pivotal in advancing surveillance and weapons technologies, yet the Geneva Conventions do not bind them. This lack of accountability undermines the effectiveness of IHLin regulating modern warfare and highlights the need for legal reforms to address these emerging challenges.("Wired for War", 2009) In the same way, the role of private actors in developing cyber capabilities, arguing that transferring these technologies to non-state actors poses significant risks to global security. The Stuxnet virus, allegedly developed by the United States and Israel, provides a vivid example of the challenges posed by unregulated technology transfer. 19 While this operation did not directly violate the Geneva Conventions, it set a dangerous precedent for the use of cyber technologies in armed conflict, raising questions about the adequacy of existing legal frameworks.

6.1. War and Economy

The dilemma concerning economic interdependence and war has been engulfing the nations since the period of détente (Copeland, 1996). That is the Western parochial way of understanding this relation. One needs to understand that the States have realised the vitality of both war and trade and have accepted their inevitability. This has been made possible by trading in the means of warfare. As the countries grew scientifically and socially competent they catered to the needs of economy by adding the need and want rather than focusing on the product. The arms and armistice have been marked as essential in the contemporary and rather than moving towards disarmament we are focusing on treaties and trade deals that discuss the production of means of warfare. Further, the technology transfer is yet not being done and therefore, the deterrence is maintained.

[6] Human Rights Watch, Yemen: Coalition Bombing Campaigns Cause Civilian Deaths. (2020).

6.2. The Acceptability of Transfer

Intellectual property laws at the international level remain the major impediment for the technological rift between the developed and the developing. While the developed focused on the brain and started venturing and regulating the new phases of industrial revolution, the economy of the developing and the countries of the global South remain trapped between the sectors of primary, secondary and tertiary. TRIPS, Marrakesh Treaty and other such treaties not only regulate but block the technological exchange. This reflects the non-adherence to the technology transfer agreements and thus, its reserved acceptance and implementation.

7. The Technological Divide

The technological divide between the north and the global south has led to fear and tension therefore, causing disturbance in the balance of power. More so when this disparity is in regards to the very means of warfare. This is evident in Bilateral Investment Treaties (BITs) and Multilateral Investment Treaties (MITs), where developed nations often secure favourable terms, controlling arms-related technology transfers. For instance, Article 3 of the US-India BIT (1997) ensures "National Treatment" but allows security exceptions under Article 18, limiting technology-sharing in defence sectors. Similarly, the Energy Charter Treaty (ECT), a multilateral agreement, allows restrictions on technology transfer in sectors deemed critical to national security, impacting arms production capabilities in Least Developed Countries (LDCs). The Wassenaar Arrangement, although not a treaty, regulates dual-use technology exports, disproportionately affecting developing nations. Article 2 of the Arms Trade Treaty (ATT, 2014) further restricts the transfer of conventional weapons, limiting LDCs' access while developed nations maintain technological supremacy. These disparities reinforce geopolitical tensions and an uneven balance of power.

8. Jus in bello and Transfer of Technology

This part will discuss the challenges that law of war faces qua the international trade.

8.1. Scylla and Charybdis or Hobson's Choice

International law encounters the quandary when it comes to choosing between regulation on the production of means of warfare and facilitating international trade and business. International law faces a fundamental dilemma, regulating the production of warfare technologies while simultaneously facilitating international trade and business. This conflict is evident in arms control treaties and technology transfer regulations, which

disproportionately benefit developed nations. The Missile Technology Control Regime (MTCR) and the Wassenaar Arrangement limit access to advanced military technology for developing nations while allowing P5 states to maintain their technological superiority. The Arms Trade Treaty, Article 6 restricts arms transfers that could violate humanitarian law, yet developed nations continue to supply weapons to strategic allies, reinforcing global power imbalances.

8.2. The Fragmentation of the Law of War

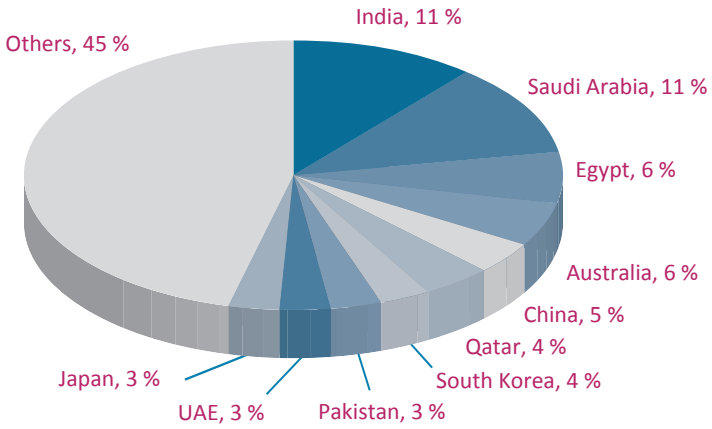
The just war theory has been bifurcated into jus ad bellum and jus in bello (Hampson, 2018). This part asserts that international law of war cannot satiate its purpose until it has composite control for forming laws and regulating both the facets (Peters, 2017). This unilateral development has distorted the law of war, reinforcing disparities between the developed and developing world. The power to shape these laws lies primarily with the P5 nations, particularly the United States, which remains absent from key Hague Conventions and the ICC while continuing to be the world's largest arms manufacturer (Whittle, 2015). Some of the prominent criticisms in the past two decades have been raised by the countries of the global South particularly the countries in the African continent. The 2009 and 2010 arrest warrants against Sudan's former President, the 2011 action on Kenyatta and 2016 DRC unilateral decisions have questioned the sanctity of the ICC.

8.3. Venturing into the Principles

Key principles of law of armed conflict have been misused to justify military interventions by powerful nations. Article 51 of AP I of Geneva Conventions prohibiting indiscriminate attacks, is often applied selectively. The principle of proportionality is manipulated through the rhetoric of 'precision strikes', where civilian casualties are dismissed as collateral damage. Similarly, the justification of military necessity allows powerful states to bypass legal constraints, as seen in drone strikes carried out without adherence to international protocols.

9. Trade, Technology and War

The dilemma faced by the IHL is not due to the advancement in the modern weapon system but due to the sale and disbursement of these weapon systems and their parts and products. It is pertinent to notice that the major producers of these weapons are still present in the first and the second world, with the top 5 producers being from the United States itself however, the major purchasers being in the third or the developing nations. According to the SIPRI Fact Sheet published in March 2022, titled 'Trends in International Arms Transfer, 2021'the top 5 importers for the year 2017–2021 were India, Saudi Arabia, Egypt, Australia and China (Fig.).



Percentage of WEAPON Import

It is germane to know that all of these countries have a turbulent geo-politics because of the tumultuous relations with their neighbouring States. While two new States were carved by the Colonial Empire from the majestic India, the debacle over the Xinjiang and Aksa chin provinces have kept it in conflict with the neighbouring State of China too. Both the countries of Egypt and Saudi Arabia have not only to conform to the Middle East Policies but have also to counter the challenges faced due to their geographical locations. Australia might appear to be away from the Conventional Policy making however the Refugee and Environmental crisis has led it to join the Quad for securing its position in the Pacific and Oceania (Hashimy, 2023; Jayaram, 2024). It would be legally incorrect to mention that these countries have on-going Non-International Arms Conflict as it has not been declared vide the AP II however, it would not be wrong to name these insurgencies and secessionist movements. Again, in this post neo-liberal era the States have been working parallelly on different fronts and have been performing the role of both friends and fiends with their counterparts. This might appear a peaceful propagation but in reality, it is antithetical to IHL as it would not only bring the States in consensus against the law but the Sovereign power would undermine the international law (Mearsheimer, 2022).

Technology Readiness Level (hereinafter referred as TRL) developed by National Aeronautics and Space Administration (hereinafter referred as NASA) provides measurement of maturity of the weapons (Olechowski et al., 2020). Further the Manufacturing Readiness Level (MRL) provides for the efficacy and the ease of development. In the contemporary the weapons are tested on the basis of TRL. (Ferreira et al., 2021). However, there are certain challenges with this approach as propounded by J C Mankins and A Olechwoski along with his fellow researchers. The major criticism comes in the form of involvement of human assessment methodology for ascertaining these levels. Also, the readiness comes in nine levels and both level 8 and level 9 which tests for fight qualified and fight proven are ascertainment made on the pretext of human assessment and calculation and this is quite different from a real war scenario. However, automating it would create further challenges. Also, the IHL still has not brought within its ambit the TRL in the ascertainment of the means and methods of warfare and neither has the same been enumerated

under the Customary IHL. Further these assessments are not in consonance with the IHL principles of Humanity, Distinction, Proportionality, and Military Necessity. Thus, though the modern weapons have developed and will be developing further with the advancement in technology the IHL and its augmenting rules and laws needs to be taken into consideration by the States for the procurement of the weapons.

10. Third World and Unheard Narratives

This part discusses the subjugated narratives qua laws of war and trade from the global south.

10.1. TWAIL and WTO and Regulation on Means of Warfare

The global arms industry remains a site of deep structural inequality, where the production and transfer of military technology occur almost exclusively from the vantage point of developed nations (Chimni, 2022). According to SIPRI, the five largest arms exporters the United States, France, Russia, China, and Germany account for the majority of global arms sales, with the US alone responsible for 42 % of total exports. Meanwhile, developing nations remain heavily reliant on these suppliers, lacking the capacity to produce advanced weaponry independently. This asymmetry is reinforced through WTO frameworks, particularly the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (Upreti, 2022), which privileges the Global North by safeguarding patents and restricting the dissemination of critical military technologies (Dent, 2021).

Technology transfer occurs in two primary ways: voluntary licensing and foreign direct investment (FDI) (Osano & Koine, 2016) However, both mechanisms overwhelmingly favor developed states. UNCTAD reports that over 80 % of global technology licensing fees flow to firms in the United States (Van Norman & Eisenkot, 2017), Europe, and Japan, ensuring the continued monopoly of high-value defense innovation (Cheng, 2021). From a TWAIL perspective, this is a continuation of colonial power structures, where developing nations remain subordinated through a cycle of dependency. The WTO's regulatory regime (Ezell & Cory, 2019), rather than facilitating equitable access to military technology, perpetuates neo-colonial hierarchies, limiting the agency of the Global South in matters of security and warfare.

10.2. International Trade and International Laws of War

According to the Stockholm International Peace Research Institute (hereinafter referred as SIPRI) report published in December, 2022 titled "The SIPRI Top 100 Arms-Producing and Military Services Companies, 2021" the combined arms sales though rose from the 2021 baseline (in US Dollars) but were affected due to decrease in production of the Semiconductors resultant of the COVID-19 Pandemic. This also resulted from

the complex supply chain these companies have been following. For example, the Company General Dynamics Ranked 5th, relies on a supply-chain involving 11,000 (Eleven Thousand) companies. Thus, in order to evade the different levels of legal bars this trend is beneficial and further economically feasible for these giant traders. The resource crunch War also hindered their growth as the supply of pertinent raw materials in the form of Aluminium (Hashimy & Benjamin, 2023), Copper, Zinc and Titanium were restricted due to different import-export sanctions from the European Union (EU) and various other countries (Nadkarni et al., 2024). One major challenge that the State's face particularly the USA is the acquisition and mergers of these mammoth companies. The Competition law indeed puts a restraint on any such detrimental merger or acquisition however, the dependency of the large number of suppliers on one major company is another challenge that needs to be tackled (Spulber, 2023). The IHL does not talk about these challenges further, them falling with the vicinity of the municipal laws, the IHL cannot envisage much in the very domain thus, opening the escape-gate for these armistice producers and developers (Dunworth, 2020).

11. Propositions and Suggestions

This paper suggests that the countries should form an international organisation at par with the General Assembly and the Security Council and the same shall have equal representation from every country around the world irrespective of their UN membership. Further, these countries should not only have ONE VOTE each, their monetary share to the organisation should be irrelevant in their representation. These members shall be the one adjudicating and justifying the efficacy of the defence deals and also the mergers and acquisitions of the defence companies' vis a vis the status quo, global, social, economic and environmental measures and then analyse them from the lens of IHL. Once these deals have satisfied all these criteria then they shall be sanctioned for execution. Also, the executions shall be permitted only in accordance with the geo-political scenario of the countries signing them and its effect over the countries that would be affected by the same. The major criticism of the same would come in the form that such an agreement would not any deter and impede the defence deals to be executed and also, that the developed countries would still be at the upper echelon considering their existing deals which they can impede at their will at any given point. Also, the purchasers could form the lobby and disrupt the deals of the other upcoming purchasers and thus, the organisation would be futile. However, merely disrupting the organisation on the basis of these would be both naïve and puerile.

Addressing dual-use dilemmas requires a multifaceted approach integrating legal reforms, ethical oversight, and international cooperation. The following recommendations outline specific measures to enhance the Geneva Conventions' applicability to modern technology transfers.

11.1. Economy and Human Development

As stated above every country shares a major chunk of their budget to its military and defence. While the developed countries invest less chunk of their budget as compared to the developing countries, the investment is still high. We do believe in the deterrent school of thought and we do understand the importance of procurement of weapons in this age of uncertainty. However, what we fail to understand as a student of IHL is the rampant and excessive production and procurement of these weapons. IHL tends to regulate the inevitable, the war. On the other hand, such procurements and productions can not only disrupt the balance of power but shall also undermine the investment in other sectors.

11.2. Environment

Napalm bomb, Agent orange, ICBMs, Killer Robots, Ground Based Air Surveillance Radars and many others are the names people debate about (Johnson & Johnson, 2023). While the quotient of military necessity and the concept of just war propounds for their support and efficacy, the environmentalists understand the severe, long-term and widespread threat that they have caused and they can cause to the environment.

"The United Nations Environment Programme (UNEP) has found that over the last 60 years, at least 40 percent of all internal conflicts have been linked to the exploitation of natural resources, whether high-value resources such as timber, diamonds, gold and oil, or scarce resources such as fertile land and water. Conflicts involving natural resources have also been found to be twice as likely to relapse".

11.3. Development of Supplementary Protocols

States should negotiate and adopt additional protocols to the Geneva Conventions explicitly addressing technology transfer, particularly concerning dual-use items and emerging military technologies. These protocols should define the responsibilities of states and non-state actors in preventing the proliferation of technologies that could be used in violations of IHL. For instance, A supplementary protocol could explicitly prohibit the transfer of AI-driven autonomous weapons unless stringent human oversight mechanisms are in place.

11.4. Establishment of International Monitoring Mechanisms

An international regulatory body should be created to oversee and monitor the transfer of sensitive technologies. This body could operate under the auspices of the United Nations and collaborate with existing export control regimes such as the Wassenaar Arrangement. For example, A centralised global database could track dual-use technology exports and ensure compliance with IHL, preventing unauthorised transfers to conflict zones.

11.5. Promotion of Transparency and Information Sharing

States and private entities involved in technology development and transfer should adopt transparent practices and share information regarding the end-use of dual-use technologies. For example, to prevent human rights abuses, technology firms could be required to disclose detailed risk assessments before selling surveillance technology to foreign governments.

11.6. Strengthening National Legislations

States should enact and enforce domestic laws that regulate the export of dual-use technologies. National regulatory frameworks should include mandatory human rights impact assessments and compliance measures aligned with IHL. For instance, Governments could introduce legislation requiring licensing for the sale of AI-based targeting systems, ensuring their use aligns with humanitarian law.

11.7. Proposed Amendments to Geneva Conventions Articles

Amending Article 35(2) of Additional Protocol I to explicitly include emerging technologies such as AI-driven weapons and cyber warfare tools as prohibited means of warfare if they lead to disproportionate suffering or indiscriminate harm (Bothe, 2017). Amending Article 36 of Additional Protocol I to mandate states to conduct legal reviews of technology transfers to ensure compliance with IHL, extending review requirements beyond traditional weapons to include AI, cyber tools (Melzer, 2008), and surveillance systems (Copeland et al., 2023). To introduce a new Article on Technology Transfer Regulation. It will be proper to introduce a new provision explicitly prohibiting the transfer of dual-use technologies to non-state actors engaged in armed conflict unless such transfers comply with stringent humanitarian guidelines.

Conclusion

International Armed Conflict can have a devastating impact on the sovereign parties to it. The Sovereign being the post-Westphalia States have to focus not only on the State security but also on individual security. This can only be ascertained with the help of proper rules and regulations and the same is provided by IHL. The Sovereigns need to get accustomed to the IHL and its principles and the future of weapons in military and defence shall be proceeded through the lens of IHL in order to ascertain the better and peaceful global future. The Geneva Conventions, while foundational to IHL, are ill-equipped to address the challenges posed by technology transfer in modern warfare. The principles of distinction, proportionality, and the prohibition of unnecessary suffering are increasingly difficult to apply in the context of advanced military technologies. The lack of clear guidelines

on the transfer of technologies such as armed drones, autonomous weapons, and cyber capabilities has created a regulatory vacuum that undermines the effectiveness of the Conventions. Addressing these challenges will require significant legal reforms, including negotiating an additional protocol to the Geneva Conventions that explicitly regulates technology transfer.

References

Al Karawi, Z. K. M. (2024). The hague conventions: cornerstone of modern international law. *Russian Law Journal*, *12*(1), 2027–2033.

Alexander, A. (2015). A Short History of International Humanitarian Law. *European Journal of International Law*, *26*(1), 109–138. https://doi.org/10.1093/ejil/chv002

Anderman, S., & Kallaugher, J. (2006). *Technology Transfer and The New Eu Competition Rules: Intellectual Property Licensing After Modernisation* (Oxford, 2006; online edn, Oxford Academic, 31 Oct. 2023). https://doi.org/10.1093/oso/9780199282142.001.0001

Ansari, S., & Babu, R. R. (2018). 5. North American Free Trade Agreement (NAFTA). *Yearbook of International Environmental Law*, *29*, 390–397. https://doi.org/10.1093/yiel/yvz032

Ayamga, M., Akaba, S., & Nyaaba, A. A. (2021). Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change*, *167*, 120677. https://doi.org/10.1016/j.techfore.2021.120677

Azam, M. (2020). Does military spending stifle economic growth? The empirical evidence from non-OECD countries. *Heliyon*, *6*(12), e05853. https://doi.org/10.1016/j.heliyon.2020.e05853

Baltag, C., Joshi, R., & Duggal, K. (2023). Recent Trends in Investment Arbitration on the Right to Regulate, Environment, Health and Corporate Social Responsibility: Too Much or Too Little? *ICSID Review – Foreign Investment Law Journal*, *38*(2), 381–421. https://doi.org/10.1093/icsidreview/siac031

Beard, J. (2019). The Principle of Proportionality in an Era of High Technology. In W. S. Williams, & C. M. Ford (Eds.), *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare* (pp. 261–288). Oxford University Press. https://doi.org/10.1093/oso/9780190915360.003.0009

Bethlehem, D., McRae, D., Neufeld, R., & Van Damme, I. (Eds.). (2009). *The Oxford Handbook of International Trade Law*. Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199231928.013.0001

Bothe, M. (2017). The International Committee of the Red Cross and the Additional Protocols of 1977. In R. Geiß, A. Zimmermann, & S. Haumer (Eds.), *Humanizing the Laws of War: The Red Cross and the Development of International Humanitarian Law* (pp. 57–80). Cambridge University Press. https://doi.org/10.1017/9781316759967.004

Boyle, M. J. (2013). The costs and consequences of drone warfare. *International Affairs*, *89*(1), 1–29. https://doi.org/10.1111/1468-2346.12002

Byrne, M. (2016). Consent and the use of force: An examination of 'intervention by invitation' as a basis for US drone strikes in Pakistan, Somalia and Yemen. *Journal on the Use of Force and International Law*, *3*(1), 97–125. https://doi.org/10.1080/20531702.2015.1135658

Cassese, A. (2008). Weapons Causing Unnecessary Suffering: Are They Prohibited? In A. Cassese, P. Gaeta, & S. Zappalà (Eds.), *The Human Dimension of International Law: Selected Papers of Antonio Cassese* (pp. 192–217). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199232918.003.0009

Chapter Seven: Latin America and the Caribbean: Regional trends in 2024 380; Regional defence policy and economics 382; Arms procurement and defence-industrial trends 392; Armed forces data section 393. (2025). *The Military Balance*, *125*(1), 380–439. https://doi.org/10.1080/04597222.2025.2445479

Cheng, T. K. (2021). Technology Transfers in Developing Countries. In T. K. Cheng (Ed.), *The Patent-Competition Interface in Developing Countries* (pp. 54–81). Oxford University Press. https://doi.org/10.1093/oso/9780192857354.003.0003

Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, *35*(1), 29–54. https://doi.org/10.1017/S0922156521000534

Chinkin, C. M. (1989). The Challenge of Soft Law: Development and Change in International Law. *The International and Comparative Law Quarterly*, *38*(4), 850–866. https://doi.org/10.1093/iclqaj/38.4.850

Clapham, A., Casey-Maslen, S., Giacca, G., & Parker, S. (2016). *The Arms Trade Treaty: A Commentary*. Oxford University Press.

Copeland, D. C. (1996). Economic Interdependence and War: A Theory of Trade Expectations. *International Security*, *20*(4), 5–41. https://doi.org/10.2307/2539041

Copeland, D., Liivoja, R., & Sanders, L. (2023). The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems. *Journal of Conflict and Security Law*, *28*(2), 285–316. https://doi.org/10.1093/jcsl/krac035

Ezell, St., & Cory, N. (2019). *The Way Forward for Intellectual Property Internationally*. ITIF.

da Silva, C., & Wood, B. (Eds.). (2021). *The Arms Trade Treaty: Weapons and International Law*. Intersentia. https://doi.org/10.1017/9781839701603

Dando, M. R., & Pearson, G. S. (1997). The Fourth Review Conference of the Biological and Toxin Weapons Convention: Issues, Outcomes, and Unfinished Business. *Politics and the Life Sciences*, *16*(1), 105–126. https://doi.org/10.1017/S0730938400020311

Daniele, L. (2024). Incidentality of the civilian harm in international humanitarian law and its Contra Legem antonyms in recent discourses on the laws of war. *Journal of Conflict and Security Law*, *29*(1), 21–54. https://doi.org/10.1093/jcsl/krae004

D'Ascanio, M. (2017). The Arms Trade Treaty: A Commentary Andrew Clapham, Stuart Casey-Maslen, Gilles Giacca and Sarah Parker. *International Review of the Red Cross*, *99*(904), 459–462. https://doi.org/10.1017/S1816383118000073

Dent, C. (2021). Patents over military equipment: Shifting uses for shifting modes of governance. *Griffith Law Review*, *30*(2), 295–312. https://doi.org/10.1080/10383441.2021.1925410

Dunworth, T. (Ed.). (2020). Humanitarian Disarmament Rising: The Vietnam War and the Campaigns against Indiscriminate Weapons. In *Humanitarian Disarmament: An Historical Enquiry* (pp. 80–111). Cambridge University Press. https://doi.org/10.1017/9781108644105.004

Ferreira, C. V., Biesek, F. L., & Scalice, R. K. (2021). Product innovation management model based on manufacturing readiness level (MRL), design for manufacturing and assembly (DFMA) and technology readiness level (TRL). *Journal of the Brazilian Society of Mechanical Sciences and Engineering*, *43*, 360. https://doi.org/10.1007/s40430-021-03080-8

Gkagkas, G., Vergados, D. J., Michalas, A., & Dossis, M. (2024). The Advantage of the 5G Network for Enhancing the Internet of Things and the Evolution of the 6G Network. *Sensors*, *24*(8), 2455. https://doi.org/10.3390/s24082455

Goodman, R. (2013). The Power to Kill or Capture Enemy Combatants. *European Journal of International Law*, *24*(3), 819–853. https://doi.org/10.1093/ejil/cht048

Gottwald, J., Buch, L. F., & Leal Filho, W. (2013). Technology Transfer. In S. O. Idowu, N. Capaldi, L. Zu, & A. D. Gupta (Eds.), *Encyclopedia of Corporate Social Responsibility* (pp. 2503–2511). Springer. https://doi.org/10.1007/978-3-642-28036-8_673

Gunaratne, P. R. (2013). US Drone Strikes and their Impact on International Security in a Post 9/11 World. *Journal of the Royal Asiatic Society of Sri Lanka*, *58*(2), 73–93.

Haines, S. (2014). 1907 Hague Convention VIII Relative to the Laying of Automatic Submarine Contact Mines. *International Law Studies*, *90*, 412–445.

Hampson, F. J. (2018). Law of War/Law of Armed Conflict/International Humanitarian Law. In M. J. Bowman, & D. Kritsiotis (Eds.), *Conceptual and Contextual Perspectives on the Modern Law of Treaties* (pp. 538–577). Cambridge University Press. https://doi.org/10.1017/9781316179031.019

Hashimy, S. Q. (2023). The Agonising Narrative of Environmental Dilapidation in the tussle of Armed Conflict; From the Lens of International Humanitarian Laws. *Journal of Global Ecology and Environment*, *17*(2), 45–59. https://doi.org/10.56557/jogee/2023/v17i28145

Hashimy, S. Q. (2024). Justice for Victims of Atrocity Crimes: The ICC's Pursuit in the Prosecution of War Crimes in Afghanistan. *Eastern Africa Journal on International Humanitarian Law*, *3*(1), 49–111. https://doi.org/10.2139/ssrn.4352525

Hashimy, S. Q., & Benjamin, M. S. (2023). Exploring the Complexities of the Russia-Ukraine Conflict: A Close Look from the Lens of International Law and Global Responses. *The Indian Journal of Politics*, *57*(3–4), 91–125.

Jain, V., & Gill, S. (2022). Atmanirbhar Bharat: India's Quest for Self-reliance in Post-Covid-19 World. *Journal of Polity and Society*, *14*(2), 109–123.

Jarose, J. (2024). A Sleeping Giant? The ENMOD Convention as a Limit on Intentional Environmental Harm in Armed Conflict and Beyond. *American Journal of International Law*, *118*(3), 468–511. https://doi.org/10.1017/ajil.2024.15

Jayaram, D. (2024). Shifting discourses of climate security in India: Domestic and international dimensions. *Third World Quarterly*, *45*(14), 2108–2126. https://doi.org/10.1080/01436597.2024.2314003

Johnson, J., & Johnson, J. (2023). *AI and the Bomb: Nuclear Strategy and Risk in the Digital Age*. Oxford University Press.

Kaldor, M. (1986). The Weapons Succession Process. *World Politics*, *38*(4), 577–595. https://doi.org/10.2307/2010167

Kelemen, R. D., & McNamara, K. R. (2022). State-building and the European Union: Markets, War, and Europe's Uneven Political Development. *Comparative Political Studies*, *55*(6), 963–991. https://doi.org/10.1177/00104140211047393

Kim, H., Park, B. I., Al-Tabbaa, O., & Khan, Z. (2024). Knowledge transfer and protection in international joint ventures: An integrative review. *International Business Review*, *33*(5), 102300. https://doi.org/10.1016/j.ibusrev.2024.102300

Kiss, A.-C., & Lammers, J. G. (Eds.). (2021). *Hague Yearbook of International Law / Annuaire de La Haye de Droit International* (Vol. 13 (2000)). Brill.

Lak, M. W. J. (2009). Note on the Chemical Weapons Convention's Second Review Conference, Held at The Hague on 7–18 April 2008. *Journal of Conflict and Security Law*, *14*(2), 353–381. https://doi.org/10.1093/jcsl/krp022

Larik, J. (2023). EU law and the governance of Global Spaces: Ambitions, constraints and legal creativity. *Journal of European Integration*, *45*(8), 1125–1142. https://doi.org/10.1080/07036337.2023.2270670

Li, L. (2008). India's Security Concept and Its China Policy in the Post-Cold War Era. *The Chinese Journal of International Politics*, *2*(2), 229–261. https://doi.org/10.1093/cjip/pon009

Liivoja, R. (2024). Protecting Warfighters from Superfluous Injury and Unnecessary Suffering. In M. Killingsworth & T. McCormack (Eds.), *Civility, Barbarism and the Evolution of International Humanitarian Law: Who do the Laws of War Protect?* (pp. 177–199). Cambridge University Press. https://doi.org/10.1017/9781108764049.010

Lupu, Y., & Wallace, G. P. R. (2024). The Laws of War and Public Support for Foreign Combatants. *International Organization*, *78*(4), 823–852. https://doi.org/10.1017/S0020818324000274

Lustgarten, L. (2015). The arms trade treaty: achievements, failings, future. *International & Comparative Law Quarterly*, *64*(3), 569–600. https://doi.org/10.1017/S0020589315000202

Maskus, K. E. (2022). The International Intellectual Property System from an Economist's Perspective. In H. Grosse Ruse-Khan, & A. Metzger (Eds.), *Intellectual Property Ordering beyond Borders* (pp. 3–27). Cambridge University Press. https://doi.org/10.1017/9781009071338.003

McClean, D. (2002). The Hague Convention on International Child Abduction. By Paul R. Beaumont and Peter E. McEleavy [Oxford: Oxford University Press, 1999, ISBN 0–19–826064–4. xxv + 332 pp £65]. *International & Comparative Law Quarterly*, *51*(1), 188–189. https://doi.org/10.1093/iclq/51.1.188

McClelland, J. (2003). The review of weapons in accordance with Article 36 of Additional Protocol I. *International Review of the Red Cross*, *85*(850), 397–415. https://doi.org/10.1017/S0035336100115229 дои не найден

McElroy, R. J. (1991). The Geneva Protocol of 1925. In M. Krepon, & D. Caldwell (Eds.), *The Politics of Arms Control Treaty Ratification* (pp. 125–166). Palgrave Macmillan US. https://doi.org/10.1007/978-1-137-04534-8_4

McKinnon, C. (Ed.). (2008). *Issues in Political Theory*. Oxford University Press.

Mearsheimer, J. J. (2022). The Causes and Consequences of the Ukraine War. *Horizons: Journal of International Relations and Sustainable Development*, *21*, 12–27.

Melzer, N. (2008). The Principle of Distinction under International Humanitarian Law. In N. Melzer (Ed.), *Targeted Killing in International Law* (pp. 300–366). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199533169.003.0011

Muchlinski, P. T. (2021). Intellectual Property and Technology Transfer. In P. T. Muchlinski (Ed.), *Multinational Enterprises and the Law* (3rd Ed., pp. 469–508). Oxford University Press. https://doi.org/10.1093/law/9780198824138.003.0012

Nadkarni, V., D'Anieri, P., Kerr, S., Sharafutdinova, G., Pu, X., Ollapally, D. M., Velasco Junior, P., Moore, C., & Divsallar, A. (2024). Forum: The Russia – Ukraine War and Reactions from the Global South. *The Chinese Journal of International Politics*, *17*(4), 449–489. https://doi.org/10.1093/cjip/poae021

Nedeski, N. (Ed.). (2022a). The Distinction between Bilateral and Multilateral Legal Relations in the International Law of Obligations. In *Shared Obligations in International Law* (pp. 54–96). Cambridge University Press. https://doi.org/10.1017/9781108893985.003

Nedeski, N. (Ed.). (2022b). The Distinction between Bilateral and Multilateral Legal Relations in the International Law of Obligations. In *Shared Obligations in International Law* (pp. 54–96). Cambridge University Press. https://doi.org/10.1017/9781108893985.003

Ní Shúilleabháin, M., & Trimmings, K. (2024). The Hague Convention on the Recognition of Divorces and Legal Separations 1970: An effective mechanism for regulating divorce as between the UK and the EU post-Brexit? *International Journal of Law, Policy and the Family*, *38*(1), ebae019. https://doi.org/10.1093/lawfam/ebae019

Olechowski, A. L., Eppinger, S. D., Joglekar, N., & Tomaschek, K. (2020). Technology readiness levels: Shortcomings and improvement opportunities. *Systems Engineering*, *23*(4), 395–408. https://doi.org/10.1002/sys.21533

Osano, H. M., & Koine, P. W. (2016). Role of foreign direct investment on technology transfer and economic growth in Kenya: A case of the energy sector. *Journal of Innovation and Entrepreneurship*, *5*(1), 31. https://doi.org/10.1186/s13731-016-0059-3

Osimen, G. U., Newo, O., & Fulani, O. M. (2024). Artificial intelligence and arms control in modern warfare. *Cogent Social Sciences*, *10*(1), 2407514. https://doi.org/10.1080/23311886.2024.2407514

Pandey, N., de Coninck, H., & Sagar, A. D. (2022). Beyond technology transfer: Innovation cooperation to advance sustainable development in developing countries. *WIREs Energy and Environment*, *11*(2), e422. https://doi.org/10.1002/wene.422

Peters, A. (2017). The refinement of international law: From fragmentation to regime interaction and politicization. *International Journal of Constitutional Law*, *15*(3), 671–704. https://doi.org/10.1093/icon/mox056

Pomson, O. (2023). 'Objects'? The Legal Status of Computer Data under International Humanitarian Law. *Journal of Conflict and Security Law*, *28*(2), 349–387. https://doi.org/10.1093/jcsl/krad002

Qi, Y., & Chu, X. (2022). Development of the digital economy, transformation of the economic structure and leaping of the middle-income trap. *China Political Economy*, *5*(1), 14–39. https://doi.org/10.1108/CPE-09-2022-0012

Raslan, R. A. A. (2024). Climbing up the Ladder: Technology Transfer-Related Policies in the Context of the Belt and Road Initiative. *Utrecht Law Review*, *20*(1), 19–43. https://doi.org/10.36633/ulr.922

Ratner, S. R. (2011). Law Promotion Beyond Law Talk: The Red Cross, Persuasion, and the Laws of War. *European Journal of International Law*, *22*(2), 459–506. https://doi.org/10.1093/ejil/chr025

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Saeed, L. (2025). The Impact of Military Expenditures on Economic Growth: A New Instrumental Variables Approach. *Defence and Peace Economics*, *36*(1), 86–101. https://doi.org/10.1080/10242694.2023.2259651

Schindler, D., & Toman, J. (2004a). No. 9 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight. In *The Laws of Armed Conflicts* (pp. 91–93). Brill. https://doi.org/10.1163/9789047405238_012

Schindler, D., & Toman, J. (2004b). No. 25 Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons. In *The Laws of Armed Conflicts* (pp. 309–313). Brill. https://doi.org/10.1163/9789047405238_029

Schmitt, M. N. (2008). The Principle of Distinction and Weapon Systems on the Contemporary Battlefield. *Connections: The Quarterly Journal*, *7*(1), 46–56. https://doi.org/10.11610/connections.07.1.03

Sinha, S. (2023). India's Military Modernisation: Role and Impact of France. *Journal of Asian Security and International Affairs*, *10*(3), 325–341. https://doi.org/10.1177/23477970231207256

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Spulber, D. F. (2023). Antitrust and Innovation Competition. *Journal of Antitrust Enforcement*, *11*(1), 5–50. https://doi.org/10.1093/jaenfo/jnac013

Stahn, C. (2006). 'Jus ad bellum', 'jus in bello'... 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force. *European Journal of International Law*, *17*(5), 921–943. https://doi.org/10.1093/ejil/chl037

Stoll, P.-T. (2022). Hybrid International Intellectual Property Protection: Coherence, Governance and Balance. In H. Grosse Ruse-Khan, & A. Metzger (Eds.), *Intellectual Property Ordering beyond Borders* (pp. 96–118). Cambridge University Press. https://doi.org/10.1017/9781009071338.006

Strachan, H. (2020). Michael Howard and the dimensions of military history. *War in History*, *27*(4), 536–551. https://doi.org/10.1177/0968344520915028

Szenes, Z. (2023). Reinforcing deterrence: Assessing NATO's 2022 Strategic Concept. *Defense & Security Analysis*, *39*(4), 539–560. https://doi.org/10.1080/14751798.2023.2270230

Tabassi, L. (2007). The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention). In G. Ulfstein (Ed.), *Making Treaties Work: Human Rights, Environment and Arms Control* (pp. 273–300). Cambridge University Press. https://doi.org/10.1017/CBO9780511494345.013

Traven, D. (Ed.). (2021). Humanizing Hell: The Hague Peace Conferences and the Second World War, 1899–1945. In *Law and Sentiment in International Politics: Ethics, Emotions, and the Evolution of the Laws of War* (pp. 193–237). Cambridge University Press. https://doi.org/10.1017/9781108954280.009

Upreti, P. N. (2022). A TWAIL critique of intellectual property and related disputes in investor-state dispute settlement. *The Journal of World Intellectual Property*, *25*(1), 220–237. https://doi.org/10.1111/jwip.12217

van den Boogaard, J. (Ed.). (2023). The Concept of Proportionality in International Humanitarian Law. In *Proportionality in International Humanitarian Law: Refocusing the Balance in Practice* (pp. 51–87). Cambridge University Press. https://doi.org/10.1017/9781108954648.007

Van Norman, G. A., & Eisenkot, R. (2017). Technology Transfer: From the Research Bench to Commercialization: Part 2: The Commercialization Process. *JACC: Basic to Translational Science*, *2*(2), 197–208. https://doi.org/10.1016/j.jacbts.2017.03.004

Vidigal, G. (2013). From Bilateral to Multilateral Law-making: Legislation, Practice, Evolution and the Future of Inter Se Agreements in the WTO. *European Journal of International Law*, *24*(4), 1027–1053. https://doi.org/10.1093/ejil/cht064

Villiger, M. E. (2008). *Commentary on the 1969 Vienna Convention on the Law of Treaties*. Brill. https://doi.org/10.1163/ej.9789004168046.i-1058

Webster, A. (2011). Hague Conventions (1899, 1907). In *The Encyclopedia of War*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781444338232.wbeow271

Whittle, D. (2015). The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action. *European Journal of International Law*, *26*(3), 671–698. https://doi.org/10.1093/ejil/chv042

Winter, E. (2022). The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law. *Journal of Conflict and Security Law*, *27*(1), 1–20. https://doi.org/10.1093/jcsl/krac001

Wired for War: The Robotics Revolution and Conflict in the 21st Century, P.W. Singer (New York: Penguin, 2009), 512 pp., $30 cloth. (2009). *Ethics & International Affairs*, *23*(3), 312–313. https://doi.org/10.1111/j.1747-7093.2009.00222_4.x

Authors information

Nisha Bhaskar – LLM, Researcher, The West Bengal National University of Juridical Sciences
Address: 12 LB Block, Sector III, Salt Lake, Kolkata 700098, West Bengal, India
E-mail: nishabhaskar414@gmail.com
ORCID ID: https://orcid.org/0009-0005-9128-1526

Jackson Simango Magoge – LLM (Corporate and Commercial Law), Assistant Lecturer, Department of Humanities and Social Sciences, National Institute of Transport
Address: Mabibo, Ubungo, P.O. Box 705, Dar es Salaam, 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

Sayed Qudrat Hashimy – PhD Scholar, LLM (International Law), Research Scholar (Law), Department of Studies in Law, University of Mysore
Address: Manasagangotri, Mysore 570005, India
E-mail: sayedqudrathashim@law.uni-mysore.ac.in
ORCID ID: https://orcid.org/0000-0001-9835-0575

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 – February 13, 2025
Date of approval – March 2, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:341.3:004.8
EDN: https://elibrary.ru/ifibfo
DOI: https://doi.org/10.21202/jdtl.2025.10

Передача технологий в эпоху военных конфликтов: правовые вызовы для международной торговли и международного гуманитарного права

Ниша Бхаскар ✉

Национальный юридический университет Западной Бенгалии, Калькутта, Индия

Джексон Симанго Магоге

Национальный институт транспорта, Дар-эс-Салам, Танзания

Саид Кудрат Хашими

Майсурский университет, Майсур, Индия

Ключевые слова

военное право,
Гаагские конвенции,
Женевские конвенции,
искусственный интеллект,
международная торговля,
международное гуманитарное право,
передача технологий,
право,
средства ведения войны,
цифровые технологии

Аннотация

Цель: настоящее исследование направлено на выявление сложных взаимосвязей между международной торговлей и военным правом в контексте передачи технологий, а также на анализ правовых последствий технологических трансферов для международного гуманитарного права с целью прояснения влияния передачи технологий в международной торговле на регулирование средств ведения войны и определения правовых пробелов в существующих международных конвенциях.

Методы: в исследовании применяется комплексный правовой анализ международных документов, включая Женевские конвенции и дополнительные протоколы к ним, Гаагские конвенции, а также современные международные соглашения в области торговли и технологий. Использован сравнительно-правовой метод для изучения национальных законодательств различных государств, а также системный подход к анализу взаимодействия норм международного гуманитарного права и международного торгового права.

Результаты: исследование выявило существенные правовые пробелы в регулировании передачи технологий двойного назначения в военное время. Установлено, что современные технологии, включая искусственный интеллект, автономные системы вооружений

✉ Корреспондирующий автор

и кибернетические средства, создают регулятивный вакуум, который подрывает эффективность существующих международных конвенций. Продемонстрирован значительный технологический разрыв между странами Глобального Севера и Юга.

Научная новизна: работа представляет первое комплексное исследование эволюции технологий в контексте международного гуманитарного права с акцентом на необходимость разработки специальных механизмов регулирования. Предложена концептуальная модель интеграции норм передачи технологий в систему международных договоров о разоружении с учетом принципов пропорциональности и различия.

Практическая значимость: исследование предлагает конкретные поправки к статьям Женевских конвенций, включая модификацию статьи 35(2) Дополнительного протокола I для включения новых технологий и расширение требований ст. 36 относительно правовых обзоров технологических трансферов. Разработанные рекомендации могут служить основой для создания международных механизмов мониторинга и повышения прозрачности в сфере передачи военных технологий.

Для цитирования

Бхаскар, Н., Магоге, Дж. С., Хашими, С. К. (2025). Передача технологий в эпоху военных конфликтов: правовые вызовы для международной торговли и международного гуманитарного права. *Journal of Digital Technologies and Law*, *3*(2), 222–258. https://doi.org/10.21202/jdtl.2025.10

Список литературы

Al Karawi, Z. K. M. (2024). The hague conventions: cornerstone of modern international law. *Russian Law Journal*, *12*(1), 2027–2033.

Alexander, A. (2015). A Short History of International Humanitarian Law. *European Journal of International Law*, *26*(1), 109–138. https://doi.org/10.1093/ejil/chv002

Anderman, S., & Kallaugher, J. (2006). *Technology Transfer and The New Eu Competition Rules: Intellectual Property Licensing After Modernisation* (Oxford, 2006; online edn, Oxford Academic, 31 Oct. 2023). https://doi.org/10.1093/oso/9780199282142.001.0001

Ansari, S., & Babu, R. R. (2018). 5. North American Free Trade Agreement (NAFTA). *Yearbook of International Environmental Law*, *29*, 390–397. https://doi.org/10.1093/yiel/yvz032

Ayamga, M., Akaba, S., & Nyaaba, A. A. (2021). Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change*, *167*, 120677. https://doi.org/10.1016/j.techfore.2021.120677

Azam, M. (2020). Does military spending stifle economic growth? The empirical evidence from non-OECD countries. *Heliyon*, *6*(12), e05853. https://doi.org/10.1016/j.heliyon.2020.e05853

Baltag, C., Joshi, R., & Duggal, K. (2023). Recent Trends in Investment Arbitration on the Right to Regulate, Environment, Health and Corporate Social Responsibility: Too Much or Too Little? *ICSID Review – Foreign Investment Law Journal*, *38*(2), 381–421. https://doi.org/10.1093/icsidreview/siac031

Beard, J. (2019). The Principle of Proportionality in an Era of High Technology. In W. S. Williams, & C. M. Ford (Eds.), *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare* (pp. 261–288). Oxford University Press. https://doi.org/10.1093/oso/9780190915360.003.0009

Bethlehem, D., McRae, D., Neufeld, R., & Van Damme, I. (Eds.). (2009). *The Oxford Handbook of International Trade Law*. Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199231928.013.0001

Bothe, M. (2017). The International Committee of the Red Cross and the Additional Protocols of 1977. In R. Geiß, A. Zimmermann, & S. Haumer (Eds.), *Humanizing the Laws of War: The Red Cross and the Development of International Humanitarian Law* (pp. 57–80). Cambridge University Press. https://doi.org/10.1017/9781316759967.004

Boyle, M. J. (2013). The costs and consequences of drone warfare. *International Affairs*, *89*(1), 1–29. https://doi.org/10.1111/1468-2346.12002

Byrne, M. (2016). Consent and the use of force: An examination of 'intervention by invitation' as a basis for US drone strikes in Pakistan, Somalia and Yemen. *Journal on the Use of Force and International Law*, *3*(1), 97–125. https://doi.org/10.1080/20531702.2015.1135658

Cassese, A. (2008). Weapons Causing Unnecessary Suffering: Are They Prohibited? In A. Cassese, P. Gaeta, & S. Zappalà (Eds.), *The Human Dimension of International Law: Selected Papers of Antonio Cassese* (pp. 192–217). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199232918.003.0009

Chapter Seven: Latin America and the Caribbean: Regional trends in 2024 380; Regional defence policy and economics 382; Arms procurement and defence-industrial trends 392; Armed forces data section 393. (2025). *The Military Balance*, *125*(1), 380–439. https://doi.org/10.1080/04597222.2025.2445479

Cheng, T. K. (2021). Technology Transfers in Developing Countries. In T. K. Cheng (Ed.), *The Patent-Competition Interface in Developing Countries* (pp. 54–81). Oxford University Press. https://doi.org/10.1093/oso/9780192857354.003.0003

Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, *35*(1), 29–54. https://doi.org/10.1017/S0922156521000534

Chinkin, C. M. (1989). The Challenge of Soft Law: Development and Change in International Law. *The International and Comparative Law Quarterly*, *38*(4), 850–866. https://doi.org/10.1093/iclqaj/38.4.850

Clapham, A., Casey-Maslen, S., Giacca, G., & Parker, S. (2016). *The Arms Trade Treaty: A Commentary*. Oxford University Press.

Copeland, D. C. (1996). Economic Interdependence and War: A Theory of Trade Expectations. *International Security*, *20*(4), 5–41. https://doi.org/10.2307/2539041

Copeland, D., Liivoja, R., & Sanders, L. (2023). The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems. *Journal of Conflict and Security Law*, *28*(2), 285–316. https://doi.org/10.1093/jcsl/krac035

Ezell, St., & Cory, N. (2019). *The Way Forward for Intellectual Property Internationally*. ITIF.

da Silva, C., & Wood, B. (Eds.). (2021). *The Arms Trade Treaty: Weapons and International Law*. Intersentia. https://doi.org/10.1017/9781839701603

Dando, M. R., & Pearson, G. S. (1997). The Fourth Review Conference of the Biological and Toxin Weapons Convention: Issues, Outcomes, and Unfinished Business. *Politics and the Life Sciences*, *16*(1), 105–126. https://doi.org/10.1017/S0730938400020311

Daniele, L. (2024). Incidentality of the civilian harm in international humanitarian law and its Contra Legem antonyms in recent discourses on the laws of war. *Journal of Conflict and Security Law*, *29*(1), 21–54. https://doi.org/10.1093/jcsl/krae004

D'Ascanio, M. (2017). The Arms Trade Treaty: A Commentary Andrew Clapham, Stuart Casey-Maslen, Gilles Giacca and Sarah Parker. *International Review of the Red Cross*, *99*(904), 459–462. https://doi.org/10.1017/S1816383118000073

Dent, C. (2021). Patents over military equipment: Shifting uses for shifting modes of governance. *Griffith Law Review*, *30*(2), 295–312. https://doi.org/10.1080/10383441.2021.1925410

Dunworth, T. (Ed.). (2020). Humanitarian Disarmament Rising: The Vietnam War and the Campaigns against Indiscriminate Weapons. In *Humanitarian Disarmament: An Historical Enquiry* (pp. 80–111). Cambridge University Press. https://doi.org/10.1017/9781108644105.004

Ferreira, C. V., Biesek, F. L., & Scalice, R. K. (2021). Product innovation management model based on manufacturing readiness level (MRL), design for manufacturing and assembly (DFMA) and technology readiness level (TRL). *Journal of the Brazilian Society of Mechanical Sciences and Engineering*, *43*, 360. https://doi.org/10.1007/s40430-021-03080-8

Gkagkas, G., Vergados, D. J., Michalas, A., & Dossis, M. (2024). The Advantage of the 5G Network for Enhancing the Internet of Things and the Evolution of the 6G Network. *Sensors*, *24*(8), 2455. https://doi.org/10.3390/s24082455

Goodman, R. (2013). The Power to Kill or Capture Enemy Combatants. *European Journal of International Law*, *24*(3), 819–853. https://doi.org/10.1093/ejil/cht048

Gottwald, J., Buch, L. F., & Leal Filho, W. (2013). Technology Transfer. In S. O. Idowu, N. Capaldi, L. Zu, & A. D. Gupta (Eds.), *Encyclopedia of Corporate Social Responsibility* (pp. 2503–2511). Springer. https://doi.org/10.1007/978-3-642-28036-8_673

Gunaratne, P. R. (2013). US Drone Strikes and their Impact on International Security in a Post 9/11 World. *Journal of the Royal Asiatic Society of Sri Lanka*, *58*(2), 73–93.

Haines, S. (2014). 1907 Hague Convention VIII Relative to the Laying of Automatic Submarine Contact Mines. *International Law Studies*, *90*, 412–445.

Hampson, F. J. (2018). Law of War/Law of Armed Conflict/International Humanitarian Law. In M. J. Bowman, & D. Kritsiotis (Eds.), *Conceptual and Contextual Perspectives on the Modern Law of Treaties* (pp. 538–577). Cambridge University Press. https://doi.org/10.1017/9781316179031.019

Hashimy, S. Q. (2023). The Agonising Narrative of Environmental Dilapidation in the tussle of Armed Conflict; From the Lens of International Humanitarian Laws. *Journal of Global Ecology and Environment*, *17*(2), 45–59. https://doi.org/10.56557/jogee/2023/v17i28145

Hashimy, S. Q. (2024). Justice for Victims of Atrocity Crimes: The ICC's Pursuit in the Prosecution of War Crimes in Afghanistan. *Eastern Africa Journal on International Humanitarian Law*, *3*(1), 49–111. https://doi.org/10.2139/ssrn.4352525

Hashimy, S. Q., & Benjamin, M. S. (2023). Exploring the Complexities of the Russia-Ukraine Conflict: A Close Look from the Lens of International Law and Global Responses. *The Indian Journal of Politics*, *57*(3–4), 91–125.

Jain, V., & Gill, S. (2022). Atmanirbhar Bharat: India's Quest for Self-reliance in Post-Covid-19 World. *Journal of Polity and Society*, *14*(2), 109–123.

Jarose, J. (2024). A Sleeping Giant? The ENMOD Convention as a Limit on Intentional Environmental Harm in Armed Conflict and Beyond. *American Journal of International Law*, *118*(3), 468–511. https://doi.org/10.1017/ajil.2024.15

Jayaram, D. (2024). Shifting discourses of climate security in India: Domestic and international dimensions. *Third World Quarterly*, *45*(14), 2108–2126. https://doi.org/10.1080/01436597.2024.2314003

Johnson, J., & Johnson, J. (2023). *AI and the Bomb: Nuclear Strategy and Risk in the Digital Age*. Oxford University Press.

Kaldor, M. (1986). The Weapons Succession Process. *World Politics*, *38*(4), 577–595. https://doi.org/10.2307/2010167

Kelemen, R. D., & McNamara, K. R. (2022). State-building and the European Union: Markets, War, and Europe's Uneven Political Development. *Comparative Political Studies*, *55*(6), 963–991. https://doi.org/10.1177/00104140211047393

Kim, H., Park, B. I., Al-Tabbaa, O., & Khan, Z. (2024). Knowledge transfer and protection in international joint ventures: An integrative review. *International Business Review*, *33*(5), 102300. https://doi.org/10.1016/j.ibusrev.2024.102300

Kiss, A.-C., & Lammers, J. G. (Eds.). (2021). *Hague Yearbook of International Law / Annuaire de La Haye de Droit International* (Vol. 13 (2000)). Brill.

Lak, M. W. J. (2009). Note on the Chemical Weapons Convention's Second Review Conference, Held at The Hague on 7–18 April 2008. *Journal of Conflict and Security Law*, *14*(2), 353–381. https://doi.org/10.1093/jcsl/krp022

Larik, J. (2023). EU law and the governance of Global Spaces: Ambitions, constraints and legal creativity. *Journal of European Integration*, *45*(8), 1125–1142. https://doi.org/10.1080/07036337.2023.2270670

Li, L. (2008). India's Security Concept and Its China Policy in the Post-Cold War Era. *The Chinese Journal of International Politics*, *2*(2), 229–261. https://doi.org/10.1093/cjip/pon009

Liivoja, R. (2024). Protecting Warfighters from Superfluous Injury and Unnecessary Suffering. In M. Killingsworth & T. McCormack (Eds.), *Civility, Barbarism and the Evolution of International Humanitarian Law: Who do the Laws of War Protect?* (pp. 177–199). Cambridge University Press. https://doi.org/10.1017/9781108764049.010

Lupu, Y., & Wallace, G. P. R. (2024). The Laws of War and Public Support for Foreign Combatants. *International Organization*, *78*(4), 823–852. https://doi.org/10.1017/S0020818324000274

Lustgarten, L. (2015). The arms trade treaty: achievements, failings, future. *International & Comparative Law Quarterly*, *64*(3), 569–600. https://doi.org/10.1017/S0020589315000202

Maskus, K. E. (2022). The International Intellectual Property System from an Economist's Perspective. In H. Grosse Ruse-Khan, & A. Metzger (Eds.), *Intellectual Property Ordering beyond Borders* (pp. 3–27). Cambridge University Press. https://doi.org/10.1017/9781009071338.003

McClean, D. (2002). The Hague Convention on International Child Abduction. By Paul R. Beaumont and Peter E. McEleavy [Oxford: Oxford University Press, 1999, ISBN 0–19–826064–4. xxv + 332 pp £65]. *International & Comparative Law Quarterly*, *51*(1), 188–189. https://doi.org/10.1093/iclq/51.1.188

McClelland, J. (2003). The review of weapons in accordance with Article 36 of Additional Protocol I. *International Review of the Red Cross*, *85*(850), 397–415. https://doi.org/10.1017/S0035336100115229 дои не найден

McElroy, R. J. (1991). The Geneva Protocol of 1925. In M. Krepon, & D. Caldwell (Eds.), *The Politics of Arms Control Treaty Ratification* (pp. 125–166). Palgrave Macmillan US. https://doi.org/10.1007/978-1-137-04534-8_4

McKinnon, C. (Ed.). (2008). *Issues in Political Theory*. Oxford University Press.

Mearsheimer, J. J. (2022). The Causes and Consequences of the Ukraine War. *Horizons: Journal of International Relations and Sustainable Development*, *21*, 12–27.

Melzer, N. (2008). The Principle of Distinction under International Humanitarian Law. In N. Melzer (Ed.), *Targeted Killing in International Law* (pp. 300–366). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199533169.003.0011

Muchlinski, P. T. (2021). Intellectual Property and Technology Transfer. In P. T. Muchlinski (Ed.), *Multinational Enterprises and the Law* (3rd Ed., pp. 469–508). Oxford University Press. https://doi.org/10.1093/law/9780198824138.003.0012

Nadkarni, V., D'Anieri, P., Kerr, S., Sharafutdinova, G., Pu, X., Ollapally, D. M., Velasco Junior, P., Moore, C., & Divsallar, A. (2024). Forum: The Russia – Ukraine War and Reactions from the Global South. *The Chinese Journal of International Politics*, *17*(4), 449–489. https://doi.org/10.1093/cjip/poae021

Nedeski, N. (Ed.). (2022a). The Distinction between Bilateral and Multilateral Legal Relations in the International Law of Obligations. In *Shared Obligations in International Law* (pp. 54–96). Cambridge University Press. https://doi.org/10.1017/9781108893985.003

Nedeski, N. (Ed.). (2022b). The Distinction between Bilateral and Multilateral Legal Relations in the International Law of Obligations. In *Shared Obligations in International Law* (pp. 54–96). Cambridge University Press. https://doi.org/10.1017/9781108893985.003

Ní Shúilleabháin, M., & Trimmings, K. (2024). The Hague Convention on the Recognition of Divorces and Legal Separations 1970: An effective mechanism for regulating divorce as between the UK and the EU post-Brexit? *International Journal of Law, Policy and the Family*, *38*(1), ebae019. https://doi.org/10.1093/lawfam/ebae019

Olechowski, A. L., Eppinger, S. D., Joglekar, N., & Tomaschek, K. (2020). Technology readiness levels: Shortcomings and improvement opportunities. *Systems Engineering*, *23*(4), 395–408. https://doi.org/10.1002/sys.21533

Osano, H. M., & Koine, P. W. (2016). Role of foreign direct investment on technology transfer and economic growth in Kenya: A case of the energy sector. *Journal of Innovation and Entrepreneurship*, *5*(1), 31. https://doi.org/10.1186/s13731-016-0059-3

Osimen, G. U., Newo, O., & Fulani, O. M. (2024). Artificial intelligence and arms control in modern warfare. *Cogent Social Sciences*, *10*(1), 2407514. https://doi.org/10.1080/23311886.2024.2407514

Pandey, N., de Coninck, H., & Sagar, A. D. (2022). Beyond technology transfer: Innovation cooperation to advance sustainable development in developing countries. *WIREs Energy and Environment*, *11*(2), e422. https://doi.org/10.1002/wene.422

Peters, A. (2017). The refinement of international law: From fragmentation to regime interaction and politicization. *International Journal of Constitutional Law*, *15*(3), 671–704. https://doi.org/10.1093/icon/mox056

Pomson, O. (2023). 'Objects'? The Legal Status of Computer Data under International Humanitarian Law. *Journal of Conflict and Security Law*, *28*(2), 349–387. https://doi.org/10.1093/jcsl/krad002

Qi, Y., & Chu, X. (2022). Development of the digital economy, transformation of the economic structure and leaping of the middle-income trap. *China Political Economy*, *5*(1), 14–39. https://doi.org/10.1108/CPE-09-2022-0012

Raslan, R. A. A. (2024). Climbing up the Ladder: Technology Transfer-Related Policies in the Context of the Belt and Road Initiative. *Utrecht Law Review*, *20*(1), 19–43. https://doi.org/10.36633/ulr.922

Ratner, S. R. (2011). Law Promotion Beyond Law Talk: The Red Cross, Persuasion, and the Laws of War. *European Journal of International Law*, *22*(2), 459–506. https://doi.org/10.1093/ejil/chr025

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Saeed, L. (2025). The Impact of Military Expenditures on Economic Growth: A New Instrumental Variables Approach. *Defence and Peace Economics*, *36*(1), 86–101. https://doi.org/10.1080/10242694.2023.2259651

Schindler, D., & Toman, J. (2004a). No. 9 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight. In *The Laws of Armed Conflicts* (pp. 91–93). Brill. https://doi.org/10.1163/9789047405238_012

Schindler, D., & Toman, J. (2004b). No. 25 Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons. In *The Laws of Armed Conflicts* (pp. 309–313). Brill. https://doi.org/10.1163/9789047405238_029

Schmitt, M. N. (2008). The Principle of Distinction and Weapon Systems on the Contemporary Battlefield. *Connections: The Quarterly Journal*, *7*(1), 46–56. https://doi.org/10.11610/connections.07.1.03

Sinha, S. (2023). India's Military Modernisation: Role and Impact of France. *Journal of Asian Security and International Affairs*, *10*(3), 325–341. https://doi.org/10.1177/23477970231207256

Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

Spulber, D. F. (2023). Antitrust and Innovation Competition. *Journal of Antitrust Enforcement*, *11*(1), 5–50. https://doi.org/10.1093/jaenfo/jnac013

Stahn, C. (2006). 'Jus ad bellum', 'jus in bello'… 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force. *European Journal of International Law*, *17*(5), 921–943. https://doi.org/10.1093/ejil/chl037

Stoll, P.-T. (2022). Hybrid International Intellectual Property Protection: Coherence, Governance and Balance. In H. Grosse Ruse-Khan, & A. Metzger (Eds.), *Intellectual Property Ordering beyond Borders* (pp. 96–118). Cambridge University Press. https://doi.org/10.1017/9781009071338.006

Strachan, H. (2020). Michael Howard and the dimensions of military history. *War in History*, *27*(4), 536–551. https://doi.org/10.1177/0968344520915028

Szenes, Z. (2023). Reinforcing deterrence: Assessing NATO's 2022 Strategic Concept. *Defense & Security Analysis*, *39*(4), 539–560. https://doi.org/10.1080/14751798.2023.2270230

Tabassi, L. (2007). The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention). In G. Ulfstein (Ed.), *Making Treaties Work: Human Rights, Environment and Arms Control* (pp. 273–300). Cambridge University Press. https://doi.org/10.1017/CBO9780511494345.013

Traven, D. (Ed.). (2021). Humanizing Hell: The Hague Peace Conferences and the Second World War, 1899–1945. In *Law and Sentiment in International Politics: Ethics, Emotions, and the Evolution of the Laws of War* (pp. 193–237). Cambridge University Press. https://doi.org/10.1017/9781108954280.009

Upreti, P. N. (2022). A TWAIL critique of intellectual property and related disputes in investor-state dispute settlement. *The Journal of World Intellectual Property*, *25*(1), 220–237. https://doi.org/10.1111/jwip.12217

van den Boogaard, J. (Ed.). (2023). The Concept of Proportionality in International Humanitarian Law. In *Proportionality in International Humanitarian Law: Refocusing the Balance in Practice* (pp. 51–87). Cambridge University Press. https://doi.org/10.1017/9781108954648.007

Van Norman, G. A., & Eisenkot, R. (2017). Technology Transfer: From the Research Bench to Commercialization: Part 2: The Commercialization Process. *JACC: Basic to Translational Science*, *2*(2), 197–208. https://doi.org/10.1016/j.jacbts.2017.03.004

Vidigal, G. (2013). From Bilateral to Multilateral Law-making: Legislation, Practice, Evolution and the Future of Inter Se Agreements in the WTO. *European Journal of International Law*, *24*(4), 1027–1053. https://doi.org/10.1093/ejil/cht064

Villiger, M. E. (2008). *Commentary on the 1969 Vienna Convention on the Law of Treaties*. Brill. https://doi.org/10.1163/ej.9789004168046.i-1058

Webster, A. (2011). Hague Conventions (1899, 1907). In *The Encyclopedia of War*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781444338232.wbeow271

Whittle, D. (2015). The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action. *European Journal of International Law*, *26*(3), 671–698. https://doi.org/10.1093/ejil/chv042

Winter, E. (2022). The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law. *Journal of Conflict and Security Law*, *27*(1), 1–20. https://doi.org/10.1093/jcsl/krac001

Wired for War: The Robotics Revolution and Conflict in the 21st Century, P.W. Singer (New York: Penguin, 2009), 512 pp., $30 cloth. (2009). *Ethics & International Affairs*, *23*(3), 312–313. https://doi.org/10.1111/j.1747-7093.2009.00222_4.x

Сведения об авторах

Бхаскар Ниша – магистр права, научный сотрудник, Национальный юридический университет Западной Бенгалии
Адрес: Индия, Западная Бенгалия, Калькутта 700098, Солт Лейк, сектор III, блок 12 LB
E-mail: nishabhaskar414@gmail.com
ORCID ID: https://orcid.org/0009-0005-9128-1526

Магоге Джексон Симанго – магистр права в области корпоративного и коммерческого права, ассистент преподавателя, факультет гуманитарных и общественных наук, Национальный институт транспорта
Адрес: Танзания г. Дар-эс-Салам, P.O. Box 705, Убунго, Мабибо
E-mail: simangojackson@gmail.com
ORCID ID: https://orcid.org/0000-0001-8096-6929
Google Scholar ID: https://scholar.google.com/citations?user=8FERpVoAAAAJ

Хашими Саид Кудрат – PhD, магистр права в области международного права, научный сотрудник в области права, факультет правоведения, Майсурский университет
Адрес: Индия, 570005, г. Майсур, Манасаганготри
E-mail: sayedqudrathashim@law.uni-mysore.ac.in
ORCID ID: https://orcid.org/0000-0001-9835-0575

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: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 13 февраля 2025 г.
Дата одобрения после рецензирования – 2 марта 2025 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.

Research article
UDC 34:004:347.1:004.7
EDN: https://elibrary.ru/kxekjy
DOI: https://doi.org/10.21202/jdtl.2025.11

Third-Party Payment Regulation: Analysis of Risks and Legal Mechanisms in China

Li Jingrong
Lanzhou University of Finance and Economics, Lanzhou, China

Shawuya Jigeer
Peter the Great St. Petersburg Polytechnic University, Saint Petersburg, Russia

Keywords

digital economy,
digital technologies,
e-commerce,
law,
legislation,
payment platform,
regulation,
risk,
safety,
third-party payments

Abstract

Objective: to identify the main risks and problems in the field of third-party payments in China; to analyze the current legislation on the regulation of this sector; and to propose scientifically sound ways to improve the effectiveness of regulation of such payment systems.

Methods: the study used a set of general scientific methods, including analysis, induction and synthesis. The authors comprehensively analyzed the current state and legal regulation of third-party payments in China in order to develop practical recommendations for the introduction of effective regulatory mechanisms in this area. A comparative-legal analysis of existing regulations and international experience in regulating financial technologies was performed.

Results: it was found that third-party payments have become an integral part of e-commerce, effectively solving the problems of high transaction costs and shortage of credit resources in Chinese e-commerce. The analysis showed that the payment industry is facing serious challenges, including insufficient regulation, financial and technological risks. The authors revealed a market competitive structure according to the "2+1+N" model with the dominance of large payment platforms. Practical recommendations were developed to improve legal mechanisms ensuring the stability and security of the third-party payments sector, including the creation of a single regulator and increased supervision of deposited funds.

✉ Corresponding author

Scientific novelty: the study complements the scientific base in the field of financial technology regulation, systematizing the main risks of the third-party payments sector and analyzing the modern regulatory framework. It takes into account the latest changes in the industry, which allows the authors to form a comprehensive understanding of the legal challenges in this area. For the first time, an integrated risk assessment model for third-party payment systems was proposed.

Practical significance: the findings have practical implications for improving regulatory efficiency, which is relevant both for third-party payment service providers and for financial regulators when developing policies in the field of financial technology and digital payments. The results can be used to improve the legislative framework and create specialized financial supervisory authorities.

For citation

Jingrong, Li, & Jigeer, Sh. (2025). Third-Party Payment Regulation: Analysis of Risks and Legal Mechanisms in China. *Journal of Digital Technologies and Law, 3*(2), 259–274. https://doi.org/10.21202/jdtl.2025.11

Contents

Introduction

Third-party payment refers to a payment service provided by a non-banking institution for fund transfer, payment and settlement through the Internet or mobile devices (Liu et al., 2020; Thakor, 2020; Fan et al., 2023). With the development of financial technologies and the rise of e-commerce, third-party payment has expanded decisively and serves as an essential component of the financial system. In China, the competitive

pattern in the payments industry can be summarized as a "2+1+N" structure: Alipay and WeChat Pay account for nearly 60 % of transactions; UnionPay provides key clearing and settlement services; and a few third-party licensed payment companies are competing for market share in this field. The proportion of China's online payment users compared with all Internet users has remained steady at approximately 85 percent in 2022.

Payment by third parties have been advantageous for both the economy and society. A major aspect of e-commerce is currently involving third-party payment by effectively solving the problems of high cost and lack of credit in e-commerce (Tang et al., 2021; Zhao & Sun, 2012; Qiu, 2025). Third-party payment is becoming increasingly important in the payment system, and the potential risks brought by new technologies and business models have put forward higher requirements for regulation. This work investigates the potential risks associated with third-party payment by reviewing the relevant regulatory framework, and proposes possible solutions to improve the effectiveness of regulation.

1. Development status and regulatory framework of third-party payment

1.1. Current development status of third-party payment

There is no standardized definition of third-party payment. In the particular case of China, the exponential development of e-commerce is a prerequisite for the introduction of third-party payments. For e-commerce, electronic payment is an essential and vital instrument. The emergence of the third-party payment service is in line with the development of e-commerce, and is also one of the specific forms of online payment innovations. Alipay was introduced as a payment instrument for secured transactions to solve the trust issue that hindered the development of e-commerce marketplace of Alibaba (Ye et al., 2023; Du, 2025), and now it is one of the biggest payment platforms worldwide. The third-party payment service is based on large-scale online portals, and uses the credit of the banks with which it cooperates as its credit guarantee (Yao et al., 2018; Lee & Shin, 2018). In this context, third-party payment refers to a payment service provided by a non-banking institution for the purpose of transferring, paying and clearing funds via the Internet or mobile devices. Third-party payment includes online payment and offline payment. Online payment is usually used for e-commerce transactions, where users complete the payment through the third-party payment platform; offline payment is mostly observed in physical stores, where users complete the transaction through mobile devices. Figure 1 shows China's third-party payment market share in 2023[1].

[1] Market share of leading third-party online payment providers in China in 3rd quarter of 2023. Statista. https://clck.ru/3MEJeK

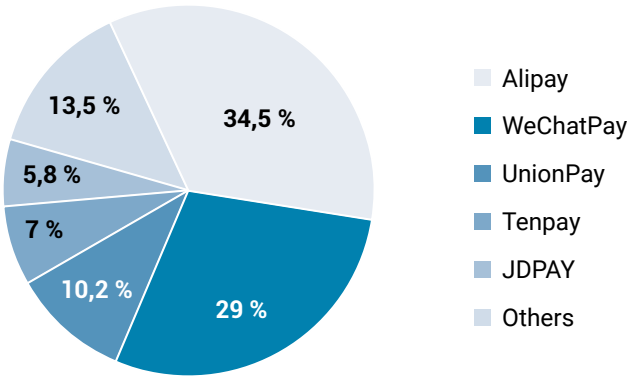


Figure. 1. China's third-party payment market share

The data presented in Figure 1 on third-party payment market share shows that Alipay, WeChat Pay, and UnionPay ranked the top three with market shares of 34.5, 29, and 10.2 %, respectively, and the sum of the market shares of these three reached 73.7 %, indicating a high degree of concentration in the market.

Figure 2 presents the data on the scale of third-party payment, which grew from 99.27 trillion yuan in 2016 to 337.87 trillion yuan in 2022, and it is predicted that the scale of China's third-party transactions will maintain its growth in the future, and is expected to reach 644 trillion yuan by 2028[2].

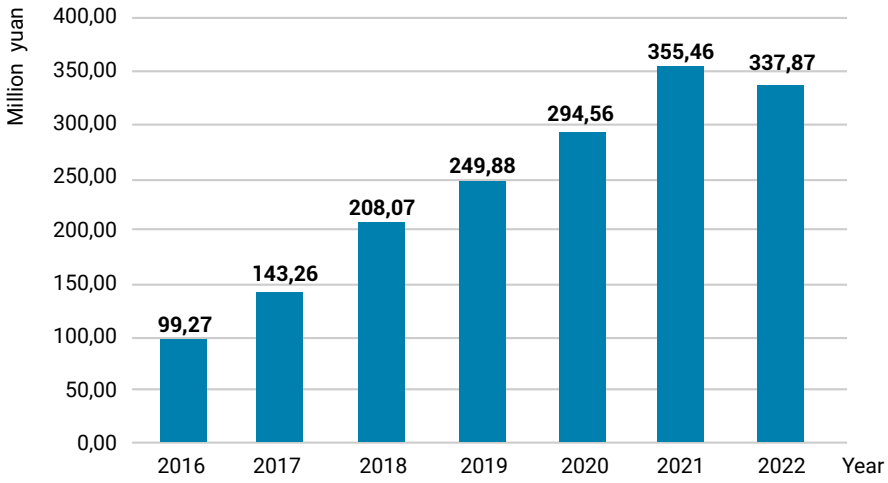


Figure. 2. Scale of China's third-party payment transactions

1.2. Regulatory framework of third-party payment

Third-party payments need to be addressed by the regulation framework due to their increasing significance in the payment system and the potential threats involved. China's third-party payment regulatory framework has a long process from absence to existence, from loose to strict regulation.

2 Ibid.

Prior to 2010, China had no clear regulatory organization and regulatory framework for third-party payment, and the third-party payment sphere was relatively unorganized, with high level of risks associated with payments. The People's Bank of China (PBOC) as the central bank of the country promulgated the "Administrative Measures for the Payment Services Provided by Non-financial Institutions" in 2010, which states that the PBOC supervises all aspects of the third-party payment institutions' operations, including the issuance of licenses, the continuous and stable operation of the institutions, risk management and control, risk disposal, and the withdrawal from the market. This clearly establishes that China adopts an institutional regulatory model for third-party payment institutions. Adoption of the regulation represents the commencement of legislation on third-party payment (Liu Zhaolu, 2018; Chen & Wang, 2024).

China has been emphasizing regulations on third-party payments as the sector thrives, and has successively introduced a series of legislations and regulations, including the strengthening of the entry of payment institutions, the supervision of fund security and the supervision of anti-money laundering. From 2010 to 2023, the People's Bank of China (PBOC), the China Banking Regulatory Commission (CBRC), the State Administration of Foreign Exchange (SAFE) and other financial regulators issued many relevant regulations and legislations to ensure that the third-party payment industry operates in a stable and prudent condition. Table summarizes China's main regulations and legislations related to third-party payments.

China's main regulations and legislations related to third-party payments

Regulations	Date	Main content
Administrative Measures for the Payment Services Provided by Non-financial Institutions	2010.06.14	The document clearly stipulates that third-party payment institutions should submit applications to the Central Bank for the issuance of a license for the provision of payment services. Third-party payment institutions are obliged to meet the qualifications for registration, which raises the entry threshold, and clarifies the issue of attribution of customer provisioning funds
Measures for the Supervision and Administration of Combating Money Laundering and Financing of Terrorism by Financial Institutions	2012.08.01	The document emphasizes that third-party payment institutions should set up a special anti-money laundering and anti-terrorist financing department to take charge of anti-money laundering measures. Third-party payment institutions are required to verify the authenticity of users' identities
Measures for the Custody of Clients' Reserves of Payment Institutions	2012.06.07	The document clarifies the depository and use of funds in transit, and strictly bans diversion by third-party payment institutions
Announcement of the China Banking Regulatory Commission on the Results of the Review of Regulatory Documents	2014.04.09	The document stipulates that third-party payment is applicable to the online payment business of non-bank payment institutions. At the same time, it makes clear regulations on account management, identity verification and information protection, transaction limits and risk control, supervision and management, and penalties
Notice of the State Administration of Foreign Exchange on the Pilot Cross-border Foreign Exchange Payment Business of Payment Institutions	2015.01.29	The document specifies that payment institutions engaged in cross-border payment activities are subject to the supervision and administration of the SAFE

End of Table

Regulations	Date	Main content
Administrative Measures for Online Payment Business of Non-bank Payment Institutions	2016.07.01	The document requires that payment institutions should follow the principle of mainly serving e-commerce development and providing small, fast, convenient and micro payment services. They should offer online payment services based on customers' bank accounts or prescribed payment accounts. Meanwhile, establish and improve the risk reserve fund and transaction compensation systems to safeguard customers' rights
Notice of the General Office of the People's Bank of China on Matters concerning Implementing the Centralized Deposit of the Funds of Pending Payments of Clients of Payment Institutions	2017.01.13	The document requires that the proportion of customer reserve funds be determined by the People's Bank of China based on the business types of payment institutions and adjusted as needed for management. Customer reserve funds are included in deposit accounts with no interest
Notice of the General Office of the People's Bank of China on Matters concerning Complete Centralized Deposit of the Funds of Pending Payments of Clients of Payment Institutions	2018.06.29	The document specifies that payment institutions increase the centralized deposit ratio of payment institutions' customer reserve funds, and requires 100% centralized deposit by January 14, 2019
Notice of the General Office of the People's Bank of China on Matters concerning Implementing the Centralized Deposit of the Funds of Pending Payments of Clients of Payment Institutions	2018.11.20	The document requires that payment institutions should cancel the remaining reserve funds accounts in commercial banks before January 14, 2019, and open "centralized provisioning depository accounts" in the branch of the People's Bank of China where the legal person is located
Regulation on the Supervision and Administration of Non-Banking Payment Institutions	2023.12.09	The document is the first administrative legislation in China's payment industry, which raises the level of non-bank payment supervision and aims to comprehensively strengthen the supervision of non-bank payment institutions

Since 2010, with the rapid development of e-commerce and mobile payment, the central bank has issued relevant regulatory legislations, issuing a large number of licenses to encourage the development of the non-bank payment industry and officially including non-bank payment institutions into the regulatory framework. The number of users of non-bank payment institutions continues to grow due to the convenience they offer, and as a result an increasing amount of customer information is being concentrated on these platforms, but there are significant vulnerabilities in the management of customer information by non-bank payment institutions compared to experienced and regulated traditional banks. As a result, regulators are gradually strengthening this aspect of supervision to protect customer information security. The central bank stopped issuing new licenses after 2015, and at the same time, introduced more strict rules to regulate the development of the industry, with a particular focus on the safety of customer funds and the security of personal information (Junwen et al., 2019).

After decades of development, China has established a payment and clearing system centered on the central bank's payment and clearing system, with the joint participation of commercial banks, clearing agencies and non-bank payment institutions, which is widely accessible and efficient. China has implemented an institutional regulatory model in the field of third-party payments, but with the development of Internet

finance, the boundaries between various financial and non-financial institutions are gradually becoming ambiguous, and the drawbacks of the institutional regulatory model are gradually becoming apparent. In 2023, State council issued "Regulation on the Supervision and Administration of Non-Banking Payment Institutions", which is the first administrative legislation in China's payment industry. The content of the regulation mainly includes four aspects: (a) to clarify the definition of non-bank payment institutions and the licensing of their operation; (b) to improve the regulations on payment services; (c) to protect the legitimate rights and interests of users; and (d) to clarify the supervisory responsibilities and legal liabilities. The document provides a clearer definition of the rights and obligations of all parties in the payment industry, and enables the supervisory authorities to exercise their administrative functions in accordance with the regulatory framework[3].

2. Risks Related to Third-Party Payments

2.1. Inadequate regulation

Third party payment sector is regulated by the People's Bank of China. However, due to its issuance of departmental regulations, the legal status of regulatory regulations is low. This limits the strength of its regulation. This leads to inadequate supervision and regulatory loopholes. In the regulatory system, there is the problem of common supervision by multiple departments, which leads to poor coordination among regulatory departments and unclear regulatory responsibilities. In addition, the lack of uniform standards and norms for supervision makes it difficult to effectively regulate the third-party payment industry (Ding, 2021).

Secondly, compared with the traditional financial industry laws and regulations system, third-party payment as a new industry, rapid development. Targeted special laws and regulations are still scarce and lagging behind. Although China has promulgated a «Management Measures» to make specific provisions on the access and supervision of third-party payment, it cannot meet the rapid development of Internet technology and the large-scale use of third-party payment, which has led to the emergence of a variety of risk issues. It is impossible to prevent legal problems arising in the third-party payment industry in a timely manner, and there are still a large number of gaps in supervision (Liu Jin, 2018). At the same time, there are also some gaps and shortcomings in the third-party payment regulatory rules in cross-border payment, risk prevention, user information protection, which makes it difficult to fully protect the rights and interests of users. Especially in cross-border payment, the regulatory regulations are weak and difficult to regulate, and it is easy to have capital outflow and security loopholes.

[3] Regulation on the Supervision and Administration of Non-Banking Payment Institutions. Order No. 768 of the State Council of the People's Republic of China. (2023, September 12). Chinalawinfo. https://clck.ru/3MEJjF

2.2. Financial risk

Sinking fund risk. Sinking funds refer to unused idle funds in society. As an intermediary between buyers and sellers, the third-party payment platform does not have the ownership of the funds during the whole transaction process, but with the continuous growth of the transaction scale, the amount of funds deposited on the third-party payment platform becomes very huge (Ding, 2021). As China's largest third-party payment platform, Alipay holds a large amount of funds that have not yet been timely transferred to the counterparty's account, and this large amount of funds is temporarily stagnated in the Alipay system. The flow of large amounts of funds may be exploited by some speculators to engage in malicious market manipulation and cause abnormal market volatility. At the same time, the flow of a large amount of money may create pressure on the market and affect market stability.

Cash-in disorder. Alipay relies on network electronic information technology, but due to the virtual nature of the network, some users may maliciously use fake transactions to cash out. This compromises users' personal information and causes losses to users' private property (Xiong, 2023).

2.3. Technology risk

With the rapid development of technology, hacker attacks, data leakage and other security issues are becoming increasingly serious. If the technical protection measures of online payment companies are not in place, they may suffer serious security incidents, resulting in consequences such as leakage of user information and theft of funds. In addition, technological upgrades may also pose a challenge to online payment companies, e.g., the application of new technologies may require companies to invest a large amount of money in upgrading and transformation, while technological failures may lead to difficulties for companies. Third-party payment platforms have the commonality of survival based on financial technologies, operational risks in the fintech sector also exist in these payment platforms based on the functioning of fintech (Xu et al., 2020; Yao & Li, 2022; Huang et al., 2024).

3. Recommendations on Enhancing the Effectiveness of Third-Party Payment Regulation

3.1. Establish a comprehensive legal framework

Continuously improve the laws and regulations on third-party payment, clarify the responsibilities and obligations of all parties, and provide legal guarantees for the safe and stable development of the payment market. Establish a unified third-party payment regulatory authority to specifically supervise the field, ensure the compliance of third-party payment institutions and punish violations. Update laws and regulations on third-party payment in a timely manner to ensure that there is a law to follow (Ding, 2021).

3.2. Supervision of funds

The regulatory authorities will be responsible for the supervision of third-party payment institutions regarding the clearing, custody, and risk management of their activities. A firewall will be established between the deposited funds and the operating funds, and different financial institutions will be selected for specialized supervision to prevent misappropriation of funds (Zhang, 2018; Zhu, 2024). In strengthening the management of reserve funds, it is necessary to clarify the legal ownership of the precipitated funds and the fruits thereof, and to strictly control and screen the investment fields and investment directions of the precipitated funds, curb money laundering, and strive to establish and improve the relevant legal supervision system.

The use of funds is strictly in accordance with the Bank's audit procedures to improve the management of deposited funds. Second, third-party payment institutions are required to keep users' funds in separate accounts from their own funds, and conduct regular inspections and reports to ensure the safety of funds and the smooth operation of clearing. At the same time, regulators will also review and guide third-party payment institutions on risk management and contingency plans to ensure that risks can be dealt with in a timely manner when they arise, so as to safeguard the stability and security of the market.

3.3. Technical assurance

The technical systems of third-party payment institutions are monitored and audited to ensure that their systems are stable, reliable, secure and efficient. At the same time, regulators may also use encryption technology to protect user information to ensure that it is not illegally accessed or misused (Xu et al., 2020; Yao & Li, 2022).

Third-party payment plays an important role in e-commerce, and the government should strengthen supervision and establish an appropriate regulatory system to protect consumers' rights and interests. Regulatory authorities should strengthen the formulation and adjustment of regulatory policies, improve the regulatory system and unify the market order. Third-party payment platforms must unswervingly strengthen internal risk control management, actively introduce new technologies. Make every effort to create a safe and reliable network environment, thereby effectively guaranteeing the safety of funds. Only under the premise of achieving security, stability and compliance can third-party payment achieve healthy, stable and comprehensive development and play an important role in the e-commerce ecosystem.

Conclusion

Third-party payments have had a markedly beneficial impact on economic and social development. Third-party payment has become an essential part of e-commerce, effectively solving the problems of high cost and lack of credit in e-commerce.

The rapid development of third-party payments poses significant regulatory challenges. The financial innovation of third-party payment is bound to bring a lot of payment risk problems. Therefore, it is necessary to seriously summarize, review and study the current status of the development and regulation of third-party payment in China, so as to provide practical evidence for the implementation of effective regulation. The regulation of third-party payment should be scientific, rigorous and effective. The construction of the regulatory framework requires multi-dimensional considerations, meeting regulatory requirements to ensure standardized operation and laying the foundation for the stable development of the industry; focusing on the future to leave space for innovation and promote the progress of the industry; attaching importance to risk control and establishing a sound prevention and control system; protecting the sustainability of innovation and encouraging reasonable innovation; at the same time, safeguarding the rights and interests of payers and consumers and protecting their legitimate rights and interests. On the premise of safety, stability and compliance, it is urgent to promote the standardized and orderly development of the third-party payment sector, which is crucial to precisely controlling risks and guaranteeing the stability of the payment sector.

References

Chen, W., & Wang, X. (2024). Can mobile payment innovation contribute to low-carbon sustainable economic development? Spatial econometric analysis based on Chinese city-level data. *Cities*, *155*, 105425. https://doi.org/10.1016/j.cities.2024.105425

Ding, Jie (2021). Legal Issues of Third-Party Payment in the Context of Internet Finance. *Dispute Settlement*, *7*(4), 169–178. https://doi.org/10.12677/DS.2021.74022

Du, S. (2025). More to give in marriage? County-level sex ratios and marriage payments in China. *Social Science Research*, *127*, 103141. https://doi.org/10.1016/j.ssresearch.2025.103141

Fan, X., Zhao, W., Zhang, T., & Yan, E. (2023). Mobile payment, third-party payment platform entry and information sharing in supply chains. *Annals of Operations Research*, *329*, 353–372. https://doi.org/10.1007/s10479-020-03749-8

Huang, Z., Wang, L., & Yu, W. (2024). Financial development, electronic payments, and residents' consumption: Evidence from rural China. *Finance Research Letters*, *71*, 106455. https://doi.org/10.1016/j.frl.2024.106455

Junwen, Zh., Jianwei, D., & Ming, G. (2019). Objectives and institutional arrangements of third-party payment supervision – International comparison and policy recommendations. *Financial Regulation Analysis*. 03.006. https://doi.org/DOI:10.13490/j.cnki.frr.2019.03.006

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, *61*(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003

Liu Zhaolu. (2018). *China's third-party electronic payment model*, 33. 029. Northeast Agricultural University.

Liu, J., Li, X., & Wang, S. (2020). What have we learnt from 10 years of fintech research? A scientometric analysis. *Technological Forecasting and Social Change, 155*, 120022. https://doi.org/10.1016/j.techfore.2020.120022

Liu, Jin. (2018). *The Regulatory Model of Non-Bank Payment Institutions in China and International Comparison. Research report*. Institute for Fintech research Tsinghua university.

Qiu, W. (2025). Does Mobile Payment Adoption Increase Household Portfolio Diversification? Evidence from China. *Finance Research Letters*, *75*, 106911. https://doi.org/10.1016/j.frl.2025.106911

Tang, Y. M., Chau, K. Y., Hong, L., Ip, Y. K., & Yan, W. (2021). Financial innovation in digital payment with WeChat towards electronic business success. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1844–1861. https://doi.org/10.3390/jtaer16050103

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation*, *41*, 100833. https://doi.org/10.1016/j.jfi.2019.100833

Xiong, Cen. (2023). China's third-party payment risk and control suggestions, *E-commerce*, *6*.

Xu, R., Mi, C., Mierzwiak, R., & Meng, R. (2020). Complex network construction of Internet finance risk. *Physica A: Statistical Mechanics and its Applications*, *540*, 122930. https://doi.org/10.1016/j.physa.2019.122930

Yao, M., Di, H., Zheng, X., & Xu, X. (2018). Impact of payment technology innovations on the traditional financial industry: A focus on China. *Technological Forecasting and Social Change*, *135*, 199–207. https://doi.org/10.1016/j.techfore.2017.12.023

Yao, Y., & Li, J. (2022). Operational risk assessment of third-party payment platforms: a case study of China. *Financial Innovation*, *8*, 19. https://doi.org/10.1186/s40854-022-00332-x

Ye, W., Chen, W., & Fortunati, L. (2023). Mobile payment in China: A study from a sociological perspective. *Journal of Communication Inquiry*, *47*(3), 222–248. https://doi.org/10.1177/01968599211052965

Zhang, Z. (2018). Law and economic growth in China: a case study of the stock market. *Asian Journal of Law and Society*, *5*(2), 333–357. https://doi.org/10.1017/als.2018.17

Zhao, X., & Sun, Y. (2012). A study of third-party online payment: Risk control and supervision analysis. *WHICEB 2012 PROCEEDINGS*. 95.

Zhu, Jing. (2024). Research on Legal Supervision Issues of Third-Party Payment. *E-commerce Letters*, *13*(1), 44–49. https://doi.org/10.12677/ecl.2024.131006

Authors information

Li Jingrong – Bachelor student, Faculty of International Education, Lanzhou University of Finance and Economics
Address: 4 Wei Le Avenue, 730101, Lanzhou, China
E-mail: Lee18334799908@gmail.com
ORCID ID: https://orcid.org/0009-0006-2916-8917

Shawuya Jigeer – PhD student, Assistant, Graduate School of Industrial Economics, Peter the Great St. Petersburg Polytechnic University
Address: Polytechnicheskaya St, 29, 195251, Saint Petersburg, Russia
E-mail: shauya.ts@edu.spbstu.ru
ORCID ID: https://orcid.org/0000-0003-3610-0460
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57236746000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HLG-6496-2023
Google Scholar ID: https://scholar.google.com/citations?user=ilwN9hAAAAAJ

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 13, 2024
Date of approval – November 4, 2024
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:347.1:004.7
EDN: https://elibrary.ru/kxekjy
DOI: https://doi.org/10.21202/jdtl.2025.11

Регулирование платежей третьей стороной: анализ рисков и правовых механизмов в Китае

Ли Цзинрун ✉

Университет финансов и экономики в Ланьчжоу, Ланьчжоу, Китай

Шауйя Джигир

Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия

Ключевые слова

безопасность,
законодательство,
платежи третьей стороной,
платежная платформа,
право,
регулирование,
риск,
цифровая экономика,
цифровые технологии,
электронная коммерция

Аннотация

Цель: выявить основные риски и проблемы в сфере платежей третьей стороной в Китае, проанализировать действующее законодательство о регулировании данного сектора и предложить научно обоснованные направления повышения эффективности регулирования подобных платежных систем.

Методы: исследование проводилось с применением комплекса общенаучных методов, включающих анализ, индукцию и синтез. Осуществлен всесторонний анализ текущего состояния развития и нормативного правового регулирования платежей третьей стороной в Китае с целью выработки практических рекомендаций для внедрения эффективных механизмов регулирования данной сферы. Применялся сравнительно-правовой анализ существующих нормативных актов и международного опыта регулирования финансовых технологий.

Результаты: установлено, что платежи третьей стороной стали неотъемлемой составляющей электронной коммерции, эффективно решая проблемы высоких транзакционных издержек и дефицита кредитных ресурсов в китайской электронной коммерции. Проведенный анализ показал, что платежная индустрия сталкивается с серьезными вызовами, включая недостаточность регулирования, финансовые и технологические риски. Выявлена конкурентная структура рынка по модели «2 + 1 + N» с доминированием крупных платежных платформ. Разработаны практические рекомендации по совершенствованию правовых механизмов для обеспечения стабильности и безопасности функционирования сектора сторонних платежей, включая создание единого регулятора и усиление надзора за депонированными средствами.

✉ Корреспондирующий автор

Научная новизна: исследование дополняет научную базу в области регулирования финансовых технологий, систематизируя основные риски индустрии сторонних платежей и анализируя современную нормативную правовую базу с учетом последних изменений в отрасли, что позволяет сформировать комплексное понимание правовых вызовов в данной сфере. Впервые предложена интегрированная модель оценки рисков для платежных систем третьих сторон.

Практическая значимость: представленные в работе выводы имеют прикладное значение для повышения эффективности регулирования, что актуально как для поставщиков платежных услуг третьих сторон, так и для финансовых регуляторов при разработке политики в области финансовых технологий и цифровых платежей. Результаты могут быть использованы при совершенствовании законодательной базы и создании специализированных органов финансового надзора.

Для цитирования

Цзинрун, Л., Джигир, Ш. (2025). Регулирование платежей третьей стороной: анализ рисков и правовых механизмов в Китае. *Journal of Digital Technologies and Law*, *3*(2), 259–274. https://doi.org/10.21202/jdtl.2025.11

Список литературы

Chen, W., & Wang, X. (2024). Can mobile payment innovation contribute to low-carbon sustainable economic development? Spatial econometric analysis based on Chinese city-level data. *Cities*, *155*, 105425. https://doi.org/10.1016/j.cities.2024.105425

Ding, Jie (2021). Legal Issues of Third-Party Payment in the Context of Internet Finance. *Dispute Settlement*, *7*(4), 169–178. https://doi.org/10.12677/DS.2021.74022

Du, S. (2025). More to give in marriage? County-level sex ratios and marriage payments in China. *Social Science Research*, *127*, 103141. https://doi.org/10.1016/j.ssresearch.2025.103141

Fan, X., Zhao, W., Zhang, T., & Yan, E. (2023). Mobile payment, third-party payment platform entry and information sharing in supply chains. *Annals of Operations Research*, *329*, 353–372. https://doi.org/10.1007/s10479-020-03749-8

Huang, Z., Wang, L., & Yu, W. (2024). Financial development, electronic payments, and residents' consumption: Evidence from rural China. *Finance Research Letters*, *71*, 106455. https://doi.org/10.1016/j.frl.2024.106455

Junwen, Zh., Jianwei, D., & Ming, G. (2019). Objectives and institutional arrangements of third-party payment supervision – International comparison and policy recommendations. *Financial Regulation Analysis*. 03.006. https://doi.org/DOI:10.13490/j.cnki.frr.2019.03.006

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, *61*(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003

Liu, Zhaolu. (2018). *China's third-party electronic payment model*, 33. 029. Northeast Agricultural University.

Liu, J., Li, X., & Wang, S. (2020). What have we learnt from 10 years of fintech research? A scientometric analysis. *Technological Forecasting and Social Change, 155*, 120022. https://doi.org/10.1016/j.techfore.2020.120022

Liu, Jin. (2018). *The Regulatory Model of Non-Bank Payment Institutions in China and International Comparison. Research report*. Institute for Fintech research Tsinghua university.

Qiu, W. (2025). Does Mobile Payment Adoption Increase Household Portfolio Diversification? Evidence from China. *Finance Research Letters*, *75*, 106911. https://doi.org/10.1016/j.frl.2025.106911

Tang, Y. M., Chau, K. Y., Hong, L., Ip, Y. K., & Yan, W. (2021). Financial innovation in digital payment with WeChat towards electronic business success. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1844–1861. https://doi.org/10.3390/jtaer16050103

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation*, *41*, 100833. https://doi.org/10.1016/j.jfi.2019.100833

Xiong, Cen. (2023). China's third-party payment risk and control suggestions, *E-commerce*, *6*.

Xu, R., Mi, C., Mierzwiak, R., & Meng, R. (2020). Complex network construction of Internet finance risk. *Physica A: Statistical Mechanics and its Applications*, *540*, 122930. https://doi.org/10.1016/j.physa.2019.122930

Yao, M., Di, H., Zheng, X., & Xu, X. (2018). Impact of payment technology innovations on the traditional financial industry: A focus on China. *Technological Forecasting and Social Change*, *135*, 199–207. https://doi.org/10.1016/j.techfore.2017.12.023

Yao, Y., & Li, J. (2022). Operational risk assessment of third-party payment platforms: a case study of China. *Financial Innovation*, *8,* 19. https://doi.org/10.1186/s40854-022-00332-x

Ye, W., Chen, W., & Fortunati, L. (2023). Mobile payment in China: A study from a sociological perspective. *Journal of Communication Inquiry*, *47*(3), 222–248. https://doi.org/10.1177/01968599211052965

Zhang, Z. (2018). Law and economic growth in China: a case study of the stock market. *Asian Journal of Law and Society*, *5*(2), 333–357. https://doi.org/10.1017/als.2018.17

Zhao, X., & Sun, Y. (2012). A study of third-party online payment: Risk control and supervision analysis. *WHICEB 2012 PROCEEDINGS*. 95.

Zhu, Jing. (2024). Research on Legal Supervision Issues of Third-Party Payment. *E-commerce Letters*, *13*(1), 44–49. https://doi.org/10.12677/ecl.2024.131006

Сведения об авторах

Цзинрун Ли – бакалавр, факультет международного образования, Университет финансов и экономики в Ланьчжоу
Адрес: Китай, 730101, г. Ланьчжоу, авеню Вей Ле, д. 4
E-mail: Lee18334799908@gmail.com
ORCID ID: https://orcid.org/0009-0006-2916-8917

Джигир Шауйя – аспирант, ассистент преподавателя, Высшая инженерно-экономическая школа, Санкт-Петербургский политехнический университет Петра Великого
Адрес: Россия, 195251, г. Санкт-Петербург, ул. Политехническая, д. 29
E-mail: shauya.ts@edu.spbstu.ru
ORCID ID: https://orcid.org/0000-0003-3610-0460
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57236746000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HLG-6496-2023
Google Scholar ID: https://scholar.google.com/citations?user=ilwN9hAAAAAJ

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 – 13 октября 2024 г.
Дата одобрения после рецензирования – 4 ноября 2024 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.

Research article
UDC 34:004:346.6:004.7
EDN: https://elibrary.ru/lqycmn
DOI: https://doi.org/10.21202/jdtl.2025.12

Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia

I Komang Oki Mayuna ✉
Brawijaya University, Malang, Indonesia

Reka Dewantara
Brawijaya University, Malang, Indonesia

Patricia Audrey Ruslijanto
Brawijaya University, Malang, Indonesia

Keywords

blockchain technology,
crypto assets,
cryptocurrency,
digital technologies,
law,
legislation,
personal data protection,
personal data,
pseudonymization,
trading in crypto assets

Abstract

Objective: to analyze the possibility of providing legal protection for pseudonymized personal data of crypto assets users in the legal system of Indonesia.

Methods: the work uses a comprehensive legal analysis based on the study of the current regulatory legal acts of Indonesia in the field of personal data protection. The research was carried out using legislative, conceptual and comparative methodological approaches, including an analysis of the Indonesian Law on Personal Data Protection, the EU General Regulation on Personal Data Protection, and the British Data Protection Act.

Results: it was established that pseudonymization of crypto assets user data in Indonesia is feasible from a legal point of view; however, the existing legislation contains significant gaps. The current Indonesian Personal Data Protection Law does not recognize pseudonymized data as a separate category of personal data subject to legal protection. The authors point out the problems with the implementation of the rule for controlling transfers of crypto assets by physical traders. As additional information for the re-identification of pseudonymized data is not stored separately, it increases the risks of privacy violations.

✉ Corresponding author

Scientific novelty: the authors provide a comprehensive analysis of the legal mechanisms for protecting pseudonymized data in the context of cryptocurrency transactions. A conceptual model is proposed for improving national legislation on personal data protection. It implies including pseudonymized data as a separate category of protected information. Recommendations are given, which establish criteria for the legitimate re-identification of pseudonymized data to ensure legal certainty in the field of protecting crypto assets users.

Practical significance: the research results can serve as a theoretical and methodological basis for reforming the Indonesian Law on Personal Data Protection and creating an effective legal mechanism for protecting crypto assets users. The proposed amendments to Article 4 of the said Law will make it possible to include pseudonymized data in the list of protected categories of personal data, which will provide legal certainty for participants in the cryptocurrency market and increase the level of their personal data protection in the digital economy.

For citation

Mayuna, I K. O., Dewantara, R., & Ruslijanto, P. A. (2025). Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia. *Journal of Digital Technologies and Law, 3*(2), 275–303. https://doi.org/10.21202/jdtl.2025.12

Contents

Introduction

The payment system has evolved; initially, it relied on physical money but now shifts to e-money. The world was recently shocked by the emergence of cryptocurrency, which is used as a payment method in trade transactions (Jati & Zulfikar, 2021). However, not all countries, including Indonesia, recognize cryptocurrency as a legal means of payment. Cryptocurrency in Indonesia cannot be used as a legal means of payment because, based on Article 2 of Law Number 7 of 2011 concerning Currency, it is stated that the official currency of Indonesia is the rupiah (Setiawan et al., 2023). However, cryptocurrency in Indonesia has been recognized as an investment instrument, as explained in Article 1 of the Minister of Trade Regulation Number 99 of 2018 concerning the General Policy for Implementing Crypto Asset Futures Trading (Crypto Asset). Therefore, in Indonesia, cryptocurrency is called a "crypto asset" (Ulya & Pambudi, 2024).

Crypto asset transactions are closely related to pseudonymisation data processing. When crypto asset investors transfer crypto assets to a digital wallet, either in the form of assets or conversion to fiat money (IDR), the transaction is recorded in the blockchain system using a pseudonymisation wallet address or public address. On the other hand, these transactions are also recorded or stored by physical traders of crypto assets as part of the implementation of the travel rule principle, as regulated in Article 38, paragraph (1) of BAPPEBTI Regulation Number 13 of 2022 concerning Amendments to BAPPEBTI Regulation Number 8 of 2021.

As a result, pseudonymisation data processing is carried out by physical crypto asset traders. However, additional information that could be used for re-identification is not stored separately from the pseudonymisation data, increasing the risk of data leakage. A pseudonym can still be linked to the data subject's identity. Moreover, research has shown that data stored within blockchains can be traced back to natural persons (obfuscated personal data subjects) if processed using adequate technical methods, potentially revealing the identity of the subject who owns the pseudonymisation data.

Unfortunately, the Personal Data Protection Law does not recognize pseudonymisation data as a type that qualifies for protection. Therefore, it is necessary to regulate pseudonymisation data as one of the categories protected under the Personal Data Protection Law to ensure legal safeguards for crypto asset investors.

1. Concept of personal data protection

1.1. Personal data protection

Personal data protection cannot be separated from the definition of data. In Latin, data is called datum, a part of information. The collection of data leads to the formation of information. In the context of personal data, different countries use different terms; some refer to it as "personal information", while others use it as "personal data". However, substantively, both terms have nearly the same meaning. Aside from these terminological

differences, there are also variations in the interpretation of the concept of personal data itself[1]. Indonesia uses the term "personal data", based on Article 1, Number 1 of the PDP Law[2]: "Personal data refers to information about an individual who is identified or can be identified, either individually or in combination with other information, directly or indirectly, through electronic or non-electronic systems".

The provisions in the PDP Law define personal data as information that can be identified or is identifiable through electronic or non-electronic means. In contrast, the GDPR does not specify this distinction.

Personal data protection encompasses at least two key concepts: securing physical personal data and establishing regulations that provide privacy guarantees for using a data subject's data. Fundamentally, data protection is closely related to safeguarding the right to privacy (Yetno, 2021). This is also emphasized by Alan Westin, who stated that data privacy is the right of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them will be communicated or collected by others[3].

Conceptually, establishing an absolute or standard definition of privacy is challenging, as the term remains a subject of ongoing debate among experts. Privacy refers to an individual's right to control personal information collection, use, disclosure, and retention (Jose, 2023). The concept of privacy was first introduced by Samuel Warren and Louis Brandeis, who stated that a fundamental human right must be protected, known as "The Right to Privacy", which means the following (Anand et al., 2020): "Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition".

Based on this explanation, the right to privacy encompasses the right to enjoy life, to be left alone, and to seek legal protection for one's privacy. According to the Big Indonesian Dictionary, privacy is defined as freedom or personal freedom. Warren and Brandeis further emphasize that privacy is the right to enjoy life and be left alone, ensuring everyone has the right to maintain their privacy (Dewi, 2017). Therefore, the right to privacy is the fundamental human right of every individual to maintain confidentiality and security (Anggen Suari & Sarjana, 2023). Everyone's privacy must be protected because an individual's privacy is compromised when personal information is made public. Therefore, privacy protection

1 Djafar, W., Sumigar, B. R. F., & Setianti, B. L. (2016). Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia. Lembaga Studi dan Advokasi Masyarakat.

2 Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 1 angka 1. (2022). Lembaran Negara Republik Indonesia, 196, Tambahan Lembaran Negara Republik Indonesia, 6820.

3 https://clck.ru/3MEF5G

is essential. However, many experts find it challenging to define and limit the concept of privacy due to its broad scope. As a result, many countries combine the idea of privacy with protecting personal data. This aligns with modern privacy theory, which Alan Westin first developed in his book Privacy and Freedom, where he states that (Pelteret & Ophoff, 2016): "Privacy is the claim of individuals, group or istitution to determine for themselves when, how, and to what extent information about them is communicated to others".

Based on this statement, privacy is the right of individuals, groups, or institutions to determine whether or not data about them will be communicated to other parties. Legal experts further developed this definition in response to information and communication technology advances, where an individual's privacy data can be accessed, processed, collected, and manipulated. As a result, one type of privacy right became known as personal data privacy.

The 1945 Constitution of the Republic of Indonesia (UUD NRI 1945) regulates the protection of human rights. After the amendment to the 1945 Constitution, the regulation of citizens' human rights became more comprehensive compared to the pre-amendment Constitution, which only addressed them in general and brief terms. The amendments to the 1945 NRI Constitution now include guarantees for protecting and fulfilling citizens' rights, one of which is the right to privacy (Asrun, 2016). The protection of the right to privacy is not explicitly regulated in the 1945 NRI Constitution. Still, the right to privacy is implicitly protected under Article 28G, paragraph (1) of the 1945 NRI Constitution, which states that[4]: "Every person has the right to protect themselves, their family, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat or fear of doing or not doing something, which is a human right".

Based on the explanation above, the right to privacy is implicitly regulated in this article. The explanation of this article aligns with the concepts of privacy discussed earlier, which include the right to honor, dignity, and property, as well as the right to a sense of security and protection from threats. In addition, privacy guarantees are also regulated in Article 29, paragraph (1), and Article 30 of Law Number 39 of 1999 concerning Human Rights. However, Indonesian laws and regulations do not define the right to privacy (Rohmansyah et al., 2023).

The right to privacy is related to personal data, where personal data is one of the elements protected by law. Thus, everyone has the right to maintain their personal data's privacy (confidentiality and security) (Priskarini et al., 2019). The European Human Rights Court also stated that the protection of personal data is fundamental and that respect for a person's right to privacy is as regulated in Article 8 of the European Convention on Human Rights (European Convention on Human Rights and Fundamental Freedoms) (Sinaga & Putri, 2020). This is also in line with the provisions of Article 28G, paragraph (1)

[4] Undang – Undang Dasar Negara Republik Indonesia Tahun. (1945). Pasal 28G ayat (1).

of the 1945 Constitution of the Republic of Indonesia, which protects personal data as part of the right to privacy. Although Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia does not explicitly mention the right to privacy, this provision implies a guarantee of the right to privacy (Soraja, 2021).

Apart from that, the explanation of Article 26 of the ITE Law Number 19 of 2016 clarifies that protecting personal data is one aspect of personal rights (privacy rights) (Priliasari, 2023). So, personal data protection is part of each individual's right to privacy. The PDP Law defines personal data protection, as explained in Article 1, number 2 of the PDP Law, which states that:[5] "Personal Data Protection is the overall effort to protect Personal Data during Personal Data processing to guarantee the constitutional rights of Personal Data subjects".

Based on this explanation, the right to protect personal data is a constitutional right of Indonesian citizens that the state must safeguard. Therefore, personal data protection is part of the right to privacy, implicitly protected under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Consequently, personal data protection is a constitutional right of citizens that the state must uphold to ensure they receive their rights. Thus, personal data is an inseparable part of the right to privacy, as protecting personal data is an integral aspect of the right to privacy guaranteed by the 1945 Constitution of the Republic of Indonesia.

1.2. Meaning of pseudonymisation data

The definition of a pseudonym in the Big Indonesian Dictionary refers to a name used to conceal one's true identity (pseudonym). Pseudonymisation of data involves replacing identifying characteristics with pseudonyms or, in other words, modifying the data so that the data subject cannot be directly identified. This pseudonymisation can only be associated with confidential identification data (additional data).

Pseudonymisation emphasizes techniques that replace, delete, or alter information that identifies an individual while keeping that information separate. Data that has undergone the pseudonymisation process remains classified as personal data and falls within the scope of data protection law.

Pseudonymisation begins with original data, which is then disguised, resulting in two data sets: pseudonymized data and additional information. Both datasets can be used to reconstruct the original data. This means that pseudonymized data can be linked back to the original data of the data subject using additional information. Thus, pseudonymisation data retains data protection principles.

[5] Undang – Undang Nomor 27, Pasal 1 angka 2. (2022), tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun, 196, Tambahan Lembaran Negara Republik Indonesia, 6820.

Article 4, paragraph (5) of the GDPR defines pseudonymisation as follows: "pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"[6].

As explained above, pseudonymized personal data falls within the scope of the GDPR. This definition clearly describes and emphasizes that data undergoing the pseudonymisation process begins and remains classified as personal data. Pseudonymisation data is still associated with a natural person who can be identified according to the definition of personal data itself. The pseudonymisation process only prevents the direct identification of the pseudonymisation data subject (Mourby et al., 2018).

Pseudonymisation, as described in Article 4, paragraph (5) of the GDPR, refers to processing personal data so that it can no longer be associated with a specific data subject without using additional information. Such additional information must be kept separately and subject to technical and organizational measures to ensure that personal data is not linked to an identifiable person. This provision clearly distinguishes between anonymized data and pseudonymisation data. In the case of anonymous data, data protection principles do not apply because the subject is not or can no longer be identified. In contrast, pseudonymisation data must adhere to data protection principles because the data belongs to an identifiable individual (Bolognini & Bistolfi, 2017). This is also explained in Recital 26 of the General Data Protection Regulation (GDPR), which states: "The principles of data protection should apply to any information concerning an identified or identifiable natural person; personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person..." (Finck & Pallas, 2020).

So, even though pseudonymisation data can be reconnected to the original data of the data owner, processors and personal data controllers must ensure that any additional information used for re-identification is stored separately. This ensures that other parties cannot access or use it without permission to re-identify the original data of the subject that has undergone the pseudonymisation process (Huang & Zheng, 2023). Therefore, re-identification can be prevented by ensuring that unauthorized parties do not gain access to additional data or information that could be used to identify the pseudonymized data (Kohlmayer et al., 2019).

[6] General Data Protection Regulation (EU GDPR). (2018, May 23). GDPR-Text.com. https://goo.su/Ke5Byw

Pseudonymisation is used as a new approach to controlling data distribution to maintain the data owner's privacy by applying pseudonyms, which hide the relationship between the information and the data owner. This pseudonymisation aims to control the flow of information to individuals to prevent the misuse of their information or privacy. Additionally, pseudonymisation also functions to limit unwanted data disclosure by unauthorized parties. One method of implementing pseudonymisation is encryption. Data that undergoes the encryption process is transformed into specific codes that generate a public key (Suryawijaya, 2023). Pseudonymisation can address privacy issues (personal data protection), confidentiality, and integrity. The scope of a pseudonym includes knowledge or information related to the holder and the pseudonym. Information about pseudonyms must only be known by the holder or an authorized party because it can refer to the data subject and reveal their identity if identified with additional data (Kumar Rai, 2016).

1.3. Meaning of anonymized data

Anonymization is replacing, modifying, or deleting individual data or information so that it cannot be re-identified. Therefore, pseudonymisation differs from anonymization in that information processed through pseudonymisation is not entirely deleted or disguised but is only replaced with a pseudonym, allowing it to be re-identified with the help of additional information stored separately. Meanwhile, anonymization not only removes names but typically disguises or completely deletes a person's information, making it impossible to identify the data subject (Hintze & El Emam, 2018).

Pseudonymisation and anonymization are two distinct terms, but they are often confused in the context of personal data protection. Data that undergoes an anonymization process will remove any information that could serve as an identifier for the data subject. In other words, anonymous data permanently disconnects the personal data from a specific identified or identifiable person. Meanwhile, pseudonymization does not remove all identifying information from the data but only reduces the association of the data set with a person's real identity (Štarchoň & Pikulík, 2019). The EU Article 29 Working Party also explains that "Pseudonymisation is not an anonymization method, as pseudonymisation only reduces the linkage of a data set with the original data of the data subject's identity"»[7]. Thus, data will be considered anonymous if the data that undergoes de-identification cannot be changed or re-identified to the subject who owns the data (Mourby et al., 2018).

[7] EU. (1995, October 24). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://clck.ru/3MEFan

Anonymization is intended to prevent the re-identification of data or individuals who have gone through the anonymization process. Thus, anonymous data does not fall under data protection principles. This is also explained in Recital 26 of the GDPR, which states that...: "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable…"[8].

Therefore, anonymous data does not fall under the principles of personal data protection because it cannot be linked back to a specific identified or identifiable person. On the other hand, pseudonymisation data still falls under the principles of personal data protection because it can be linked back to an identified or identifiable natural person. Thus, the GDPR obligates personal data controllers to separate additional information that can be used to re-identify pseudonymisation data. In addition, the controller is also obliged to consider all possible means or methods that specific individuals could use to re-identify pseudonymisation data.

1.4. Meaning of aggregated data

Aggregate data is data produced through an aggregation process (grouping data). Data aggregation is collecting and presenting raw data in summary form for statistical analysis. Aggregate data is generally known as statistical data and is usually displayed as tables, charts, graphs, or bar charts (Sinulingga, 2022). Therefore, aggregate data does not fall under personal data protection because aggregate data cannot re-identify a person's identity. This is also explained in Recital 26 of the GDPR, which states that: "…This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes"[9].

Thus, based on the explanation above, of the three types of data, namely pseudodonymisation data, anonymous data, and aggregate data, only pseudodonymisation data is subject to the principles of personal data protection. This is because pseudonymisation data can be identified as the original data of the owner, with additional information stored separately.

8 Resital 26 General Data Protection Regulation. (2022).

9 Ibid.

2. The relationship between pseudonymized data protection of crypto asset customers and crypto asset trading

Cryptocurrency is a currency not centralized by banks; it is created using computer encryption technology recorded on a blockchain platform. Users use cryptocurrency to store and make transactions, although not all countries legalize cryptocurrency as a means of payment in trade transactions. For example, as regulated in Article 2 of Law Number 7 of 2011, Indonesia stipulates that the legal means of payment is the rupiah (Setiawan et al., 2023). So, in this case, cryptocurrency is not a legal currency in Indonesia that can be used as a means of payment. This was also expressly stated by Bank Indonesia, which declared that cryptocurrency cannot be used as a means of payment in Indonesia. Furthermore, the prohibition on crypto assets as a means of payment in Indonesia is explicitly regulated in Bank Indonesia Regulation Number 20 of 2018 concerning Electronic Money (Chang, 2019).

On the other hand, cryptocurrency can be used as an investment instrument in Indonesia, as explained in Article 1 of the Minister of Trade Regulation Number 99 of 2018 concerning the General Policy for Implementing Crypto Asset Futures Trading (Crypto Asset). Thus, cryptocurrency is recognized as a "Crypto Asset" in Indonesia (Ulya & Pambudi, 2024). Crypto assets can be defined as private assets that rely on a blockchain system to secure digital value or contractual rights. These assets can be transferred, stored, or traded electronically. Abroad, crypto assets are usually known as cryptocurrency, and cryptocurrency can be used as virtual currency in buying and selling transactions (Pudjastuti & Westra, 2021). Meanwhile, crypto assets can only be used as investment instruments in Indonesia.

Crypto assets are digital currency systems that are secured using cryptographic techniques (Faozi & Segara Gustanto, 2022). Cryptography refers to encryption, which converts text into signs or symbols. Cryptocurrency uses a technology called blockchain (Ausop & Aulia, 2018). Therefore, cryptocurrency is a digital currency that stores digital data related to users' crypto asset transactions in the blockchain system. Thus, cryptocurrency cannot be separated from the blockchain because it is connected, with the blockchain functioning as a data storage system for crypto asset investors.

In computer systems, there are three types of networks, one of which is a distributed network. Distributed systems are not subject to any central authority, so each system node is part of a network and is directly connected to other system nodes (Suryawijaya, 2023).

Blockchain implements a distributed system, so all system nodes in the network have the same rights and obligations to store information and are connected (Handoko et al., 2024). Blockchain-based systems offer a higher level of transparency compared to existing records and ledgers. Because of this transparency, changes are visible to everyone on the network, and transactions cannot be changed or deleted once they are entered into the blockchain. Blockchain provides transparency to everyone in the network, allowing them to see the transactions in the blockchain system (Nanda Sari & Gelar, 2024).

Besides that, blockchain also implements a decentralized system, which aims to eliminate the involvement of intermediaries (third parties), thereby increasing transparency and trust in the system (Abdul Karim & Hadinata, 2023). Decentralized blockchain essentially allows everyone to connect to the network so that they have access to the blockchain system (Suryawijaya, 2023). What's more, data that has been entered into the blockchain cannot be changed or deleted. Data in blocks entered into the blockchain system can also be traced back to previous blocks. With this blockchain system, transactions carried out in the past cannot be changed, so they still leave clear traces. However, security in blockchain systems is not perfect. This is because the blockchain system is transparent and decentralized, meaning everyone can see transactions in the blockchain network (Jamwal et al., 2024). Therefore, many experts study blockchain because it is considered that security in blockchain technology is not yet entirely perfect for protecting blockchain users' data, as stated by researchers from the Open Data Institute (Utomo, 2022).

However, many users feel that this transparency is not a problem for privacy because of pseudonymization, where only users with the private key can use it to redescribe the public key. However, in the concept of personal data protection, the controller must be able to guarantee that the data stored is kept confidential and available and that only authorized parties can access the data. In reality, however, the data entered into the blockchain system contradicts the principles of confidentiality and availability because everyone can see the data entered into the blockchain system, as the blockchain is transparent (Tatar et al., 2020). Even though the data entered into the blockchain system is Pseudonymisation, research has shown that the data found in the blockchain can refer to individual people (disguised personal data subjects) if this is done by connecting data available on the blockchain network to data outside the network or by analyzing the context of transactions that occur on the blockchain using network analysis. Moreover, the user's real identity can also be revealed when using information outside the network. Furthermore, if additional data is not stored separately from the public key, it can reveal the user's real identity. For example, a study shows that it is still possible to re-identify crypto asset customers by tracking pseudonymous wallet addresses and transactional data in the blockchain system (Tatar et al., 2020).

Therefore, crypto assets are closely related to the processing of pseudonymisation data. In the crypto asset trading transaction mechanism, crypto asset transactions are closely related to the pseudonymisation data process. When crypto asset investors carry out transactions (exchange or transfer) of crypto assets, whether from crypto assets to fiat money (IDR) or vice versa, or from one crypto asset to another, the transaction will be entered into the blockchain system in the form of a pseudonymisation public address/wallet address. As a result, everyone in the blockchain system can see transactions made by crypto asset investors, even though they won't know the identity of the user who created the transaction, as the public address/wallet address entered into the blockchain system is Pseudonymisation. Furthermore, the transaction will also be recorded or saved by the crypto asset trader as a financial record, which will be reported to CoFTRA to prevent crypto asset transactions from being used as a mode for committing criminal acts such as money laundering.

Thus, the physical trading of crypto assets cannot be separated from processing personal data in pseudonymisation data, especially regarding pseudonymisation data protection. This is because crypto asset trading transactions involve pseudonymous wallet addresses recorded in the blockchain system. Moreover, physical crypto asset traders are required to apply the Know Your Customer (KYC) principle, which involves collecting customer personal data as part of anti-money laundering programs and efforts to prevent the financing of terrorism and the proliferation of weapons of mass destruction. Therefore, personal data collection activities by crypto asset traders can result in "additional information" that may be used to re-identify the pseudonymisation data of crypto asset customers (Atikah, 2023).

In addition, pseudonymous wallet addresses are collected by physical crypto asset traders as a form of applying the travel rule principle. The travel rule is a regulation that requires virtual asset service providers (crypto asset traders) to collect, store, and transmit certain information about the sending and receiving assets in every transaction carried out, including transactions that cross jurisdictional boundaries (Maulana, 2024). This is in line with on-chain crypto asset trading transactions, where the user's public address/wallet address is recorded in the blockchain system and on the platform used by crypto asset customers to carry out crypto asset trading transactions. This raises the risk that the crypto asset customer's public address/wallet address may be re-identified with additional information obtained and collected by the crypto asset trader as part of implementing the know your customer (KYC) principle (Alfin et al., 2024).

Thus, personal data is processed in pseudonymous form and carried out by physical crypto asset traders. However, the implementation of the travel rule principle does not consider the principle of protecting personal data in pseudonymisation form, where "additional information" that can be used for re-identification should be stored separately. Therefore, crypto asset trading is closely related to protecting the pseudonymisation data of crypto asset investors. Hence, regulations must guarantee the protection of crypto asset investors' pseudonymisation data processing in the crypto asset transaction process.

3. Data pseudonymization and reidentification regulations

3.1. Indonesian Personal Data Protection Law

The protection of personal data is a constitutional right of Indonesian citizens. This is also confirmed in Article 1, number 2 of the PDP Law, which states that personal data protection is the overall effort to protect personal data in processing personal data to guarantee the constitutional rights of personal data subjects. The personal data in question refers to data about natural persons who are identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems. Based on the explanation of Article 1, point 1 of the PDP Law, this article indirectly accommodates the meaning of pseudonymisation

data. Pseudonymisation data refers to the alteration or replacement of identifying data characteristics with a pseudonym so that it does not allow the data subject to be identified directly without the help of additional information stored separately.

Unfortunately, the PDP Law does not regulate pseudonymisation data as one of the types of data that receives protection. This can be seen from the provisions of Article 4, paragraph (1) of the PDP Law, which divides personal data into two types: specific and general personal data. Specific personal data includes health data and information, biometric data, genetic data, criminal records, children's data, personal financial data, and other data by statutory provisions. Meanwhile, general personal data includes full name, gender, nationality, religion, marital status, and/or personal data combined to identify a person (Adhiwisaksana & Allagan, 2023). However, both types of personal data, specific and general personal data, do not include pseudonymisation data as part of the personal data that receive protection.

Even though Article 4, paragraph (3), letter f of the PDP Law includes "personal data combined to identify a person", the Elucidation to Article 4, paragraph (3), letter f of the PDP Law only includes cell phone numbers and IP addresses. Implicitly, "personal data combined to identify a person" means that the data functions to identify or link the individual owner of the personal data. Therefore, it fundamentally differs from pseudonymisation data, which is not intended to identify or link natural persons. Instead, pseudonymisation data is meant to disguise the data subject's identity, making re-identification impossible without using additional information that is stored separately.

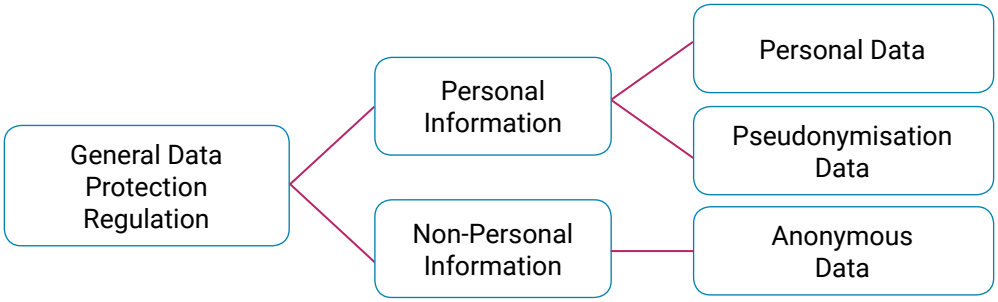
Moreover, the PDP Law also does not regulate the re-identification criteria considered valid for pseudonymisation data. Additionally, the PDP Law does not regulate the requirements for processing pseudonymisation data that has been re-identified and is considered valid. The PDP Law does not address pseudonymisation data as data subject to data protection principles. Thus, the PDP Law does not regulate the re-identification and processing of re-identified personal data, which could result in personal data violations.

3.2. General Data Protection Regulation

The European Union issued the General Data Protection Regulation (GDPR), which includes regulations related to de-identification, one of which is pseudonymisation. The GDPR introduced the concept of pseudonymisation and contributed to popularizing the idea of pseudonymisation data, which falls between personal data and anonymous data. The GDPR emphasizes that the storage and protection of additional information must be carried out separately in the definition of pseudonymisation information. This is explained in Article 4, paragraph (5) of the GDPR (Joo & Kwon, 2023).

Article 4, paragraph (1) GDPR defines personal data, as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier

such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Imakura et al., 2023). The personal data subject to data protection principles according to GDPR are as follows (Joo & Kwon, 2023):



The personal data subject to data protection principles

Sourse: (Joo & Kwon, 2023).

The GDPR protects pseudonymisation data, which is not considered anonymous because it can be identified or re-identified using additional information that must be stored separately (Limniotis, 2021). The GDPR provides data protection principles for pseudonymisation data, as explained in Recital 26 of the GDPR, which states: "The principles of data protection should apply to any information concerning an identified or identifiable natural person; personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person"[10]. The European Union includes pseudonymisation data within the scope of "personal data", so pseudonymisation data is protected by law (Wahyuningtyas, 2024).

However, the GDPR does not provide data protection principles for anonymous data, as explained in Recital 26 of the GDPR, which states: "...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable..."[11]. This is because, in essence, anonymous data is intended to prevent re-identification, so data that has gone through the anonymization process cannot be linked or re-identified to a particular individual (Dat & An, 2024).

Therefore, Article 29 of GDPR obligates data controllers to separate additional information that can be used to link personal data that has undergone a pseudonymisation process. Additionally, the controller must also consider all means or methods that may be used by certain parties to re-identify pseudonymisation data. This is a form

[10] Resital 26 General Data Protection Regulation. (2022).

[11] Ibid.

of legal protection against pseudonymisation data processing (Finck & Pallas, 2020). Unfortunately, the GDPR does not provide further regulations regarding the criteria for re-identification of pseudonymisation data that is considered valid. On the other hand, the GDPR obligates member countries to establish legal rules that apply to violations of the provisions of the GDPR, as regulated in Article 84 paragraph (1) of the GDPR.

3.3. Data Protection Act 2018

The General Data Protection Regulation (GDPR) affects European Union countries, requiring them to adopt the GDPR into their respective national personal data protection laws. Therefore, the GDPR obligates member countries to establish legal rules that apply to violations of its provisions, as regulated in Article 84 paragraph (1) of the GDPR. In addition, member countries must also encourage the preparation of codes of ethics that can support the implementation of the GDPR, one of which is related to pseudonymisation data, as regulated in Article 40 paragraph (2) letter d of the GDPR. Consequently, the UK established data protection regulations, namely the Data Protection Act 2018, which regulates the re-identification of pseudonymisation data. Article 171, paragraph (2) of the UK DPA 2018 defines de-identification and re-identification as follows[12]:

"(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a)".

Any person who re-identifies information that constitutes personal data, which has been de-identified (pseudonymized) without the consent of the controller or responsible controller or supervisor, constitutes a personal data violation, as regulated in Article 171 paragraph (1) of the DPA 2018. Therefore, provisions in paragraphs (1) and (2) of Article 171 of the DPA 2018 refer to or represent pseudonymization as outlined in Article 4, paragraph (5) of the GDPR. Thus, anyone who re-identifies pseudonymisation data is considered to have committed a personal data violation.

However, the 2018 DPA provides criteria for re-identification that are considered valid, one of which is for the public interest, including the purpose of preventing or detecting crime, when required or permitted by law or court order, and in the public interest, as regulated in Article 171 paragraph (3) of the 2018 DPA. In addition, identification is considered valid if it is based on reasonable confidence and for special purposes such as academic research, as regulated in Article 171 paragraph (4). Furthermore, the 2018 DPA also regulates personal data violations concerning the processing of re-identified personal data if it turns out that the data processing was carried out without permission from the responsible party and the re-identification violates the provisions of Article 171 paragraph (1) of the 2018 DPA.

[12] Data Protection Act. (2018), Article 171 Paragraph (2).

The 2018 DPA also provides criteria for processing re-identified personal data that is considered lawful, namely for the public interest, which includes the purpose of preventing or detecting crime, required or permitted by law or court order, and in the public interest, as regulated in Article 171 paragraph (6) of the 2018 DPA. In addition, processing re-identified personal data is considered lawful if it is based on reasonable belief and for specific purposes, such as academic research, as regulated in Article 171 paragraph (7). However, Article 171 paragraph (7) does not include “effectiveness testing” as one of the criteria, whereas in Article 171 paragraph (4), “effectiveness testing” is included in the criteria for re-identification that is considered valid.

4. Crypto asset customers' pseudonymisation data protection challenges in Indonesia

The right to privacy is every person’s right to live without interference in their private life, whether by other people or the state. Thus, the state is responsible and obligated to regulate and recognize these rights. Privacy, as a right inherent to humans, can be divided into several types, one of which is information privacy. Information considered private can come in various forms depending on its intended use. Simson Garfinkel divides it into five types: personal information, private information, personal identity information, pseudonymous or anonymous information, and aggregate information (Syailendra et al., 2024).

The right to privacy is implicitly regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Protecting personal data is closely related to the right to privacy, as it constitutes one type of privacy right. Therefore, personal data protection is part of human rights, as regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia (Priskarini et al., 2019). Therefore, Indonesia established the Personal Data Protection Law as a form of protection for human rights, specifically the right to privacy.

Unfortunately, the PDP Law cannot fully provide legal protection regarding pseudonymisation data processing, particularly for crypto asset customers. This is because the PDP Law does not regulate pseudonymisation data as one of the types of data that receives protection. Thus, the PDP Law, particularly Article 4, which governs types of personal data, does not yet accommodate the regulation of “pseudonymisation data” as a protected data type. Even though Article 4 paragraph (3) letter f states “personal data combined to identify a person”, the Elucidation to Article 4 paragraph (3) letter f only includes cell phone numbers and IP addresses. Furthermore, pseudonymisation data is not intended to identify a person but to disguise the subject’s identity, making direct identification impossible without using additional information stored separately.

Thus, the PDP Law cannot fully guarantee personal data protection for crypto asset customers by processing personal data as pseudonymisation data. Crypto

asset transactions are closely related to the processing of personal data in the form of pseudonymisation data because transactions (exchange or transfer) of crypto assets, whether from crypto assets to fiat money (IDR) or vice versa, and from one crypto asset to another, will be recorded in the blockchain system as a pseudonymisation public address or wallet address.

Furthermore, the transaction will also be recorded or stored by the crypto asset trader in the form of sender and user names, sender and recipient wallet addresses, and sender and user addresses as a form of application of the travel rule principle. This aligns with on-chain crypto asset trading transactions, where the user's public address/ wallet address is recorded in the blockchain system and, of course, on the platform crypto asset customers use for trading transactions.

Therefore, this processing poses a risk because the crypto asset customer's public address/wallet address could be re-identified using additional information obtained and collected by the crypto asset trader as part of implementing the know your customer (KYC) principle (Alfin et al., 2024). Thus, there are personal data collection activities in the form of pseudonymisation data, which are carried out together with "additional information" that can be used to re-identify the pseudonymisation data of crypto asset customers (Atikah, 2023).

Personal data protection in electronic systems must be carried out by respecting the privacy rights of personal data owners, as personal data is private. Thus, electronic system organizers, in this case, physical traders of crypto assets, must protect the electronic information collected as a form of application of the travel rule or know-your-customer principles (Utomo, 2020). Unfortunately, the PDP Law cannot guarantee protection for processing personal data in the form of pseudonymisation data because, in essence, the PDP Law does not regulate pseudonymisation data as one type of data with protection principles. Thus, this presents a challenge for protecting pseudonymisation data for crypto asset customers because the PDP Law does not yet accommodate legal protection arrangements for processing personal data in pseudonymisation data.

Therefore, it is necessary to reformulate the PDP Law regarding regulating the types of data that receive protection to ensure legal protection for crypto asset customers. This aligns with the theory of legal protection put forward by Philipus M. Hadjon, namely the theory of preventive legal protection, which involves establishing regulations that can protect every citizen (Tirtakoesoemah & Arafat, 2019). Therefore, it is necessary to establish regulations that govern pseudonymisation data as one type that receives protection in the PDP Law as a guarantee of legal protection provided by the government to crypto asset customers against processing personal data in the form of pseudonymisation data.

This arrangement can provide legal certainty regarding legal protection for crypto asset customers by processing personal data as pseudonymisation data by physical

traders of crypto assets. In reality, crypto asset customers currently do not obtain legal protection against processing personal data through pseudonymisation data by applying the travel rule principle. Additionally, storing "additional information", which can be used to identify pseudonymisation data, is not carried out separately, making it vulnerable to exploitation by parties not authorized to re-identify pseudonymisation data illegally (Ayunda, 2022).

Moreover, the number of crypto asset customers reported by the Republic of Indonesia Ministry of Trade website reached 21.27 million people from February 2021 to September 2024. Although Pseudonymisation data leaks are currently not known to have occurred in Indonesia, crypto-news websites have suspected or claimed that the personal information of 13 million Binance users, including names, emails, telephone numbers, and residential addresses, has been leaked. However, personal data leaks in the form of names, emails, and telephone numbers can be a significant trigger for pseudonymisation data leaks. This data can be used as "additional information" to re-identify the individuals who own the pseudonymisation data.

In addition, re-identifying pseudonymisation data can also result in hacking crypto asset customers' private addresses (private key compromise). A private key compromise refers to unauthorized access by a particular person to a crypto asset customer's private key. After investigation, it was discovered that 19 cases of private key compromise had occurred, resulting in financial losses of $641.54 million in 2022 and $231.00 million in 2023 (Multazam et al., 2024). Therefore, Indonesia needs to build a robust and coordinated information technology legal system to achieve legal certainty regarding protecting crypto asset customers by processing personal data in pseudonymisation form.

This aligns with the legal convergence theory put forward by Danrivanto Budhijanto, who adapted the 4C Convergence theory. The legal convergence theory focuses on the unification of technological, economic, and legal variables in human relations in the digital era. It highlights the need for the formation of laws, both at the national and international levels, to accommodate these technological developments (Rizko Ramadoni et al., 2021). Research has shown that data found in blockchains can refer to natural persons (obfuscated personal data subjects) if handled in an adequate technical manner. This can be done by connecting data available on the blockchain network to data outside the network and analyzing the context of transactions that occur on the blockchain through network analysis. Furthermore, the user's real identity can be revealed when using information outside the network (Jamwal et al., 2024).

Thus, it is necessary to regulate pseudonymisation data in the PDP Law to guarantee legal certainty regarding the legal protection of crypto asset customers' pseudonymisation data processing. Since the PDP Law does not regulate it, it poses a challenge or obstacle for crypto asset customers to obtain legal protection concerning pseudonymisation data processing.

Conclusions

Protection of personal data is part of the right to privacy, which is implicitly regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia as part of the human rights of Indonesian citizens. Therefore, the state must protect the processing of its citizens' data, including that of crypto asset customers. Physical crypto asset trading transactions are closely related to pseudonymisation data processing. On-chain crypto asset transactions, in the form of exchanges or transfers, will be recorded in the blockchain system as a wallet address or public address. In addition, physical crypto asset traders will also record and store transaction details, such as sender and recipient names, sender and recipient wallet addresses, and sender and recipient addresses, as part of their obligation to apply the travel rule principle.

Even though, in principle, the protection of pseudonymisation data requires that "additional information" that can be used to re-identify pseudonymisation data must be stored separately, physical crypto asset traders have, in practice, processed the pseudonymisation data of crypto asset customers. Unfortunately, the PDP Law does not regulate pseudonymisation data as a type subject to personal data protection principles. Moreover, physical traders of crypto assets are obligated to apply the know your customer principle.

Thus, Article 4 of the PDP Law needs to be reformed by adding "pseudonymisation data" as one type of personal data. This would give crypto asset customers legal certainty regarding legal protection in processing personal data as pseudonymisation data. Additionally, the PDP Law must accommodate criteria for re-identifying pseudonymisation data that is considered valid to guarantee legal certainty for crypto asset customers. Therefore, legal protection for crypto asset customers in processing personal data in pseudonymisation data will be achievable (not impossible) because regulations will govern it.

References

Abdul Karim, M. S., & Hadinata, F. (2023). Implikasi Filosofis Desentralisasi Bitcoin Dalam Perspektif Empire Negri-Hardt. *Jaqfi: Jurnal Aqidah dan Filsafat Islam*, *8*(1), 48–60. (In Indonesian). https://doi.org/10.15575/jaqfi.v8i1.26627

Adhiwisaksana, M. F., & Allagan, T. M. P. (2023). Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element. *Indonesian Journal of International Law*, *20*(3), 442–470. https://doi.org/10.17304/ijil.vol20.3.2

Alfin, M. H., Idayanti, S., & Rahayu, K. (2024). Regulasi Dan Mekanisme Jual Beli Aset Kripto Di Indonesia. *Jurnal Ilmiah Mahasiswa Ekonomi Syariah (JIMESHA)*, *3*(2), 179–188. (In Indonesian). https://doi.org/10.36908/jimesha.v3i2.312

Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law As a Patronage From the Development of Communication and Information Technology in Indonesia. *Perspektif*, *25*(1), 54–62. https://doi.org/10.30742/perspektif.v25i1.750

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. (In Indonesian). https://doi.org/10.38043/jah.v6i1.4484

Asrun, A. M. (2016). Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan di Mahkamah Konstitusi. *Jurnal Cita Hukum*, *4*(1), 133–154. (In Indonesian). https://doi.org/10.15408/jch.v4i1.3200

Atikah, I. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial Dan Budaya Syar-I, 10*(2), 497–514. (In Indonesian). https://doi.org/10.15408/sjsbs.v10i2.31691

Ausop, A. Z., & Aulia, E. S. N. (2018). Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam. *Jurnal Sosioteknologi*, *17*(1), 74–92. (In Indonesian). https://doi.org/10.5614/sostek.itbj.2018.17.1.8

Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform*, *18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law and Security Review*, *33*(2), 171–181. https://doi.org/10.1016/j.clsr.2016.11.002

Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, *6*(1), 76–93. https://doi.org/10.21776/ub.blj.2019.006.01.06

Dat, H. L. N. T., & An, C. T. T. (2024). The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam. *Vietnamese Journal of Legal Sciences*, *11*(2), 1–13. https://doi.org/10.2478/vjls-2024-0007

Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, *4*(1), 117–128. https://doi.org/10.21776/ub.blj.2017.004.01.06

Faozi, M., & Segara Gustanto, E. (2022). Kripto, Blockchain, Bitcoin, dan Masa Depan Bank Islam: Sebuah Literatur Review. *Quranomic: Jurnal Ekonomi Dan Bisnis Islam*, *1*(2), 127–151. (In Indonesian).

Finck, M., & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Handoko, R. M., Aulyansyah, B., Trisna, A., & Delon, R. (2024). Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, *4*(2), 64–74. (In Indonesian).

Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection and Privacy*, *2*(2), 145–158. https://doi.org/10.69554/qsst9019

Huang, T., & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data. *IEEE Access*, *11*, 109225–109236. https://doi.org/10.1109/ACCESS.2023.3321578

Imakura, A., Sakurai, T., Okada, Y., Fujii, T., Sakamoto, T., & Abe, H. (2023). Non-readily identifiable data collaboration analysis for multiple datasets including personal information. *Information Fusion*, *98*, 101826. https://doi.org/10.1016/j.inffus.2023.101826

Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, *232*, 104019. https://doi.org/10.1016/j.jnca.2024.104019

Jati, Hardian Satria, Zulfikar, A. A. (2021). Transaksi Cryptocurrency Perspektif Hukum Ekonomi Syariah. *Al-Adalah: Jurnal Hukum Dan Politik Islam*, *6*(2), 137–148. (In Indonesian). EDN: https://elibrary.ru/mrkhni. DOI: https://doi.org/10.35673/ajmpi.v6i2.1616

Joo, M. H., & Kwon, H. Y. (2023). Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, *40*(2), 101805. https://doi.org/10.1016/j.giq.2023.101805

Jose, N. S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal*, *10*(1), 34–58. https://doi.org/10.21776/ub.blj.2023.010.01.03

Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? *BMC Medical Informatics and Decision Making*, *19*(1), 1–7. https://doi.org/10.1186/s12911-019-0905-x

Kumar Rai, B. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, *5*(4).

Limniotis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, *5*(4), 1–33. https://doi.org/10.3390/cryptography5040034

Maulana, E. T. (2024). Regulasi Travel Rule Terhadap Transaksi Aset Virtual Lintas Batas Dalam Konteks Decentralized Finance Di Indonesia: Studi Banding Terhadap Markets In Crypto-Assets (Mica) Di Uni Eropa. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *6*(3), 565–584. (In Indonesian).

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, *34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Multazam, M. T., Phahlevi, R. R., Purnomo, M. I., Purwaningsih, S. B., & Sabirov, B. (2024). Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *11*(1), 26–52. https://doi.org/10.22304/pjih.v11n1.a2

Nanda Sari, A., & Gelar, T. (2024). Blockchain: Teknologi Dan Implementasinya. *Jurnal Mnemonic*, *7*(1), 63–70. (In Indonesian). https://doi.org/10.36040/mnemonic.v7i1.6961

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, *19*(1), 277–301. https://doi.org/10.28945/3573

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection Of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia). *Jurnal Rechts Vinding*, *12*(2), 261–279. (In Indonesian).

Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *6*(3), 556–575. https://doi.org/10.22304/pjih.v6n3.a7

Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, *9*(11), 1–10. (In Indonesian).

Rizko Ramadoni, S., Sukarmi, S., & Nur Widhiyanti, H. (2021). Konvergensi Hukum Penentuan Suku Bunga dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *9*(4), 821–837. (In Indonesian). https://doi.org/10.24843/jmhu.2020.v09.i04.p11

Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilasasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1099–1110. (In Indonesian). https://doi.org/10.37680/almanhaj.v5i2.3054

Setiawan, R. C., Idayanti, S., & Wildan, M. (2023). Perkembangan Komoditi Digital Dalam Aset Kripto Di Indonesia. *Pancasakti Law Journal*, *1*(2), 369–384. (In Indonesian).

Sinaga, E. M. C., & Putri, M. Ch. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237–256. (In Indonesian). https://doi.org/10.33331/rechtsvinding.v9i2.428

Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, *4*(1), 18–37. https://doi.org/10.33756/jlr.v4i1.11973

Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif Ham. *Seminar Nasional – Kota Ramah Hak Asasi Manusia*, *1*, 20–32. (In Indonesian).

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices – mobile phones. *Procedia Computer Science*, *151*(2018), 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. (In Indonesian). https://doi.org/10.21787/jskp.2.2023.55-68

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, *14*(2), 56–72.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, *38*, 105454. https://doi.org/10.1016/j.clsr.2020.105454

Tirtakoesoemah, A. J., & Arafat, M. R. (2019). Penerapan Teori Perlindungan Hukum Terhadap Hak Cipta Atas Penyiaran. *Pena Justisia*, *18*(1), 1–14. (In Indonesian). https://doi.org/10.31941/pj.v18i1.1084

Ulya, W., & Pambudi, L. A. (2024). Analisis Kebijakan Cryptocurrency dalam Perspektif Sadd Al-Dzari'ah. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, *5*(2), 102–111. (In Indonesian).

Utomo, T. P. (2022). Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan. *Buletin Perpustakaan*, *4*(2), 173–200. (In Indonesian).

Utomo, Y. A. (2020). Legal Protection for Problem Debtor Related to the Use of the Artificial Intelligence System in Peer to Peer Lending. *Yuridika*, *35*(3), 657. https://doi.org/10.20473/ydk.v35i3.19007

Wahyuningtyas, S. Yu. (2024). Legal Issues of Online Reputation Portability in the Digital Economy. *Jurnal Perkotaan*, *15*(2), 63–81. https://doi.org/10.25170/perkotaan.v15i2.5670

Yetno, A. (2021). Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia. *Satya Dharma: Journal Ilmu Hukum*, *4*(1). (In Indonesian).

Authors information

Mayuna I Komang Oki – Master of Law Student, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: okimayuna04@student.ub.ac.id
ORCID ID: https://orcid.org/0009-0002-0016-4788
Google Scholar ID: https://scholar.google.com/citations?user=H4cIKpwAAAAJ

Dewantara Reka – Dr. (Law), Associate Professor, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: rainerfh@ub.ac.id
ORCID ID: https://orcid.org/0000-0002-6010-0279
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58317982600
Google Scholar ID: https://scholar.google.co.id/citations?user=kP38YuQAAAAJ

Ruslijanto Patricia Audrey – Dr. (Law), Associate Professor, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: patricia@ub.ac.id
ORCID ID: https://orcid.org/0009-0006-6621-832X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201777768
Google Scholar ID: https://scholar.google.com/citations?user=TSr2eYoAAAAJ

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 – February 21, 2025
Date of approval – March 15, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:346.6:004.7
EDN: https://elibrary.ru/lqycmn
DOI: https://doi.org/10.21202/jdtl.2025.12

Псевдонимизация персональных данных пользователей криптоактивов: проблемы правового регулирования в Индонезии

И Команг Оки Маюна ✉
Университет Бравиджая, Маланг, Индонезия

Река Девантара
Университет Бравиджая, Маланг, Индонезия

Патриция Одри Руслиджанто
Университет Бравиджая, Маланг, Индонезия

Ключевые слова

законодательство,
защита персональных данных,
криптоактивы,
криптовалюта,
персональные данные,
право,
псевдонимизация,
технология блокчейн,
торговля криптоактивами,
цифровые технологии

Аннотация

Цель: анализ возможности обеспечения правовой защиты псевдонимизированных персональных данных пользователей криптоактивов в правовой системе Индонезии.

Методы: в работе применяется комплексный правовой анализ, основанный на изучении действующих нормативных правовых актов Индонезии в сфере защиты персональных данных. Исследование реализовано с использованием законодательного, концептуального и сравнительного методологических подходов, включающих анализ положений индонезийского Закона о защите персональных данных, Общего регламента Европейского союза по защите персональных данных и британского Закона о защите данных.

Результаты: установлено, что псевдонимизация данных пользователей криптоактивов в Индонезии осуществима с правовой точки зрения, однако существующее законодательство содержит существенные пробелы. Действующий Закон о защите персональных данных Индонезии не признает псевдонимизированные данные в качестве отдельной категории персональных данных, подлежащих правовой защите. Выявлена проблематичность реализации правила контроля переводов физическими трейдерами криптоактивов, поскольку дополнительная информация для реидентификации псевдонимизированных данных не хранится отдельно, что увеличивает риски нарушения конфиденциальности.

✉ Корреспондирующий автор

Научная новизна: проведен комплексный анализ правовых механизмов защиты псевдонимизированных данных в контексте криптовалютных операций. Предложена концептуальная модель совершенствования национального законодательства о защите персональных данных путем включения псевдонимизированных данных в качестве отдельной категории защищаемой информации. Разработаны рекомендации по установлению критериев законной реидентификации псевдонимизированных данных для обеспечения правовой определенности в сфере защиты пользователей криптоактивов.

Практическая значимость: результаты исследования могут служить теоретико-методологической основой для реформирования индонезийского Закона о защите персональных данных и создания эффективного правового механизма защиты пользователей криптоактивов. Предложенные изменения в ст. 4 указанного Закона позволят включить псевдонимизированные данные в перечень защищаемых категорий персональных данных, что обеспечит правовую определенность для участников криптовалютного рынка и повысит уровень защиты их персональных данных в условиях цифровой экономики.

Для цитирования

Маюна, И К. О., Девантара, Р., Руслиджанто, П. О. (2025). Псевдонимизация персональных данных пользователей криптоактивов: проблемы правового регулирования в Индонезии. *Journal of Digital Technologies and Law*, *3*(2), 275–303. https://doi.org/10.21202/jdtl.2025.12

Список литературы

Abdul Karim, M. S., & Hadinata, F. (2023). Implikasi Filosofis Desentralisasi Bitcoin Dalam Perspektif Empire Negri-Hardt. *Jaqfi: Jurnal Aqidah dan Filsafat Islam*, *8*(1), 48–60. (In Indonesian). https://doi.org/10.15575/jaqfi.v8i1.26627

Adhiwisaksana, M. F., & Allagan, T. M. P. (2023). Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element. *Indonesian Journal of International Law*, *20*(3), 442–470. https://doi.org/10.17304/ijil.vol20.3.2

Alfin, M. H., Idayanti, S., & Rahayu, K. (2024). Regulasi Dan Mekanisme Jual Beli Aset Kripto Di Indonesia. *Jurnal Ilmiah Mahasiswa Ekonomi Syariah (JIMESHA)*, *3*(2), 179–188. (In Indonesian). https://doi.org/10.36908/jimesha.v3i2.312

Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law As a Patronage From the Development of Communication and Information Technology in Indonesia. *Perspektif*, *25*(1), 54–62. https://doi.org/10.30742/perspektif.v25i1.750

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. (In Indonesian). https://doi.org/10.38043/jah.v6i1.4484

Asrun, A. M. (2016). Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan di Mahkamah Konstitusi. *Jurnal Cita Hukum*, *4*(1), 133–154. (In Indonesian). https://doi.org/10.15408/jch.v4i1.3200

Atikah, I. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial Dan Budaya Syar-I, 10*(2), 497–514. (In Indonesian). https://doi.org/10.15408/sjsbs.v10i2.31691

Ausop, A. Z., & Aulia, E. S. N. (2018). Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam. *Jurnal Sosioteknologi*, *17*(1), 74–92. (In Indonesian). https://doi.org/10.5614/sostek.itbj.2018.17.1.8

Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform*, *18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law and Security Review*, *33*(2), 171–181. https://doi.org/10.1016/j.clsr.2016.11.002

Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, *6*(1), 76–93. https://doi.org/10.21776/ub.blj.2019.006.01.06

Dat, H. L. N. T., & An, C. T. T. (2024). The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam. *Vietnamese Journal of Legal Sciences*, *11*(2), 1–13. https://doi.org/10.2478/vjls-2024-0007

Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, *4*(1), 117–128. https://doi.org/10.21776/ub.blj.2017.004.01.06

Faozi, M., & Segara Gustanto, E. (2022). Kripto, Blockchain, Bitcoin, dan Masa Depan Bank Islam: Sebuah Literatur Review. *Quranomic: Jurnal Ekonomi Dan Bisnis Islam*, *1*(2), 127–151. (In Indonesian).

Finck, M., & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Handoko, R. M., Aulyansyah, B., Trisna, A., & Delon, R. (2024). Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, *4*(2), 64–74. (In Indonesian).

Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection and Privacy*, *2*(2), 145–158. https://doi.org/10.69554/qsst9019

Huang, T., & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data. *IEEE Access*, *11*, 109225–109236. https://doi.org/10.1109/ACCESS.2023.3321578

Imakura, A., Sakurai, T., Okada, Y., Fujii, T., Sakamoto, T., & Abe, H. (2023). Non-readily identifiable data collaboration analysis for multiple datasets including personal information. *Information Fusion*, *98*, 101826. https://doi.org/10.1016/j.inffus.2023.101826

Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, *232*, 104019. https://doi.org/10.1016/j.jnca.2024.104019

Jati, Hardian Satria, Zulfikar, A. A. (2021). Transaksi Cryptocurrency Perspektif Hukum Ekonomi Syariah. *Al-Adalah: Jurnal Hukum Dan Politik Islam*, *6*(2), 137–148. (In Indonesian). EDN: https://elibrary.ru/mrkhni. DOI: https://doi.org/10.35673/ajmpi.v6i2.1616

Joo, M. H., & Kwon, H. Y. (2023). Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, *40*(2), 101805. https://doi.org/10.1016/j.giq.2023.101805

Jose, N. S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal*, *10*(1), 34–58. https://doi.org/10.21776/ub.blj.2023.010.01.03

Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? *BMC Medical Informatics and Decision Making*, *19*(1), 1–7. https://doi.org/10.1186/s12911-019-0905-x

Kumar Rai, B. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, *5*(4).

Limniotis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, *5*(4), 1–33. https://doi.org/10.3390/cryptography5040034

Maulana, E. T. (2024). Regulasi Travel Rule Terhadap Transaksi Aset Virtual Lintas Batas Dalam Konteks Decentralized Finance Di Indonesia: Studi Banding Terhadap Markets In Crypto-Assets (Mica) Di Uni Eropa. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *6*(3), 565–584. (In Indonesian).

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, *34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Multazam, M. T., Phahlevi, R. R., Purnomo, M. I., Purwaningsih, S. B., & Sabirov, B. (2024). Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *11*(1), 26–52. https://doi.org/10.22304/pjih.v11n1.a2

Nanda Sari, A., & Gelar, T. (2024). Blockchain: Teknologi Dan Implementasinya. *Jurnal Mnemonic*, *7*(1), 63–70. (In Indonesian). https://doi.org/10.36040/mnemonic.v7i1.6961

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, *19*(1), 277–301. https://doi.org/10.28945/3573

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection Of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia). *Jurnal Rechts Vinding*, *12*(2), 261–279. (In Indonesian).

Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *6*(3), 556–575. https://doi.org/10.22304/pjih.v6n3.a7

Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, *9*(11), 1–10. (In Indonesian).

Rizko Ramadoni, S., Sukarmi, S., & Nur Widhiyanti, H. (2021). Konvergensi Hukum Penentuan Suku Bunga dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *9*(4), 821–837. (In Indonesian). https://doi.org/10.24843/jmhu.2020.v09.i04.p11

Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilasasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1099–1110. (In Indonesian).

Setiawan, R. C., Idayanti, S., & Wildan, M. (2023). Perkembangan Komoditi Digital Dalam Aset Kripto Di Indonesia. *Pancasakti Law Journal*, *1*(2), 369–384. (In Indonesian). https://doi.org/10.24905/plj.v1i2.32

Sinaga, E. M. C., & Putri, M. Ch. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237–256. (In Indonesian). https://doi.org/10.33331/rechtsvinding.v9i2.428

Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, *4*(1), 18–37. https://doi.org/10.33756/jlr.v4i1.11973

Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif Ham. *Seminar Nasional – Kota Ramah Hak Asasi Manusia*, *1*, 20–32. (In Indonesian).

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices – mobile phones. *Procedia Computer Science*, *151*(2018), 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. (In Indonesian). https://doi.org/10.21787/jskp.2.2023.55-68

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, *14*(2), 56–72.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, *38*, 105454. https://doi.org/10.1016/j.clsr.2020.105454

Tirtakoesoemah, A. J., & Arafat, M. R. (2019). Penerapan Teori Perlindungan Hukum Terhadap Hak Cipta Atas Penyiaran. *Pena Justisia*, *18*(1), 1–14. (In Indonesian). https://doi.org/10.31941/pj.v18i1.1084

Ulya, W., & Pambudi, L. A. (2024). Analisis Kebijakan Cryptocurrency dalam Perspektif Sadd Al-Dzari'ah. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, *5*(2), 102–111. (In Indonesian).

Utomo, T. P. (2022). Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan. *Buletin Perpustakaan*, *4*(2), 173–200. (In Indonesian).

Utomo, Y. A. (2020). Legal Protection for Problem Debtor Related to the Use of the Artificial Intelligence System in Peer to Peer Lending. *Yuridika*, *35*(3), 657. https://doi.org/10.20473/ydk.v35i3.19007

Wahyuningtyas, S. Yu. (2024). Legal Issues of Online Reputation Portability in the Digital Economy. *Jurnal Perkotaan*, *15*(2), 63–81. https://doi.org/10.25170/perkotaan.v15i2.5670

Yetno, A. (2021). Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia. *Satya Dharma: Journal Ilmu Hukum*, *4*(1). (In Indonesian).

Сведения об авторах

Маюна И Команг Оки – магистрант в области права, факультет права, Университет Бравиджая
Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169
E-mail: okimayuna04@student.ub.ac.id
ORCID ID: https://orcid.org/0009-0002-0016-4788
Google Scholar ID: https://scholar.google.com/citations?user=H4clKpwAAAAJ

Девантара Река – доктор права, доцент, факультет права, Университет Бравиджая
Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169
E-mail: rainerfh@ub.ac.id
ORCID ID: https://orcid.org/0000-0002-6010-0279
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58317982600
Google Scholar ID: https://scholar.google.co.id/citations?user=kP38YuQAAAAJ

Руслиджанто Патриция Одри – доктор права, доцент, факультет права, Университет Бравиджая
Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169
E-mail: patricia@ub.ac.id
ORCID ID: https://orcid.org/0009-0006-6621-832X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201777768
Google Scholar ID: https://scholar.google.com/citations?user=TSr2eYoAAAAJ

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: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 21 февраля 2025 г.
Дата одобрения после рецензирования – 15 марта 2025 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.

Research article
UDC 34:004:34.096:004.8
EDN: https://elibrary.ru/nzbqnm
DOI: https://doi.org/10.21202/jdtl.2025.13

Regulatory Barriers in Digital Mergers and Acquisitions: Antitrust Regulation of Technology Sector

Kolawole Afuwape

O. P. Jindal Global University, Sonipat, India

Keywords

antimonopoly legislation,
competition,
digital economy,
digital technologies,
dominant position,
law,
legislation,
mergers and acquisitions,
technology giant,
technology sector

Abstract

Objective: to determine the nature and degree of influence of the antimonopoly legislation of the European Union and the USA on mergers and acquisitions in the technology sector.

Methods: the work uses a comparative and interdisciplinary approach combining legal analysis and economic modeling. The author performed a comparative analysis of the legislation of the European Union and the US, summarized antimonopoly regulation practices, and considered doctrinal sources and modern empirical data. The methods used include content analysis of regulations, case studies of the largest digital companies, and elements of forecasting the impact of regulatory changes on innovation activity and market dynamics.

Results: various approaches to regulation of mergers and acquisitions in the digital economy were considered. The peculiarities of law enforcement in the European Union and the USA were analyzed. It was proved that strict antitrust measures can both restrain market concentration and create barriers to innovation. The author found that the practice of applying the EU Law on Digital Markets and the US relevant acts significantly affects structural changes in the technology sector, forming new competition models. Recommendations are given on improving international cooperation and developing common and fair regulatory standards for digital markets. Special attention is paid to the problems of determining the dominant position, regulatory control, and specific features of digital markets.

Scientific novelty: the article systematically compares the regulatory regimes of the world's leading jurisdictions through the prism of digital mergers and acquisitions. It expands the categorical apparatus through modern approaches to the analysis of network effects, competition for data, and new forms of market power. The author applies his own criterion for analyzing the comprehensive examination of transactions from the viewpoint of sustainability and innovation potential.

Practical significance: the conclusions and recommendations contribute to the formation of a more flexible and adaptive regulatory policy towards technology giants, which is essential for lawmakers, regulators, corporate strategists and researchers of the digital economy.

For citation

Afuwape, K. (2025). Regulatory Barriers in Digital Mergers and Acquisitions: Antitrust Regulation of Technology Secto. *Journal of Digital Technologies and Law, 3*(2), 304–337. https://doi.org/10.21202/jdtl.2025.13

Contents

Introduction

The five biggest technological players Apple, Alphabet (Google), Amazon, Facebook[1] and Microsoft known as GAFAM are some of the largest market capitalization enterprises around the globe (Odrobina, 2023). As platforms with more than one side, they cover a vast network of products, applications, services, content and customers. It covers its costs mainly in the way that they create revenue by providing services to the different user groups discovered around the platform and by connecting them as well as within each group. In 2025, the total investment by GAFAM in research and development (R&D) is anticipated to reach remarkable levels[2]. Collectively, these corporations are expected to allocate more than $140 billion towards R&D initiatives, a figure that considerably exceeds the R&D expenditures of most countries, except for leading nations such as the United States, China, and Japan (Abbott & Spulber, 2024). The GAFAM companies consistently enhance their research and development expenditures each year, motivated by progress in artificial intelligence, cloud computing, augmented reality, and various other cutting-edge technologies (Coveri et al., 2024). Notably, Amazon, Alphabet (the parent company of Google), and Microsoft are at the forefront, with each investing tens of billions of dollars to advance and refine infrastructure, software, and novel technological innovations[3]. This huge investment highlights the crucial influence of these companies in developing the global innovation landscape, emphasizing their commitment to both internal expansion and market supremacy via technological advancement. They are also engaged in a highly vigorous level of M&A activities, alongside these significant investments (Jin et al., 2023).

1. Overview of Mergers and Acquisitions (M&A) in the Digital Economy

Below are the reasons any of the GAFAM platforms would be desirous of acquiring one of the innovative startup companies. First, the platform may require the products that are being offered by that startup to be used avails[4]. The GAFAM are increasingly competing on attention from consumers to keep them on the platform[5]. In this regard, product offer or features expansion is related to competition; acquisition therefore is how the firm

1 The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

2 Buntz, B. (2024, June 17). Top 30 R&D spending leaders of 2023: Big Tech firms spending hit new heights. R&D World. https://clck.ru/3MBq4m

3 Nouveau, P. (2022). Falling behind and in between the United States and China: can the European Union drive its digital transformation away from industrial path dependency? In J.-Ch. Defraigne, J. Wouters, E. Traversa, & D. Zurstrassen (Eds.), EU Industrial Policy in the Multipolar Economy (Ch. 11, pp. 332–381). Edward Elgar Publishing.

4 Maitry, R. (2022). Gafam Market Power: the role of a firm's age, data, and overlapping economic activities in merger and acquisition strategies.

5 Ibid.

enlarges its ecosystem. Secondly, the platform may want an input from the startup[6]. They, of course, have the valuable assets that tool might be interesting for the platform: innovation, patent, engineer, talent, customer base (Čirjevskis, 2019). Lastly, acquisition can be used as a way of regulating competition within the platform and keeping it the leading influencer in the market (Kretschmer et al., 2022). Because in the digital economy the most significant sources of value are the network effects, the company with many active users can ultimately become a direct competitor to the owner of the dominant network even if it did not provide similar services when acquiring the target firm (Koch & Windsperger, 2017). Thus, the object that is quantitatively small, but qualitatively significant, in acquiring a start-up is to restrict additional competition in the market. Today there are concerns that the GAFAM merely acquire startups to perpetuate their superiority on the markets (Staab, 2024).

2. Importance of Antitrust Laws in Regulating Tech M&A

Starting in the year 2024 starting offseason, the EU has implemented the first ex ante competition regulation in the digital sector through DMA, has initiated the first investigations into suspected noncompliance with DMA (Pošćić, 2024). At the same time, the EC and several EC member states' competition authorities have also continued to enforce traditional competition laws, launching comprehensive investigations into the conduct of the major incumbents of the digital sector, gradually increasing attention to digital mergers, and only recently actively investigating competition issues in such innovative spheres as generative AI and the metaverse (Graef, 2024).

Much needs to be said about the current state of the merger control. Its enforcement in Europe has been gradually moving up the scale becoming much more interventionist, if not aggressive, both in the EU and in particular in the United Kingdom that brought additional unpredictability into the global M&A market (Mateev, 2017). Academic literature has rather recently turned its concern to 'killer acquisitions,' wherein incumbent firms take over especially innovative targets or Nasch, or potential competitors (Saouma et al., 2023). There are also an increasing extent assessing non-barrier factors, meaning non-price remedies (quality, innovation), non-horizontal or ecosystem theories of harm (Robertson, 2024). Another novel somewhat controversial tool in the hands of the EC in digital mergers is a shift of its policy in Article 22 of the EU Merger Regulation (EUMR) (Krzykowski, 2024). The policy has since been transformative and has been relevant in three instances almost, none of which is exclusively in the digital sector (Illumina/Grail, Qualcomm/Autotalks and EEX/Nasdaq) (Tzanaki, 2023). The digital mergers under consideration in this section were

[6] Andersson, L., & Vergeer, V. L. (2023). Acquisitions vs corporate-startup collaboration: corporations quest to bemore innovative: A case study on the advantages and disadvantages of startupacquisitions and startup collaboration.

declared to the EC through the traditional means, these mergers show that the merged companies were satisfied with the traditional way asking for merger notification. Also, the March 2023 ECJ judgment – Towercast, allows national regulators to examine closed transactions ex post using abuse of dominance rules (Kyle et al., 2024). On the national level, Germany and Austria implemented a transaction value in 2017 due to an assumed lack of effectiveness against potential killer acquisitions, particularly in the digital economy and pharma/healthcare sectors (Kızılay, 2024).

The year 2023 saw high-profile challenges to transactions in digital markets in Adobe/Figma: Figma was a target of acquisition by Adobe, a software company that bought in for US$20 billion in December 2023, but both companies declared that they had decided to call off the deal[7]. This followed protests from the EC in November 2023, and the Competition and Markets Authority (CMA). The EC had two concerns about the transaction: the Committee for the investigation of this business argues that it being interoperable might have anticompetitive effects in the market of interactive product-design tools and that it would deny Figma from being able to compete with Adobe for the digital asset-creation tools. What the EC feared most was a so-called reverse killer acquisition, where Adobe could impair the development of the competing design tool.

Amazon/iRobot: Regarding the business combination deal, a retailer and technology giant Amazon and a home appliance manufacturer making robot vacuum cleaners (RVC) iRobot announced on 29 January 2024 that they were withdrawing from the proposed merger deal due to the hostile stand of the regulators[8]. The EC delivered a statement of objections to the companies on 27 November 2023 and in mid-January signaled its intention to intervene[9]. To the ECs consideration, Amazon may be interested in refusing other robot vacuum cleaner's manufacturers to access to Amazons own online mart after the transaction. The parties opted out of the deal rather than giving assurances to the EC about the effect.

Booking/eTraveli: On September 25, 2023, the EC prohibited take-over of the Stockholm based online flight bookings service provider eTraveli by Booking Holdings through £1.5bn bid[10]. The EC noted that the synergistic deal would have further enhanced Booking. Com's dominance in the HOTs OTA market enabling it to use the eTraveli capacities to be the best flight OTA in the EU and to grow the framework of travel services of Booking. The EC stated that the 'choice screen' remedies that were provided by Booking to be

7 Kloub, J., Carroll, D., & Signoret, L. D. (2024, June 7). European Union: How the European Commission is leading the charge in digital market regulation. GCR. https://clck.ru/3MBqKH

8 European Commission. (2023, July 6). Mergers: Commission opens in-depth investigation into the proposed acquisition of iRobot by Amazon. https://clck.ru/3MBqN9

9 Amazon Scraps Deal to Buy Maker of Roomba Amid Regulatory Scrutiny. (2024, January 29). The New York Times. https://clck.ru/3MBqPY

10 European Commission. (2023, September 25). Mergers: Commission prohibits proposed acquisition of eTraveli by Booking. https://clck.ru/3MBqQe

insufficient. It must be pointed out this is also the first EC decision where an 'ecosystem' theory of harm has been employed which suggests the European agencies are looking for different theories of harm in Digital Market. It is also the first not to apply the EC's merger guidelines on horizontal/non-horizontal mergers, instead relying on the EUMR. The company also sought to contest the decision and said in its response that the ruling challenges 'the ratio decidendi of this court and all other appellate courts'[11].

3. Strategic Drivers of M&A in Technology

In addition, these data driven economies of scope may arise as a byproduct of mergers which can be of value to multisided platforms as they also provide horizontal and vertical platform integration strategies (Henten & Windekilde, 2022). As such, platforms can disseminate insights made from exercising the data they collected to operate into similar horizontal markets (Almeida, 2023; Parker et al., 2021). Vertical opportunities: through data, platforms can identify new verticals that make sense for them and provide a direct threat to both upstream producers that depend on their platforms (Khan, 2019). Not only does the platform contain all the market players' operating data but they offer a vantage point superior to that of any single producer. Such data has helped most of the mobile operating system platforms to penetrate profitable upstream applications including music, maps, news, and fitness. Secrecy in an operating system's underlying technical data gives preferential treatment to apps created under the platform rather than third-party developers (Khandelwal et al., 2024). To evaluate the social utility of mergers, the role of information and whether it can create a sequence of monopolies which merge to form an organization covering an expanded range of markets by excluding competition needs to be questioned. Fourth, and finally, any good welfare analysis must always consider the impact of network externalities, tightly connected with the nature of multisided platforms (Tan & Zhou, 2021). Merchant effects occur because a user benefits from his participation on a platform depending on other users participating in the same platform. If so, mergers can create more value by intensifying and extending those forms of network effects (Chaoxian & Wei, 2024).

Leading to first movers are post economies of scope and economies of scale and network effects that result from structural and resource asymmetries – One consequence are super platforms or platforms of platforms: The BSP Banking model is a good example for that (Albert, 2020). On the other hand, M&As created what one could call winner-take-most gatekeepers over the digital ecosystems in which platforms operate (Parker & Van Alstyne, 2024). They arrange numerous interactions between their users who depend on the gatekeeper to address group phenomena and market failures that cannot be addressed on a one-off basis. Another way of putting this is that gatekeepers have exclusive control over multi-sided markets antitrust problems (Marty & Warin, 2023).

[11] Ibid.

4. Growth of the Digital Economy

In the initial half of 2024, preliminary indicators suggest a resurgence of initial public offerings (IPOs) and significant technology mergers and acquisitions[12]. Although elevated interest rates, inflationary pressures, geopolitical influences, and uncertainties surrounding the upcoming election results may hinder certain deal-making activities, it is anticipated that mergers and acquisitions will gain momentum as market conditions begin to stabilize[13]. Software remains the predominant catalyst for mergers and acquisitions within the Technology, Media, and Telecommunications (TMT) sector[14]. While the volume of transactions has not yet returned to historical highs, the value of deals reported in the software industry during the first half of 2024 is poised to exceed that of the previous year. In the initial six months of 2024, Synopsys's proposed acquisition of Ansys, valued at $32.5 billion, represented the second-largest transaction disclosed worldwide across all sectors[15]. During this period there are total of six software megadeals or transactions more than $5 billion as compared to four megadeals that all together were witnessed in 2023 only[16].

Some factors that may affect the incidence of software transactions include transferring cyber products from being packed as on-premises/IT service solutions to being in the SaaS modality (Gupta et al., 2024). With governmental authorities tightening reporting of cyber threats and incidents and increasing appreciation of the risks, this sector is expected to emerge as one of the most interesting segments for software acquisition soon. Looking at the recent acquisitions within the cybersecurity industry, one can conclude that the trend is rather solid. More specifically, it is important to mention Cisco's $28bn takeover of Splunk, which was the biggest software deal of 2023[17]. Further, Thoma Bravo concluded its plan to buy the artificial intelligence-backed cybersecurity company Darktrace for $5.3 billion[18]. CyberArk is also in the process of acquiring Venafi, a specialist in machine identity, for $1.5 billion[19]. Furthermore, Airbus has expanded

12 Levy, B. (2025, January 28). M&A in 2025: Big deals, winning hands, and wild cards. PWC. https://clck.ru/3MBuVY

13 Berlin, M. (2025, May 20). US M&A activity fell in April as business leaders seek more clarity on tariffs and their impacts. EY Parthenon. https://clck.ru/3MBueD

14 TMT M&A Global Review, H1-24 and Outlook. (2024, July). https://clck.ru/3MBqfV

15 Synopsys to Acquire Ansys, Creating a Leader in Silicon to Systems Design Solutions. (2024, January 16). Synopsys. https://clck.ru/3Mkuvc

16 2024 Mid-Year Outlook, Global M&A Trends in Technology, Media & Telecommunications, June 25, 2024. PWC. https://clck.ru/3MBqjB

17 Bradshaw, T., Fontanella-Khan, J., & Edgecliffe-Johnson, A. (2024). HPE agrees $14 bn Juniper deal. Technology US group bulks up its networking offering in sign of M&A revival. The Financial Times, 7–7.

18 Joseph, I. (2024, October 2). Thoma Bravo Completes $5.3 bn acquisition of Darktrace. PE Hub. https://clck.ru/3MBqn6

19 Waldman, A. (2024, May 20). CyberArk to acquire Venafi from Thoma Bravo for $1.5B. TechTarget. https://clck.ru/3MBvbm

its portfolio by acquiring INFODAS, a provider of cybersecurity and IT solutions. These transactions collectively highlight the sustained interest in this critical subsector[20].

Several favorable elements, such as alleviated fears regarding a potential recession, stabilized inflation rates, substantial reserves of unallocated capital, and valuations that do not adequately represent the increasing enthusiasm for mergers and acquisitions, indicate that the TMT sector is well-positioned for growth in M&A activities over the forthcoming six to twelve months[21]. The initial quarter of 2024 experienced a persistence of the deceleration observed in the previous year, as evidenced by the initiation of 291 initial public offerings (IPOs)[22]. This figure represents a 22% decline compared to the preceding quarter and a 13% reduction when assessed year-over-year. Global proceeds reached $23.2 billion, reflecting a quarter-over-quarter increase of 7% and a year-over-year rise of 3%, suggesting a movement towards larger initial public offerings (IPOs). The TMT sector has notably illustrated this trend, representing the two largest IPOs in the first half of 2024. Reddit's $860 million offering and Astera Labs' $820 million offering could serve as indicators for forthcoming IPOs[23]. However, it is possible that some of the more prominent companies may choose to postpone their IPOs until 2025 due to prevailing macroeconomic challenges and increased regulatory oversight[24].

In the technology industry, software represented 69% of transaction volumes and 64% of transaction values. In the first half of 2024, there was a 42% decline in software transaction volumes compared to the same period in 2023. However, transaction values rose by 41%, largely attributed to six significant megadeals. The subsequent largest subsector, IT services, represented 18% of both deal volumes and deal values, experiencing a 23% reduction in deal volumes alongside a significant 68% rise in deal values during the initial half of the year, largely attributed to three major transactions[25]. Similarly, the semiconductor sector reported a 29% decrease in deal volumes; however, it witnessed an impressive 93% increase in deal values, predominantly driven by a single substantial transaction.

---

20 Airbus Completes Acquisition of Infodas to Strengthen Cybersecurity Portfolio. (2024, September 6). Manufacturing and Business Technology. https://clck.ru/3MBvem

21 Preiskel, R., Vittala, K., Preiskel, D., & Stelges, P. (2024, December 12). Technology M&A 2025. Chambers and Partners. https://clck.ru/3MBw2s

22 Sabater, A. (2024, April 15). IPO activity slowdown stretches through Q1 2024. S&P Global. https://clck.ru/3MBvqK

23 Blum, S. (2024, December 2). Despite Pops from Reddit and Astera Labs, the Sluggish IPO Market Dragged on in 2024. Inc. https://clck.ru/3MBvse

24 Thought Leadership. (2024, September 30). IPO Market Trends & Outlook 2025. https://clck.ru/3MBvu3

25 Jaber, B., & Spiegel, B. (2025, January 28). Global M&A Industry Trends in Technology, Media & Telecommunications. PWC. https://clck.ru/3MBwKQ

5. Challenges of Regulating the Digital Markets

The distinctive features of multi-sided platforms present considerable challenges for competition policy (Marty & Warin, 2023). It is essential for competition authorities and judicial bodies to account for the intricate interconnections and complexities inherent in multi-sided platform markets when evaluating specific cases (Nobrega et al., 2024). A comprehensive analysis of a platform necessitates the examination of all its facets, as well as a thorough assessment of both the direct and indirect network effects in relation to their economic implications. Regulatory bodies overseeing competition have been engaged in discussions regarding the most effective strategy for managing digital markets (Kira, 2024). One perspective advocates for an ex-ante framework, which emphasizes proactive measures aimed at preventing anti-competitive practices (Bougette et al., 2024). On the other hand, another perspective resulting from the analysis of enforcement actions advocates for an ex-post scheme that only targets individual cases (Cini & Czulno, 2022). Notably, some countries are currently trying to adopt the so-called 'mixed' model that draws elements from both frameworks[26]. The EU was among the world's first movers in the diversification of its regulatory approach through the adoption of an ex-ante regulation like with the P2B Regulation in 2019 and more recently the DMA in 2022 (Larouche & de Streel, 2021). The latter pertains to anti-competitive conduct through engaging in unfair trade practices by so called 'gatekeeper' digital platforms, which allows for swift and effective market remedies.

The DMA has been accused of possibly slowing down innovation and incurring unpredictable costs; its effectiveness will, therefore, depend on the implementation process[27]. The United Kingdom has undertaken the role of reflecting the general disposition of the regulation alignment of the European Union, albeit with some modifications. The DMCC was intended to enable the DMU to issue codes of conduct for selected companies with an emphasis on the digital marketplace[28]. In contrast to the EU's desire

---

26 BRICS Competition Law & Policy Centre. (2023, May 25). Session on "Ex-ante vs ex-post regulation of digital markets", EEF 2023. https://clck.ru/3MBw5Y. In the words of Maxim Shaskolsky, a FAS Russia official. He noted the problems FAS encounters due to the digitalization of the public procurement sphere (use of pricing algorithms and auction robots by businesses) and added that in June 2023 the FAS intends to introduce Rules and Standards Model for the Collaboration between Participants of Digital Markets in CIS Member States.

27 Portuese, A. (2021, May 24). The digital markets act: European precautionary antitrust. Information Technology and Innovation Foundation. https://clck.ru/3MBw7t

28 Egerton-Doyle, V., Hunter, J. (2024, October 7). The UK's New Digital Markets Regime: Unfettered Discretion and Power for the CMA. Kluwer Competition Law Blog. https://clck.ru/3MBwMi. The DMCC represents the first two decades of the most monumental reforms to competition and consumer law in the UK. It strengthens the CMA's current powers that current legislation focuses on its new digital markets regime, aimed at perceived competition concerns connected to a handful of the most prominent tech firms in the country – "SMS Regime". This regime will be administered by a new directorate, the Digital Markets Unit ("DMU"), which has begun in "shadow" form since 2021 to now take on its role. In the DMCC, the following three major shifts are recognized: (i) the introduction of a new-ex-ante-digital markets regime; (ii) the augmentation of CMA's consumer law enforcement powers; (iii) the built-up growth of CMA's broader administrative and investigative powers.

for a homogenous approach of putting equal burdens on all gatekeepers, the United Kingdom encourages cooperation between the authorities and companies in the country. This approach allows the firms to collaborate with the DMU to establish conducts that answer their needs while taking into consideration the features of the strategic business models. In accordance with market investigations and studies, the CMA in the United Kingdom has exclusive rights, the existence of which implies that corrective actions might be taken against certain members of the market. In the United States, the Federal Trade Commission examines anti-competitive practices individually and possesses the authority to conduct market investigations. Initiatives like the American Innovation and Choice Online Bill, which sought to implement ex-ante regulations, failed to garner significant backing[29]. Critics contended that the bills' intent was not to benefit consumers but rather to impose penalties on specific American technology companies for their anti-competitive actions, such as self-preferencing, which do not necessarily harm the market or consumers[30].

The emergence of proposals aimed at regulating competition within digital markets can be attributed to a growing dissatisfaction with conventional competition law (Gorecka, 2024). This discontent stems from the perception that investigations are often sluggish and limited in scope, while the powers to impose remedies are insufficient. Consequently, competition authorities struggle to establish the comprehensive market framework necessary for the effective functioning of these digital environments. The discussion concerning suitable regulatory frameworks for digital markets is complex, featuring advocates and opponents of regulation who present persuasive arguments and divergent perspectives on the future of competition policy in the context of the digital era (Kuenzler, 2022). The barriers to equitable competition within digital marketplaces arise not solely from traditional antitrust issues, such as tying, leveraging, foreclosure, denial of market access, and the suppression of potential competition, but also from the influence of data-centric and platform-oriented business models. The proliferation of data significantly enhances business models that rely on user-generated information

[29] Heather, S. (2022, June 17). Striking Similarities: Comparing Europe's Digital Markets Act to the American Innovation and Choice Online Act. US Chamber of Commerce. https://clck.ru/3Mkxqr. The bill covers only the largest "online platform", which, for the purposes of this bill, is defined as "a website, online or mobile application, operating system, digital assistant, or an online service" designed to: (A) enable a user to generate or upload content for other users to view or otherwise engage with on itself; (B) facilitate commerce through a website for consumers or third-party businesses; or (C) enable user searches that display a significant amount of information. Apart from those platforms specifically covered in the previous definition, subsection (e) gives the power for the FTC and DOJ jointly to designate a covered platform, and such designation will be effective for seven years.

[30] Ibid. The bills are being criticized for undermining the integrity of cyberspace and privacy of users by compelling U.S. companies to share sensitive data with foreign competitors. These bills stranglehold markets that are in any case already evolving, apply a one-size-fits-all model to disparate business models that have very unalike implications, and generally suck the life and potential out of many small players in the ecosystem. Like the DMA, domestic antitrust bills carry with them excessive sanctions unconnected in any way with actual consumer harm, thereby blighting pro-competitive conduct.

(Saura et al., 2021). The integration of a new data stream into an established dataset results in a nonlinear transformation of the overall value derived from the complete data repository. An extreme manifestation of increasing returns could significantly influence the classification of market competition.

By limiting certain anticompetitive practices through ex-ante regulation, regulatory effectiveness may be improved, and resource allocation may be optimized (Lancieri & Pereira Neto, 2022). The ruling by the Court of Justice regarding the case brought by the EC against Google concerning its comparison-shopping services (Petrucci, 2023). According to the decision, the Court of Justice confirmed the decision of the EC that restricted Google from abusing its dominant position on the online search markets. In simple terms, the court sided with the commission's argument that Google officials considered its comparison-shopping service over other similar services in violation of opposition laws. Deciding on this appeal against an earlier judgment of the EC General Court that was in favor of the commission, the Court of Justice ruled that the General Court had rightly concluded that, having regard to the characteristics of the relevant market and the particulars of the case, Google's behavior was exclusionary and did not constitute 'competition on the merits.

The European General Court ruling in the Google AdSense case annulled an EC decision imposing a fine of almost €1.5 billion on Google regarding its online advertising intermediation service, AdSense for Search, by arguing, among other things, that the EC did not consider all the relevant circumstances in its assessment of the duration of the contractual provisions concluded to be abusive (Rikap et al., 2021). The ruling further clarifies the meaning and application of the concept of exclusivity obligations within Article 102 of the Treaty on the Functioning of the European Union and clarifies the proofs necessary for the EC to carry its burden of demonstrating ability to bring about anticompetitive effects, which was followed by rulings of the Court of Justice in the Intel and Unilever Italia cases.

Another notable case is that of the EC opening an official competition on Microsoft for bundling its Teams software, a cloud-based communication and collaboration site, with the Microsoft 365 and Office 365 suites marketed to business clients (Bergqvist, 2024). Teams were bundled in with the business suite purchase, and the users were not given the option to integrate competing workplace communications services like Slack or Zoom into their Microsoft 365 or Office 365 packages. Microsoft's announcement comes ahead of a definitive decision by the EU, which has yet to be reached, about the separation of Teams from the Microsoft 365 and Office 365 suites for business customers in the EU. This move aims to mitigate potential antitrust concerns, and as a result, Microsoft 365 subscriptions that do not include Teams will be offered at a reduced price. They also revealed intentions to enhance their documentation regarding interoperability, enabling users to incorporate alternative solutions such as Slack or Zoom alongside their current offerings, including Exchange and Outlook. Thus, the actual implementation of ex-ante

regulations to bar tying and bundling would not have been required, by implication of the below investigative process.

Some key opinions that have dominated this consideration include the fear of regulation inhibiting further development, especially in this field. However, the black and white division between the concept of regulation and the concept of innovation is so firmly entrenched that people often limit their vision to a binary choice between the two. Consequently, stressing more detailed institutional and especially legal overhauls instead of disregarding regulation should help innovation and growth among organizations working in digital markets. Therefore, the task of describing essential characteristics of these regulations may be passed to individual jurisdictions that will then adapt and implement them according to their need.

6. Regulatory Scrutiny in Tech M&A

There is evidence that corporate acquisition activity is shifting more toward small deals to avoid the attention of the regulator (Enriques & Gatti, 2015). This strategic move not only avoids some regulatory impacts but is also more in tune with a move back to more selective and quick strategic growth plays. It has also affected the time that transactions take, due to long approval processes and regulatory analysis that is increasing the time that deals are open. This situation does signify the need to be very particular about planning. With the advancement and integration of technology in operations, acquisition of technology has become incredibly important and has birthed what is now famously known as “techquisitions” (Ioramashvili et al., 2024). This is referring to the tendency of more dominant firms to buy out technology startups; meaning there is a consistent morphing to growth through the application of innovative strategies. As technology increasingly serves as a fundamental element of business success, organizations are incorporating innovative solutions into their offerings.

To mitigate the competitiveness factor emerging from the platform M&A, we cannot rely on the classic ex-post regulation interventions. An ex-post antitrust approach alone is too specific and overly conservative for active markers, in many instances the damage has already been done (Stephan, 2020). Collectively these economic forces can generate market-tipping behavior for which the opportunity losses cannot be recovered ex-post. Legal remedies also require modernization, even traditional antitrust legal instruments. Most platform markets resist using the ex-post tools of antitrust analysis to determine the proper sphere of markets (Bostoen, & Vanwamel, 2024).

The current high growth digital markets require more structural approaches that rely on ex-ante regulation before harm sets in as an extra tool to the ex-post enforcement (Prado, 2022). Thus, this paper builds on this foundation by investigating how we may integrate ex-ante regulatory instruments with merger control and antitrust enforcement. It concerns those platforms which, while being specific enough to be described

as infrastructure gatekeepers due to the number of interactions they process. On this subject, it examines the M&A strategies of these platforms when expanding, and the effects on competition. One cannot examine the competition antecedents of the phenomenon and state that innovative new ex-ante regulatory mechanism for information exchange together with the right upgrade of the merger analysis policy can assist the development of competitive more competitive and innovative nature of online ecosystems by embracing the platform M&As that proportionately provide efficiency and consumer welfare.

7. Different Approaches to Regulatory Scrutiny

Mergers and acquisitions strategies have the potential to create added value by incorporating new functionalities within either the horizontal or vertical supply chain (Carril-Caccia & Pavlova, 2020). Nevertheless, it is essential to address various competition-related issues. These concerns can be categorized into three main types: dynamic competitive concerns, horizontal and conglomerate merger concerns, and vertical merger concerns.

It is essential to establish a clear distinction between the second and third categories. To achieve this, we adhere to the "End-to-End" principle, which helps differentiate the components that belong to the network layer (platform) from those that are associated with the endpoints. The principle indicates that essential functions, which are frequently utilized by most users, ought to be positioned at the core of a system to ensure their constant availability to all users. Conversely, functions that are used less often and cater to specific niche groups should be located at the periphery, accessible solely to those who have a need for them. The rationale behind this is that incorporating each system function results in an overhead cost that diminishes execution efficiency. Consequently, this suggests that ecosystem partners, such as application developers, ought to offer highly variable and less frequently utilized functions to deliver tailored solutions within specific industry sectors. This function is not applicable universally, as not all users of operating systems engage in gaming. In contrast, the platform ought to offer functions that are widely utilized across various industries, albeit with limited variety. An example of a horizontal function is the cut-and-paste feature, which is utilized by all users and the majority of office and productivity applications (Goldsmith, 2017). It is therefore more effective to integrate the functionality directly into the operating system, allowing any application to utilize it. This principle is essential to the architecture of the internet and aligns with the perspective of platforms as a foundational set of stable, gradually evolving functions, which are situated beneath a layer of modular, rapidly changing functions.

The term 'killer' acquisitions, when utilized in the context of the digital industry, may equally pertain to the acquisition of emerging companies, the competitive relevance of whose offerings could be considered largely uncertain (Ivaldi et al., 2023). A 'killer' acquisition would likely have a detrimental effect on consumer welfare by

eliminating innovative alternatives from the market (Letina et al., 2024). However, it is considerably more challenging to reach the same conclusion regarding the acquisitions of emerging competitors within the technology sector. Many of these acquisitions undoubtedly contribute positively to consumer welfare by broadening the availability of innovative products. This objective can be accomplished by incorporating newly acquired features, applications, and functionalities into the current services.

The issue of "killer acquisitions" has garnered heightened attention within the antitrust community, particularly due to their significant detrimental impact on digital innovation (Eben & Reader, 2023). On the contrary, most acquisitions of small firms by established companies are not aimed at reducing competition; rather, they significantly enhance innovation by leveraging synergies and integrating complementary technologies (Čirjevskis, 2019). These transactions are referred to as "bolt-on acquisitions" (King et al., 2018). Most times, there are valid grounds to believe that established digital companies may have occasionally suppressed potential competition through what are referred to as "killer acquisitions"[31]. The existing enforcement framework ought to be modified to incorporate a dual approach: (i) an ex-ante control mechanism that mandates entities granted "strategic market status" to report their transactions (Manganelli & Nicita, 2022); and (ii) an ex-post implementation of Article 102 Treaty on the Functioning of the European Union (TFEU) by a specialized digital markets unit (Eroğlu & Koksal, 2024).

8. Effects of Antitrust Laws on Tech M&A

In the realm of merger control, various global antitrust authorities have expressed opposition to several transactions involving prominent technology firms. During the initial half of 2024, vertical acquisitions proposed by two major players, Meta[32] and Microsoft, encountered significant pushback[33]. The FTC initiated legal challenges against both companies, while Microsoft's attempt to acquire Activision experienced tumultuous scrutiny from the EC and the CMA, culminating in a temporary block by the CMA before the parties restructured the deal[34].

The scope of merger control has expanded beyond the conventional analysis of horizontal market shares to encompass a variety of newly identified competitive threats (Gilbert & Melamed, 2024). These include potential market entry, conglomerate

---

31 Hansson, D., & Tran, J. (2024). Is Tougher Application of Article 22 of the EU Merger Control the Deal Breaker?: Examining the Commission's Enforcement Against Killer Acquisitions in the Digital Economy. https://clck.ru/3MBwdp

32 The organization is recognized as extremist, its functioning is prohibited in the territory of the Russian Federation.

33 Kheriwala, S. (2024, December 16). Antitrust actions against major tech firms: A global overview. Storyboard18. https://clck.ru/3MBwqX

34 See for example, FTC. (2024, November 13). In the Matter of Microsoft/Activision Blizzard. https://clck.ru/3MBxak

effects, the strengthening of ecosystems, innovation-related harms, killer acquisitions, self-preferencing practices, access degradation, and other vertical issues. This shift is particularly pertinent in sensitive sectors, notably the digital and healthcare industries. Merger control authorities have increasingly concentrated on issues related to innovation (Mendelsohn & Breide, 2024). Their focus extends beyond merely evaluating pipeline overlaps; they are also committed to safeguarding the conditions necessary for emerging innovations, which refer to innovations that have not yet culminated in market-ready products.

The European Commission and various other merger control authorities have grown increasingly apprehensive that significant transactions are being overlooked, leading to potential competitive detriments that cannot be addressed through conventional merger control legislation. The claim posited that major technology firms and other entities were eliminating potential competitors before they had the opportunity to emerge, a phenomenon referred to as "killer acquisitions". This term also encompasses "reverse killer acquisitions", wherein the acquiring company effectively suppresses its own innovations in favor of those developed by the target company.

The EU has adopted an alternative approach. In the merger case involving Illumina and Grail, which pertained to a consolidation of two American firms that did not meet the turnover thresholds for merger control at either the EU or national level, the European Commission nonetheless asserted its jurisdiction by revising its policy regarding the application of the referral provision within the European Merger Regulation[35]. This provision grants the EC authority to oversee a merger when one or more member states submit a referral to the Commission, particularly due to apprehensions that the merger may substantially influence competition within those member states. It is yet to be determined whether the European Court of Justice will support the European Commission's stance to scrutinize transactions under Article 22 of the EUMR, despite the absence of national merger control filings and the failure to meet EUMR thresholds, provided that the criteria outlined in Article 22 EUMR are satisfied[36]. The Illumina case has introduced ambiguity regarding the applicability of EU merger control to acquisitions of innovative firms or those deemed essential to a supply chain, even in instances where such transactions do not meet the established thresholds. In several transactions that engage innovative or supply-critical firms, the analysis of merger control concerning the involved parties can no longer be limited to evaluating turnover and market shares.

35 Article 22 EUMR.

36 Illumina/Grail: European Court of Justice strikes down the European Commission's policy of accepting referrals of non-notifiable deals. (2024, September 13). Dentons. https://clck.ru/3MBx6B. In a ruling on the Illumina/Grail case, the European Court of Justice set aside the interpretation the General Court (GC) gave to Article 22 of EU Merger Regulation 139/2004 (EUMR). This judgment is a fundamental shift, bringing to an end the EC's practice of accepting referrals under Article 22 EUMR for transactions which fell outside the scope of national review powers of a Member State of the EU.

It is essential to consider the potential for a referral under Article 22 of the EUMR, and similar considerations should be applied to other jurisdictions that possess comparable pull-in authorities[37].

Behavioral remedies, such as supply commitments or the licensing of technology to rival firms, have historically been met with skepticism as solutions for anti-competitive mergers (Glick et al., 2023). In many instances, these commitments are deemed inadequate to address the anti-competitive consequences of a merger, despite their acceptance in a few specific cases, particularly following a comprehensive Phase II investigation.[38] The recent approval by the EC regarding the Microsoft/Activision Blizzard merger exemplifies this situation (Ziermann, 2023). The EC granted a complimentary license to consumers within the European Economic Area (EEA), enabling them to stream all existing and forthcoming Activision Blizzard PC and console games through any cloud gaming service of their preference, provided they hold a valid license. Additionally, a similar complimentary license was extended to cloud gaming service providers, permitting EEA-based gamers to stream any of Activision Blizzard's PC and console titles (Norris, 2024).

The EC continues to strongly advocate for remedies that include the divestiture of certain segments of the target company or potentially even portions of the buyer's current operations.[39] The standards set by merger authorities regarding divestment remedies have become increasingly stringent. To address competition-related issues, it is often inadequate to divest merely individual assets, products, or contracts. Rather, the divestment process now generally requires the separation of an entire business that can operate independently of the merging entities, potentially necessitating the inclusion of a wider array of assets beyond those directly related to the identified concerns. For a divestment business to operate independently, it generally needs to encompass all relevant assets and business operations. Additionally, it may be necessary to integrate comprehensive central functions, including accounting, finance, human resources, information technology, and research and development. Transitional support may be necessary and allowed for a limited period after the completion of the divestiture transaction; however, the essential functions must ultimately reside within the divested entity if the merger authorities determine this to be essential.

37 Article 22 EUMR Referrals Post-Illumina: Back to the Drawing Board? (2024, September 23). European Law Blog. https://clck.ru/3MBx9v

38 Bengtsson, C., Carpi, J. M., & Subočs, A. (2021). Anticompetitive effects. In EU Competition Law Volume II: Mergers and Acquisitions (pp. 363–562). Edward Elgar Publishing.

39 EC – Competition Policy. (2009, February 24). Official Journal of the European Union. https://clck.ru/3MBxBq

9. Global Perspectives on Tech M&A Regulation

9.1. Russia

Russian legislation and regulations on antitrust in M&A remain under contemporaneous development to address novel and advanced economic and technology trends (Redkina et al., 2023). Being the governmental authority, the Federal Antimonopoly Service (FAS) is also charged with the examination and application of competition law within the Russian Federation, which includes M&A (Khokhlov, 2017). This means that the regulation of antitrust is in a phase of constant change, which provides for the ability of the Federal Antitrust Service of Russia to adopt, analyze and act on new forms of economic and technological activities. The latest changes in the antitrust legislation were adopted on July 28, 2015, and concern the shifts in the regulating of M&As and changes the procedure for performing operations and introduce the new criterion for the transaction approval (Tsyganov et al., 2023).

When conducting the analysis of the merger, the FAS used dynamic rather than static methodology that looked at market definitions in relation to various products (Shastitko et al., 2022). The FAS believed that the relevant markets were the "integrated agro-tech markets" and argued that the value of seeds, agro-chemicals, and digital solutions, separately, was lower because the competitive environment of this sector shifted thanks to continuous technology advancement. The FAS put much focus on the assessment of the effects of the merger for both the vertical and the horizontal competition (Tsyganov et al., 2023).

9.2. India

Most of the rules of merger control and competition policy in India are set by Competition Act of 2002 with the watchdog agency being the Competition Commission of India (Hiwarale et al., 2024). In these regulations, the government seeks to reign in anti-competitive behavior, encourage acceptable competition and support the consumer. There is a gradual evolution of India's merger controls and competition policies for responding to the emerging challenges in modern markets especially technology and digital space (Reddy, 2016). The current Changes in the Competition Act of 2023 depicted a movement to a more tough and extended act that is expected aim and protect consumers to regulate and encourage competition, check mergers, and acquisitions that may hamper the competition within the relevant market.

The Indian government has made recent changes to the Indian Competition Act of 2002 finer, to incorporate modern international standards and adapt to novel issues emerging in the digital economy. In addition, the government is contemplating the ex-ante regulatory mechanism compatible with the proposed work model that might be adopted in India akin to the EC's DMA now alongside the existing competition legislations (Afuwape, 2024; Soni & Kumar, 2024).

The Competition Act 2023 reduces the time within which the Competition Commission of India (CCI) must review a transaction and come up with a preliminary view. The CCI is now given 30 calendar days, against 30 working days, exclusive of clock stops. In addition, the limit of the deemed approval has reduced to a maximum of 150 calendar days with clock stops from 210 calendar days. While this switch would seem to be positive for the industry, it is important that the intensified appurtenance of approval schedules be matched with a substantial boost in the CCI's performance capability. This will allow the regulator to avoid work overload and acquire M&As at the same pace as before.

9.3. The United Kingdom

New legislation in the United Kingdom known as the Digital Markets, Competition, and Consumers Act (DMCC) comes into operation as of 1st of January 2025 (Alexiadis, 2024). This act provides the CMA with powers of greater scope for its merger control, digital markets, competition and consumer protection legislation. The extension of the number of transactions that are under merger control is possible due to the new alternative merger threshold provided by the DMCC (Alexiadis, 2024). This strategic move aims at improving fairness of the digital market, for example, by introducing new tough notification regimes for companies given 'Strategic Market Status'. Further, it greatly improves the enforcement powers of the CMA in a wider sense of the term. The CMA, however, is keen on acknowledging the need for new thresholds and proceedings to boost the volume of assessments of mergers and acquisitions aspiring to solve the market challenges with emerging competitors, also known as "killer acquisitions," whereupon the DMCC implemented new thresholds and proceedings for the CMA.

The dark line there introduced a new threshold under which the previous condition stating that the acquirer and target had to carry out overlapping activities in the UK, or the target had to have important operations in the UK, was disposed of. This change extends jurisdiction of the CMA to review acquisitions of targets where the revenue from the sale of goods and services in the United Kingdom is either nominal or in some cases nil, in addition to reviewing vertical and conglomerate mergers. However, as one will discover, achieving this figure does not mandate a filing but does allow the CMA to review a transaction. Consequently, this may encourage voluntary submissions when the threshold is satisfied, as many acquirers will seek assurance regarding the potential for CMA review of their transactions.

The DMCC grants authority to the CMA's Digital Markets Unit (DMU) to oversee the activities of significant enterprises operating within digital markets (Marinova, 2024). Upon receiving the designation of "Strategic Market Status" (SMS), these companies will be subject to obligations and stipulations as outlined by the DMCC (Highfield, 2024). The CMA has announced that its preliminary investigations will concentrate on three to four firms. Sarah Cardell, the CMA's chief executive, has underscored that these investigations will be characterized by an "evidence-based, targeted, and proportionate"

approach[40]. One of the primary responsibilities of SMS companies is to comply with customized conduct requirements (CRs) that govern their behavior concerning the activities for which they have been appointed. Since CRs are specific to each firm, they are expected to differ significantly, in contrast to the more prescriptive guidelines outlined in the European Union's DMA.

9.4. US Antitrust Scrutiny

Antitrust legislation in the US is essential for overseeing business conduct and fostering equitable competition within the market (Ganguli, 2024). The two dominant pieces of legislation profiled are the Sherman Antitrust Act and the Clayton Antitrust Act (Linneman, 2022). Sherman Antitrust Act was passed in 1890 to avoid activities that cause a hindrance to trade and thus give rise to monopoly (de Carvalho, 2024). They banned those arrangements of contracts or business affiliation that tend to restrict free competition. Among them are the Sherman Anti-Trust Act, the Clayton Antitrust legislation, which was also passed in the same year that the Interstate Commerce Act was passed, builds further these antitrust laws by prohibiting practices including price discrimination and tying arrangements and exclusive dealing. It can be argued that the level of the error of 'false negatives' is larger in merger control as opposed to sections 1 and 2 of the Sherman Act (Casey & Niblett, 2021). This may be attributed to the high standard of proof that has been put in place by the US antitrust regulations, which undergo a tough judicial scrutiny on substantive merit, basically, and not conforming to the administrative law tests. Moreover, the financial consequences of violation of the anti-trust laws are incredibly grave. The principle of the separation between the antitrust regulations and sector-specific authorities is strictly adhered to in the United States, thus, the above-mentioned policy trade-off is less simplistic compared to the trade-off in many cross-jurisdictional systems across the world.

9.5. The EU

The EC has been assessing mergers since 1990 pursuant to its Merger Regulations (EC Regulations) (Levy et al., 2021). These regulations empower the Commission as the sole institution capable of considering mergers that have a "Community aspect" and of prohibiting those which create, or strengthen, a dominant position within the Common Market. Nevertheless, according to the above-mentioned EC Regulations, the said impediment "generally results from the creation or reinforcement of a dominant position"[41].

---

[40] Israel, M., Engel, M., Kelliher, K., & Citron, P. (Eds.). (2024, December 16). UK Expands its Merger Control Regime and the CMA's Power with the Digital markets, Competition & Consumers act. Kluwer Competition Law blog. https://clck.ru/3MBxNg

[41] EU. (2004). EU Merger Regulation 139/2004. https://clck.ru/3MCJDZ

In addition to these regulations, a new and extensive set of enforcement guidelines was introduced to help in the assessment of horizontal mergers. In the EC Guidelines, it is described how the Commission assesses concentrations concerning undertakings that are actual or potential competitors on the same relevant product market (Nazzini, 2006).

10. Policy Implications of the Present and Future of Digital M&A Regulation

The state of regulation, thus, has had changes in the past few years. This evolution is in an effort to fit new technologies that also influence mergers and acquisitions across the world but mainly in United States and Europe. Antitrust authorities are intensifying scrutiny of mergers and acquisitions involving major technology firms (Crandall, 2024). The evaluation procedures are increasingly rigorous, demonstrating a dedication to maintaining equitable competition and curbing monopolistic behaviors (Xie & Wu, 2024). Broadcom's acquisition of VMware, valued at $69 billion, underwent a rigorous examination lasting 59 weeks and spanning three fiscal years, underscoring the extensive global approvals necessary for such a transaction[42]. Microsoft's acquisition of Activision has encountered scrutiny from the Federal Trade Commission (FTC) nearly two years following the announcement of the agreement (Norris, 2024). This situation illustrates that regulatory hurdles may continue to arise well beyond the initial stages of a business transaction.

The outlook of the Digital M&A is to the effect that there would be the scaling up of acquisition of startups facilitates access to innovative and exclusive technologies, enabling larger corporations to maintain a leading position within their respective sectors (Xu & Deng, 2024). Accelerated growth is leveraging on the insights and innovations derived from startups that substantially boost expansion efforts, while avoiding the protracted processes typically linked to in-house development. The emergence of market expansion boosting startups that have successfully built a presence and cultivated a customer base that can utilize resources to expedite their growth trajectory.

Artificial intelligence (AI) will significantly transform the technology landscape and is now influencing M&A processes[43]. Tools powered by AI facilitate market analysis, valuation, and due diligence, enabling organizations to make informed decisions based on data with remarkable precision. The influence of emerging technologies on businesses will drive them to adopt cutting-edge solutions utilizing blockchain, artificial intelligence, and edge computing to maintain a competitive advantage (Chatterjee et al., 2023).

---

[42] Broadcom completes its $61 billion acquisition of VMware. (2023, November 23). Times of India. https://clck.ru/3MBxjw

[43] Cazzaro, M. (2024). AI and Machine Learning in M&A: A Quantitative Analysis of Their Impact on Deal Outcomes.

As cyber threats become more sophisticated, organizations are recognizing the critical need to protect their digital assets. It is expected that M&As will increasingly prioritize cybersecurity, with companies aiming to acquire specialized cybersecurity firms to improve their data protection measures and strengthen their security infrastructures[44]. This trend will be especially relevant in sectors that manage large volumes of sensitive data, such as finance, healthcare, and e-commerce, where the preservation of digital trust is paramount.

The M&A landscape in healthcare technology is expected to maintain its robustness, particularly in sectors such as telemedicine, digital health solutions, and wearable technology. Additionally, the acquisition of biotechnology firms is likely to increase as organizations aim to capitalize on innovations in genetics, diagnostic tools, and personalized medicine to enhance their health technology portfolios.

Excellent high quality extensive data recourses are likely to lead to high market valuations among businesses. The ability to capitalize on customer data and behavior and to comprehend the trends within the industry make data-intensive businesses especially desirable. M&A strategies will, therefore, focus on entities with excellent data capabilities and capabilities, so that the acquiring companies can discover new opportunities, improve personalization tactics, and create subsidiary products that are value based (Lawton et al., 2024)

PE firms are escalating their involvement in M&As within the technology sector because of the feasible attractive returns within booming technology markets (Nary & Kaul, 2023). These firms will probably seek to acquire tech firms that work in niches like SaaS, cloud and cybersecurity firms. Such acquisitions provide PE firms resilient investment opportunities due to their capabilities to create awareness and brokerage diversified investment opportunities that can also improve their position in the technology market.

The idea of the metaverse has stirred much interest as the next level of virtual communication. Those industries, which invested in virtual reality (VR), augmented reality (AR), and immersive technologies can occupy lists of probable M&A contenders. Some of the uses of these technologies are in virtual work environments, client interaction solutions by acquiring metaaverse-related technologies an organization can increase their product portfolio and tap into the growing space in this market.

More and more, consideration of environmental, social, and governance (ESG) issues is emerging as a key element of M&A plans. With increased focus on sustainable development by the regulatory authorities and increased consciousness among the consumer organizations, green technologies, more and more are likely to feature in the M&A transactions. It is assumed that key Silicon Valley technology companies

[44] Raunio, P. (2024). Cyber Due Diligence Process Prototype. Jamk. https://clck.ru/3MBy7o

will target organizations that can show efficiency in energy management and carbon neutralization together with technological innovation with an emphasis on sustainability. Measures and initiatives that will be implemented as part of strategic management will not only advance corporate sustainability initiatives but also fit the investors' ESG approach.

Businesses would be in good shape in order to attain a better position as opposed to counterparts by coming up with more innovative solutions. A constant innovation within the specifications of software development has been attributed to the rise of the trend in consolidation and thus the mergers and acquisitions trajectories.

An increase in the regulation of M&As will occur, and organizations will be required to navigate the regulatory environment at the instigation of industry regulators that require companies to professionally manage M&As through policymaking and compliance with the modern legal disclosure and requirements of antitrust laws.

On the factor of cultural compatibility and innovation to pursue better transactions to ensure cultural compatibility as well as promote the aspect of innovation in future transactions it will be important for the next upcoming deals.

11. Recommendations

EU and US antitrust laws need to be modified for digital technology M&A separately because digital markets create new issues that were not present before. Recently, the appearance of rather large digital ecosystems has led to debates about the need for changes in antitrust laws. However, there are those people who argue that the current market trends correspond to improvements in total wellbeing. More assertiveness should be considered whilst implementing the antitrust enforcement to avoid increasing concentration with the industries addressing the unique challenges posed by digital markets.

1. Antitrust enforcement should consider adopting more assertive approaches to address the growing concentration within industries. On the other hand, the difficulties experienced in proving the negative impacts originating from the dominance of the dominant multiplatform are said to show that the assessment of consumer welfare implications of antitrust should not heavily depend on price theory.

2. The DMA requires that gatekeepers inform the EC of any M&A involving core platform services or other digital services. Additionally, the EC has the authority to temporarily suspend further M&A activities by a gatekeeper in cases of ongoing non-compliance with the DMA.

3. The EC should consider imposing levies of some of the most substantial penalties globally for violations of competition regulations. Nevertheless, the effectiveness of these significant fines is influenced by various factors, including the scale of the companies implicated, the likelihood of identifying such violations, and additional considerations.

4. The landscape of ESG regulations, legislation, and voluntary frameworks is expanding, with recent advancements particularly significant in the areas of supply chain due diligence and social considerations, including human rights. Organizations that operate with intricate supply chains, as well as those within highly regulated industries like finance, are especially susceptible to challenges and regulatory oversight related to ESG matters. From the M&As point of view, this means understanding the most efficient approaches to the process of fitting a target firm into the buyer's due diligence structure. It also covers assessment of governance and preparedness for current and future topics, including sustainability reporting, supply change management, and transition.

5. The regulation proposed in this paper involves formulation and enforcement of a "code of conduct" among the firms that have been identified as having "strategic market status." Third, it would promote better value and improved portability of personal data as well as encourage systems that are based on open standards. The unit would also aim at enhancing data openness; especially in cases where exclusive access to data constitutes exclusion in the market. Moreover, it would be designed to promote competition, evaluate mergers which may generate digital barriers to competition and collect information on trends and evolutions of digital markets.

6. Studying the consequences of digital mergers, over the long term, implies studying their effects on potential future innovation and competition besides the need to protect oneself against threats from peripheral competitors.

7. Considering the lowering or shifting the burden of proof as to infringement, or lowering what is acceptable judicial scrutiny applied on the decisions of competition authorities has been an issue in the past. Applying the direct legal prohibition of certain unilateral conducts occurred in the digital markets and shifted the burden of proof of the pro-competitive effects of the practices onto incumbent players. As such, the set recommendations should be backed by intensive, organized, and scientific research of the relevant markets, as well as assessment of the effects of the suggested changes before the application of all change processes grounded on evidence.

8. Formulate guidelines that clearly outline the potential ways in which mergers within the technology sector could hinder innovation. This should encompass qualitative evaluations of the merger's effects on competition and progress in technological development.

Conclusion

M&As have historically served as a fundamental element of the corporate sector. As the business and technological environments continue to evolve, the future of M&A is characterized by emerging trends and forecasts that are poised to influence the methods by which companies engage in business combinations activities in the forthcoming years.

The trajectory of M&As within the technology sector is characterized by dynamism and abundant opportunities, propelled by innovations in technology, shifts in regulatory frameworks, and evolving market needs. It is imperative for companies to remain vigilant and flexible to effectively maneuver through the intricate landscape of M&A activities. Through the strategic utilization of emerging technologies, a comprehensive understanding of regulatory frameworks, and an emphasis on innovation alongside cultural alignment, organizations can effectively position themselves for growth and success within the dynamic landscape of M&As. The future of M&As is poised to be both dynamic and transformative for companies globally, whether through international transactions or the acquisition of technological innovations.

References

Abbott, A. F., & Spulber, D. F. (2024). Antitrust Merger Policy and Innovation Competition. *Journal of Business & Technology Law*, *19*(2), 2.

Afuwape, K. (2024). Analysing the Ex-ante Regulations in India's Digital Competition Bill and Its Effects on Indian Business Interests. *World Competition*, *47*(4), 521–556. https://doi.org/10.54648/woco2024030

Albert, J. R. G. (2020). *Towards measuring the platform economy: Concepts, indicators, and issues* (No. 2020-28). PIDS Discussion Paper Series.

Alexiadis, P. (2024). The UK's Digital Markets, Competition and Consumers Act Passes into Law. *Business Law International*, *25*(3), 271–201.

Almeida, F. (2023). Foresights for big data across industries. *Foresight*, *25*(3), 334–348.

Bergqvist, C. (2024). *The EU's Investigation Into Microsoft Teams: A Preliminary Assessment*. https://doi.org/10.2139/ssrn.4888247

Bostoen, F., & Vanwamel, D. (2024). The Digital Markets Act: A partial solution to antitrust's remedy problem. *Common Market Law Review*, *61*(6). https://doi.org/10.54648/cola2024103

Bougette, P., Budzinski, O., & Marty, F. (2024). *Ex-ante versus Ex-post in Competition Law Enforcement: Blurred Boundaries and Economic Rationale* (No. 2024-18). Groupe de REcherche en Droit, Economie, Gestion (GREDEG CNRS), Université Côte d'Azur, France.

Carril-Caccia, F., & Pavlova, E. (2020). Mergers and acquisitions & trade: A global value chain analysis. *The World Economy*, *43*(3), 586–614. https://doi.org/10.1111/twec.12882

Casey, A. J., & Niblett, A. (2021). Micro-Detectives and Computational Merger Review. *Stan. Computational Antitrust*, *1*, 132. https://doi.org/10.51868/8

Chaoxian, G., & Wei, H. (2024). Industrial Organization in the Digital Economy Era: Evolution and Effects. *China Economist*, *19*(4), 15–36. https://doi.org/10.19602/j.chinaeconomist.2024.07.02

Chatterjee, S., Chaudhuri, R., Kamble, S., Gupta, S., & Sivarajah, U. (2023). Adoption of artificial intelligence and cutting-edge technologies for production system sustainability: a moderator-mediation analysis. *Information Systems Frontiers*, *25*(5), 1779–1794. https://doi.org/10.1007/s10796-022-10317-x

Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration*, *44*(1), 41–57. https://doi.org/10.1080/07036337.2021.2011260

Čirjevskis, A. (2019). The Role of Dynamic Capabilities as Drivers of Business Model Innovation in Mergers and Acquisitions of Technology-Advanced Firms. *Journal of Open Innovation: Technology, Market, and Complexity*, *5*(1), 12. https://doi.org/10.3390/joitmc5010012

Coveri, A., Cozza, C., & Guarascio, D. (2024). Blurring boundaries: an analysis of the digital platforms-military nexus. *Review of Political Economy*, 1–32. https://doi.org/10.1080/09538259.2024.2395832

Crandall, R. W. (2024). Towards a More Vigorous Antitrust Policy? *Review of Industrial Organization*, 1–16. https://doi.org/10.1007/s11151-024-09981-x

de Carvalho, S. (2024). The Roots of Antitrust Policy in the United States' Sherman Act. *International Investment Law Journal*, *4*(1), 92–110.

Eben, M., & Reader, D. (2023). Taking aim at innovation-crushing mergers: a killer instinct unleashed?. *Yearbook of European Law*, *42*, 286–321. https://doi.org/10.1093/yel/yead013

Enriques, L., & Gatti, M. (2015). Creeping acquisitions in Europe: enabling companies to be better safe than sorry. *Journal of Corporate Law Studies*, *15*(1), 55–101.

Eroğlu, M., & Koksal, A. (2024). Ex-Post Application of Structural Remedies to Large Online Platforms at a National Level. *İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi*, *9*(1), 135–169. https://doi.org/10.58733/imhfd.1451588

Ganguli, P. (2024). *International Perspectives on Antitrust Laws: A Comparative Study of India, the US, and the EU*. http://dx.doi.org/10.2139/ssrn.5006751

Gilbert, R. J., & Melamed, A. D. (2024). Potential Competition and the 2023 Merger Guidelines. *Review of Industrial Organization*, *65*, 269–302. https://doi.org/10.1007/s11151-024-09964-y

Glick, M., Lozada, G. A., Govindan, P., & Bush, D. (2023). The Horizontal Merger Efficiency Fallacy. *Temple Law Review*, *96*, 571. https://doi.org/10.36687/inetwp212

Goldsmith, J. (2017). A comparative user evaluation of tablets and tools for consecutive interpreters. *Proceedings of Translating and the Computer*, *39*, 40–50.

Gorecka, A. (2024). *The interface between competition law and data privacy law: violation of privacy as an exploitative theory of harm under Article 102 TFEU*. Switzerland: Springer International. https://doi.org/10.1007/978-3-031-73865-4

Graef, I. (2024). Regulating Digital Platforms: Streamlining the Interaction between the Digital Markets Act and National Competition Regimes. In *The Legal Consistency of Technology Regulation in Europe* (pp. 157–176). Hart Publishing. https://doi.org/10.5040/9781509968053.ch-008

Gupta, M., Gupta, D., & Rai, P. (2024). Exploring the Impact of Software as a Service (SaaS) on Human Life. *EAI Endorsed Transactions on Internet of Things*, *10*. https://doi.org/10.4108/eetiot.4821

Henten, A., & Windekilde, I. (2022). Demand-Side Economies of Scope in Big Tech Business Modelling and Strategy. *Systems*, *10*(6), 246. https://doi.org/10.3390/systems10060246

Highfield, J. (2024). Is Big Necessarily Bad? An Examination of the Revolutionary DMA and DMCC Designation Criteria. *North East Law Review*, *10*, 75–86.

Hiwarale, M. M. G., Irene, M., Jaiswal, D., & Tyagi, A. (2024). Competition Comission Of India: Safeguarding Fair Play In Mergers And Acqusitions In India. *Library Progress International*, *44*(3), 9966–9977.

Ioramashvili, C., Feldman, M., Guy, F., & Iammarino, S. (2024). Gathering round Big Tech: How the market for acquisitions concentrates the digital sector. *Cambridge Journal of Regions, Economy and Society*, *17*(2), 293–306. https://doi.org/10.1093/cjres/rsae003

Ivaldi, M., Petit, N., & Unekbas, S. (2023). Killer acquisitions: Evidence from EC merger cases in digital industries. *Antitrust Law Journal – TSE Working Paper*, 13-1420. https://doi.org/10.2139/ssrn.4407333

Jin, G. Z., Leccese, M., & Wagman, L. (2023). How do top acquirers compare in technology mergers? New evidence from an SP taxonomy. *International Journal of Industrial Organization*, *89*, 102891. https://doi.org/10.1016/j.ijindorg.2022.102891

Khan, L. M. (2019). The Separation of Platforms and Commerce. *Columbia Law Review*, *119*(4), 973–1098.

Khandelwal, R., Nayak, A., Chung, P., Fawaz, K., Bianchi, A., Celik, Z. B., ... & Hussain, S. R. (2024). Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 2831–2848). Philadelphia PA USA.

Khokhlov, E. (2017). The Russian Federal Antimonopoly Service's Case Against Google Related to Bundling and other Anticompetitive Practices with Respect to Android. *Journal of European Competition Law & Practice*, *8*(7), 468–474. https://doi.org/10.1093/jeclap/lpx036

King, D. R., Schriber, S., Bauer, F., & Amiri, S. (2018). Acquisitions as corporate entrepreneurship. In *Advances in mergers and acquisitions* (pp. 119–144). Emerald Publishing Limited. https://doi.org/10.1108/S1479-361X20180000017006

Kira, B. (2024). Inter-Agency Coordination and Digital Platform Regulation: Lessons from the WhatsApp Case in Brazil. *International Review of Law, Computers & Technology*, *39*(1), 6–29. https://doi.org/10.1080/13600869.2024.2351671

Kızılay, A. S. (2024). Lack of Effective Control on Killer Acquisitions in the Big Tech Market under EU Framework: Rethinking of EUMR Rules?. *Public and Private International Law Bulletin*, *44*(1), 253–280. https://doi.org/10.26650/ppil.2023.44.1.110941

Koch, T., & Windsperger, J. (2017). Seeing through the network: Competitive advantage in the digital economy. *Journal of Organization Design*, *6*, 1–30. https://doi.org/10.1186/s41469-017-0016-z

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, *43*(3), 405–424. https://doi.org/10.1002/smj.3250

Krzykowski, M. (2024). Article 22 of the EC Merger Regulation–national and European control: energy sector. In *Research Handbook on EU Competition Law and the Energy Transition* (pp. 278–297). Edward Elgar Publishing. https://doi.org/10.4337/9781803922591.00021

Kuenzler, A. (2022). What competition law can do for data privacy (and vice versa). *Computer Law & Security Review*, *47*, 105757. https://doi.org/10.1016/j.clsr.2022.105757

Kyle, M., Shah, O., & Mani, V. (2024). Hot tub time machine? What role for Towercast in EU merger control. *Journal of European Competition Law & Practice*, *15*(6), 436–443. https://doi.org/10.1093/jeclap/lpae057

Lancieri, F., & Pereira Neto, C. M. S. (2022). Designing remedies for digital markets: The interplay between antitrust and regulation. *Journal of Competition Law & Economics*, *18*(3), 613–669. https://doi.org/10.1093/joclec/nhab022

Larouche, P., de Streel, A. (2021). The European Digital Markets Act: A Revolution Grounded on Traditions. *Journal of European Competition Law & Practice*, *12*(7), 542–560. https://doi.org/10.1093/jeclap/lpab066

Lawton, T., Angwin, D., Dattée, B., Arregle, J. L., & Barbieri, P. (2024). Autonomy as a Strategic Dial: A Dynamic Framework for Managing Acquired Subsidiaries. *California Management Review*, *66*(3), 47–68. https://doi.org/10.1177/00081256241238054

Letina, I., Schmutzler, A., & Seibel, R. (2024). Killer acquisitions and beyond: policy effects on innovation strategies. *International Economic Review*, *65*(2), 591–622. https://doi.org/10.1111/iere.12689

Levy, N., Rimsa, A., & Buzatu, B. (2021). The European Commission's New Merger Referral Policy: A Creative Reform or an Unnecessary End to'Brightline'Jurisdictional Rules? *European Competition & Regulatory Law Review*, *5*, 364–379. https://doi.org/10.21552/core/2021/4/5

Linneman, D. L. (2022). From Sherman to Shut down-Understanding Antitrust Legislation Targeting Big Tech. *Business, Entrepreneurship & Tax Law Review*, *6*, 118.

Manganelli, A., & Nicita, A. (2022). *Regulating Big Techs and Their Economic Power. In Regulating Digital Markets: The European Approach* (pp. 137–165). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-89388-0_6

Marinova, M. (2024). The UK's digital market regulation: the need for a proportionality principle in the CMA's new framework. *Journal of European Competition Law & Practice*, *15*(7), 491–497. https://doi.org/10.1093/jeclap/lpae062

Marty, F., & Warin, T. (2023). Multi-sided platforms and innovation: A competition law perspective. *Competition & Change*, *27*(1), 184–204. https://doi.org/10.1177/10245294221085639

Mateev, M. (2017). Is the M&A announcement effect different across Europe? More evidences from continental Europe and the UK. *Research in International Business and Finance*, *40*, 190–216. https://doi.org/10.1016/j.ribaf.2017.02.001

Mendelsohn, J., & Breide, L. (2024). Considering the direction of innovation in EU merger control. *Journal of Responsible Innovation*, *11*(1). 2425120. https://doi.org/10.1080/23299460.2024.2425120

Nary, P., & Kaul, A. (2023). Private equity as an intermediary in the market for corporate assets. *Academy of Management Review*, *48*(4), 719–748. https://doi.org/10.5465/amr.2020.0168

Nazzini, R. (2006). Article 81 EC between time present and time past: a normative critique of "restriction of competition" in EU law. *Common Market Law Review*, *43*(2), 497–536. https://doi.org/10.54648/COLA2006005

Nobrega, J. H. C., Sigahi, T. F., Rampasso, I. S., Minatogawa, V. L. F., Moraes, G. H. S. M. D., Ávila, L. V., & Anholon, R. (2024). Managing multi-sided platforms in an emerging country: challenges, critical success factors and contrasts with traditional companies. *Journal of Manufacturing Technology Management*, *35*(2), 247–267. https://doi.org/10.1108/jmtm-11-2022-0387

Norris, M. (2024). *Activating Anti-Trust Pinch Points: Microsoft's Activision Merger Conundrum and International Irregularities in Anti-Trust Law*. https://doi.org/10.2139/ssrn.4715559

Odrobina, A. (2023). The internationalisation of platform-based businesses–the case of GAFAM. *Central European Review of Economics & Finance*, *43*(2), 17–36. https://doi.org/10.24136/ceref.2023.007

Parker, G., & Van Alstyne, M. (2024). Platforms: Their Structure, Benefits, and Challenges. In: H. Werthner, et al., *Introduction to Digital Humanism* (pp. 523–542). Springer, Cham. https://doi.org/10.1007/978-3-031-45304-5_33

Parker, G., Petropoulos, G., & Van Alstyne, M. (2021). Platform mergers and antitrust. *Industrial and Corporate Change*, *30*(5), 1307–1336. https://doi.org/10.1093/icc/dtab048

Petrucci, C. F. (2023). Self-preferencing in the EU: a legal and policy analysis of the Google Shopping case and the Digital Markets Act. *Competition Law Journal*, *22*(1), 18–29. https://doi.org/10.4337/clj.2023.01.03

Pošćić, A. (2024). The Digital Markets Act: Ensuring More Contestability and Openness in the European Digital Market. *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations*, *11*(1), 269–288. https://doi.org/10.22598/iele.2024.11.1.12

Prado, T. S. (2022). Safeguarding Competition in Digital Markets: A Comparative Analysis of Emerging Policy and Regulatory Regimes. *Quello Center Working Paper*, 05. https://doi.org/10.2139/ssrn.4137588

Reddy, K. S. (2016). Regulatory framework of mergers and acquisitions: A review of Indian statutory compliances and policy recommendations. *International Journal of Law and Management*, *58*(2), 197–215. https://doi.org/10.1108/IJLMA-03-2015-0013

Redkina, A., Molodchik, M., & Jardon, C. (2023). Russian merger control: in favor of foreign companies? *International Journal of Emerging Markets*, *18*(10), 3802–3823. https://doi.org/10.1108/IJOEM-01-2021-0109

Rikap, C., Lundvall, B. Å., Rikap, C., & Lundvall, B. Å. (2021). Alternative Futures and What is to Be Done. In *The Digital Innovation Race: Conceptualizing the Emerging New World Order*, 165–187. https://doi.org/10.1007/978-3-030-89443-6_8

Robertson, V. H. (2024). Digital merger control: adapting theories of harm. *European Competition Journal*, *20*(2), 437–459. https://doi.org/10.1080/17441056.2024.2307163

Saouma, R. E., Shelef, O., Wuebker, R., & McGahan, A. M. (2023). Incumbent Incentives In Response To Entry. *Rotman School of Management Working Paper*, *4122634*. http://dx.doi.org/10.2139/ssrn.4122634

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. *International Journal of Information Management*, *60*, 102331. https://doi.org/10.1016/j.ijinfomgt.2021.102331

Shastitko, A., Markova, O. A., & Morozov, A. N. (2022). Deceptive evidence: The experience of product market definition for the purpose of competition law enforcement. *Russian Journal of Economics*, *8*(3), 255–275. https://doi.org/10.32609/j.ruje.8.82144

Soni, M., & Kumar, R. (2024). Competition in Digital Markets in India and the Proposed Ex-Ante Regulatory Framework: A Legal Analysis of the Draft Competition Bill, 2024. *Cahiers Magellanes-NS*, *6*(2), 4887–4900. https://magellanes.com/index.php/CMN/article/view/776

Staab, P. (2024). Financial capitalism online. In *Markets and power in digital capitalism* (pp. 31–64). Manchester University Press. https://doi.org/10.7765/9781526172174.00008

Stephan, A. (2020). *The EU method of antitrust enforcement.* In *Research Handbook on Methods and Models of Competition Law* (pp. 391–413). Edward Elgar Publishing. https://doi.org/10.4337/9781785368653.00028

Tan, G., & Zhou, J. (2021). The effects of competition and entry in multi-sided markets. *The Review of Economic Studies*, *88*(2), 1002–1030. https://doi.org/10.1093/restud/rdaa036

Tsyganov, A., Davydova, L., & Dokukina, A. (2023). Merger control in Russia: Review and perspectives. *Research Handbook on Global Merger Control*, 537–562. https://doi.org/10.4337/9781800378193.00035

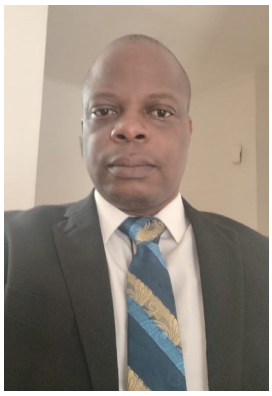
Tzanaki, A. (2023). *Dynamism and Politics in EU Merger Control: Appreciating the Gain and the Gap*. http://dx.doi.org/10.2139/ssrn.4574948

Xie, Y., & Wu, D. (2024). How does competition policy affect enterprise digitization? Dual perspectives of digital commitment and digital innovation. *Journal of Business Research*, *178*, 114651. https://doi.org/10.1016/j.jbusres.2024.114651

Xu, H., & Deng, S. (2024). Digital Mergers and Acquisitions and Enterprise Innovation Quality: Analysis Based on Research and Development Investment and Overseas Subsidiaries. *Sustainability*, *16*(3), 1120. https://doi.org/10.3390/su16031120

Ziermann, F. (2023). Assessing the World's Largest Gaming Acquisition under EU Competition Law. *Journal of European Competition Law & Practice*, *14*(4), 203–219. https://doi.org/10.1093/jeclap/lpad019

Author information



Kolawole Afuwape – Lecturer, Jindal Global Law School, O.P. Jindal Global University
Address: Sonipat Narela Road, Near Jagdishpur Village, Sonipat, Haryana 131001, India
E-mail: afuwapekolawole@gmail.com
ORCID ID: https://orcid.org/0009-0001-5686-230X
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

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 26, 2024
Date of approval – January 14, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:34.096:004.8
EDN: https://elibrary.ru/nzbqnm
DOI: https://doi.org/10.21202/jdtl.2025.13

Правовые барьеры цифровых слияний и поглощений: антимонопольное регулирование технологического сектора

Колаволе Афувапе

Глобальный университет им. О. П. Джиндала, Сонипат, Индия

Ключевые слова

антимонопольное законодательство,
доминирующее положение,
законодательство,
конкуренция,
право,
слияние и поглощение,
технологический гигант,
технологический сектор,
цифровая экономика,
цифровые технологии

Аннотация

Цель: определить характер и степень влияния антимонопольного законодательства Европейского союза и Соединенных Штатов Америки на процессы слияний и поглощений в технологическом секторе.

Методы: в работе использован сравнительный и междисциплинарный подход, сочетающий правовой анализ и экономическое моделирование. Проведен сравнительный анализ законодательства Европейского союза и Соединенных Штатов Америки, обобщение практик антимонопольного регулирования, рассмотрены доктринальные источники и современные эмпирические данные. Использованы методы контент-анализа нормативных актов, кейс-стади крупнейших цифровых компаний, а также элементы прогнозирования влияния регуляторных изменений на инновационную активность и динамику рынка.

Результаты: рассмотрены различные подходы к регулированию слияний и поглощений в цифровой экономике, проанализированы особенности правоприменения в Европейском союзе и Соединенных Штатах Америки. Обосновано, что строгие антимонопольные меры могут как сдерживать рыночную концентрацию, так и создавать барьеры для внедрения инноваций. Установлено, что практика применения Закона о цифровых рынках в Европейском союзе и соответствующих актов Соединенных Штатов Америки существенно влияет на структурные изменения в технологическом секторе, формируя новые модели конкурентной борьбы. Приведены рекомендации по совершенствованию международного сотрудничества и выработке единых справедливых регуляторных стандартов для цифровых рынков. Особое внимание уделяется проблемам определения доминирующего положения, регулятивного контроля и специфическим особенностям цифровых рынков.

Научная новизна: статья системно сопоставляет регулятивные режимы ведущих мировых юрисдикций сквозь призму цифровых слияний и поглощений, расширяя категориальный аппарат за счет современных подходов к анализу сетевых эффектов, конкуренции за данные и новых форм рыночной власти. Применен авторский критерий анализа комплексной экспертизы сделок с точки зрения устойчивости и инновационного потенциала.

Практическая значимость: выводы и рекомендации работы способствуют формированию более гибкой и адаптивной политики регулирования в отношении технологических гигантов, что важно для законотворцев, регуляторов, корпоративных стратегов и исследователей цифровой экономики.

Для цитирования

Афувапе, К. (2025). Правовые барьеры цифровых слияний и поглощений: антимонопольное регулирование технологического сектора. *Journal of Digital Technologies and Law*, *3*(2), 304–337. https://doi.org/10.21202/jdtl.2025.13

Список литературы

Abbott, A. F., & Spulber, D. F. (2024). Antitrust Merger Policy and Innovation Competition. *Journal of Business & Technology Law*, *19*(2), 2.

Afuwape, K. (2024). Analysing the Ex-ante Regulations in India's Digital Competition Bill and Its Effects on Indian Business Interests. *World Competition*, *47*(4), 521–556. https://doi.org/10.54648/woco2024030

Albert, J. R. G. (2020). *Towards measuring the platform economy: Concepts, indicators, and issues* (No. 2020-28). PIDS Discussion Paper Series.

Alexiadis, P. (2024). The UK's Digital Markets, Competition and Consumers Act Passes into Law. *Business Law International*, *25*(3), 271–201.

Almeida, F. (2023). Foresights for big data across industries. *Foresight*, *25*(3), 334–348.

Bergqvist, C. (2024). *The EU's Investigation Into Microsoft Teams: A Preliminary Assessment*. https://doi.org/10.2139/ssrn.4888247

Bostoen, F., & Vanwamel, D. (2024). The Digital Markets Act: A partial solution to antitrust's remedy problem. *Common Market Law Review*, *61*(6). https://doi.org/10.54648/cola2024103

Bougette, P., Budzinski, O., & Marty, F. (2024). *Ex-ante versus Ex-post in Competition Law Enforcement: Blurred Boundaries and Economic Rationale* (No. 2024-18). Groupe de REcherche en Droit, Economie, Gestion (GREDEG CNRS), Université Côte d'Azur, France.

Carril-Caccia, F., & Pavlova, E. (2020). Mergers and acquisitions & trade: A global value chain analysis. *The World Economy*, *43*(3), 586–614. https://doi.org/10.1111/twec.12882

Casey, A. J., & Niblett, A. (2021). Micro-Detectives and Computational Merger Review. *Stan. Computational Antitrust*, *1*, 132. https://doi.org/10.51868/8

Chaoxian, G., & Wei, H. (2024). Industrial Organization in the Digital Economy Era: Evolution and Effects. *China Economist*, *19*(4), 15–36. https://doi.org/10.19602/j.chinaeconomist.2024.07.02

Chatterjee, S., Chaudhuri, R., Kamble, S., Gupta, S., & Sivarajah, U. (2023). Adoption of artificial intelligence and cutting-edge technologies for production system sustainability: a moderator-mediation analysis. *Information Systems Frontiers*, *25*(5), 1779–1794. EDN: https://www.elibrary.ru/ckwblq. DOI: https://doi.org/10.1007/s10796-022-10317-x

Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration*, *44*(1), 41–57. EDN: https://www.elibrary.ru/jzoonr. DOI: https://doi.org/10.1080/07036337.2021.2011260

Čirjevskis, A. (2019). The Role of Dynamic Capabilities as Drivers of Business Model Innovation in Mergers and Acquisitions of Technology-Advanced Firms. *Journal of Open Innovation: Technology, Market, and Complexity*, *5*(1), 12. https://doi.org/10.3390/joitmc5010012

Coveri, A., Cozza, C., & Guarascio, D. (2024). Blurring boundaries: an analysis of the digital platforms-military nexus. *Review of Political Economy*, 1–32. https://doi.org/10.1080/09538259.2024.2395832

Crandall, R. W. (2024). Towards a More Vigorous Antitrust Policy? *Review of Industrial Organization*, 1–16. EDN: https://www.elibrary.ru/lojjqs. DOI: https://doi.org/10.1007/s11151-024-09981-x

de Carvalho, S. (2024). The Roots of Antitrust Policy in the United States' Sherman Act. *International Investment Law Journal*, *4*(1), 92–110.

Eben, M., & Reader, D. (2023). Taking aim at innovation-crushing mergers: a killer instinct unleashed?. *Yearbook of European Law*, *42*, 286–321. EDN: https://www.elibrary.ru/xqgywz. DOI: https://doi.org/10.1093/yel/yead013

Enriques, L., & Gatti, M. (2015). Creeping acquisitions in Europe: enabling companies to be better safe than sorry. *Journal of Corporate Law Studies*, *15*(1), 55–101.

Eroğlu, M., & Koksal, A. (2024). Ex-Post Application of Structural Remedies to Large Online Platforms at a National Level. *İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi*, *9*(1), 135–169. EDN: https://www.elibrary.ru/uwsezt. DOI: https://doi.org/10.58733/imhfd.1451588

Ganguli, P. (2024). *International Perspectives on Antitrust Laws: A Comparative Study of India, the US, and the EU*. http://dx.doi.org/10.2139/ssrn.5006751

Gilbert, R. J., & Melamed, A. D. (2024). Potential Competition and the 2023 Merger Guidelines. *Review of Industrial Organization*, *65*, 269–302. EDN: https://www.elibrary.ru/ladalu. DOI: https://doi.org/10.1007/s11151-024-09964-y

Glick, M., Lozada, G. A., Govindan, P., & Bush, D. (2023). The Horizontal Merger Efficiency Fallacy. *Temple Law Review*, *96*, 571. https://doi.org/10.36687/inetwp212

Goldsmith, J. (2017). A comparative user evaluation of tablets and tools for consecutive interpreters. *Proceedings of Translating and the Computer*, *39*, 40–50.

Gorecka, A. (2024). *The interface between competition law and data privacy law: violation of privacy as an exploitative theory of harm under Article 102 TFEU*. Switzerland: Springer International. https://doi.org/10.1007/978-3-031-73865-4

Graef, I. (2024). Regulating Digital Platforms: Streamlining the Interaction between the Digital Markets Act and National Competition Regimes. In *The Legal Consistency of Technology Regulation in Europe* (pp. 157–176). Hart Publishing. https://doi.org/10.5040/9781509968053.ch-008

Gupta, M., Gupta, D., & Rai, P. (2024). Exploring the Impact of Software as a Service (SaaS) on Human Life. *EAI Endorsed Transactions on Internet of Things*, *10*. EDN: https://www.elibrary.ru/kasfjk. DOI: https://doi.org/10.4108/eetiot.4821

Henten, A., & Windekilde, I. (2022). Demand-Side Economies of Scope in Big Tech Business Modelling and Strategy. *Systems*, *10*(6), 246. EDN: https://www.elibrary.ru/epxsim. DOI: https://doi.org/10.3390/systems10060246

Highfield, J. (2024). Is Big Necessarily Bad? An Examination of the Revolutionary DMA and DMCC Designation Criteria. *North East Law Review*, *10*, 75–86.

Hiwarale, M. M. G., Irene, M., Jaiswal, D., & Tyagi, A. (2024). Competition Comission Of India: Safeguarding Fair Play In Mergers And Acqusitions In India. *Library Progress International*, *44*(3), 9966–9977.

Ioramashvili, C., Feldman, M., Guy, F., & Iammarino, S. (2024). Gathering round Big Tech: How the market for acquisitions concentrates the digital sector. *Cambridge Journal of Regions, Economy and Society*, *17*(2), 293–306. https://doi.org/10.1093/cjres/rsae003

Ivaldi, M., Petit, N., & Unekbas, S. (2023). Killer acquisitions: Evidence from EC merger cases in digital industries. *Antitrust Law Journal – TSE Working Paper*, 13-1420. https://doi.org/10.2139/ssrn.4407333

Jin, G. Z., Leccese, M., & Wagman, L. (2023). How do top acquirers compare in technology mergers? New evidence from an SP taxonomy. *International Journal of Industrial Organization*, *89*, 102891. EDN: https://www.elibrary.ru/klfczd. DOI: https://doi.org/10.1016/j.ijindorg.2022.102891

Khan, L. M. (2019). The Separation of Platforms and Commerce. *Columbia Law Review*, *119*(4), 973–1098.

Khandelwal, R., Nayak, A., Chung, P., Fawaz, K., Bianchi, A., Celik, Z. B., ... & Hussain, S. R. (2024). Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 2831–2848). Philadelphia PA USA.

Khokhlov, E. (2017). The Russian Federal Antimonopoly Service's Case Against Google Related to Bundling and other Anticompetitive Practices with Respect to Android. *Journal of European Competition Law & Practice*, *8*(7), 468–474. EDN: https://www.elibrary.ru/dgikfh. DOI: https://doi.org/10.1093/jeclap/lpx036

King, D. R., Schriber, S., Bauer, F., & Amiri, S. (2018). Acquisitions as corporate entrepreneurship. In *Advances in mergers and acquisitions* (pp. 119–144). Emerald Publishing Limited. https://doi.org/10.1108/S1479-361X20180000017006

Kira, B. (2024). Inter-Agency Coordination and Digital Platform Regulation: Lessons from the WhatsApp Case in Brazil. *International Review of Law, Computers & Technology*, *39*(1), 6–29. https://doi.org/10.1080/13600869.2024.2351671

Kızılay, A. S. (2024). Lack of Effective Control on Killer Acquisitions in the Big Tech Market under EU Framework: Rethinking of EUMR Rules?. *Public and Private International Law Bulletin*, *44*(1), 253–280. https://doi.org/10.26650/ppil.2023.44.1.110941

Koch, T., & Windsperger, J. (2017). Seeing through the network: Competitive advantage in the digital economy. *Journal of Organization Design*, *6*, 1–30. EDN: https://www.elibrary.ru/ofwkdb. DOI: https://doi.org/10.1186/s41469-017-0016-z

Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, *43*(3), 405–424. EDN: https://www.elibrary.ru/uiuhrx. DOI: https://doi.org/10.1002/smj.3250

Krzykowski, M. (2024). Article 22 of the EC Merger Regulation–national and European control: energy sector. In *Research Handbook on EU Competition Law and the Energy Transition* (pp. 278–297). Edward Elgar Publishing. https://doi.org/10.4337/9781803922591.00021

Kuenzler, A. (2022). What competition law can do for data privacy (and vice versa). *Computer Law & Security Review*, *47*, 105757. EDN: https://www.elibrary.ru/iwzxrh. DOI: https://doi.org/10.1016/j.clsr.2022.105757

Kyle, M., Shah, O., & Mani, V. (2024). Hot tub time machine? What role for Towercast in EU merger control. *Journal of European Competition Law & Practice*, *15*(6), 436–443. EDN: https://www.elibrary.ru/pjruru. DOI: https://doi.org/10.1093/jeclap/lpae057

Lancieri, F., & Pereira Neto, C. M. S. (2022). Designing remedies for digital markets: The interplay between antitrust and regulation. *Journal of Competition Law & Economics*, *18*(3), 613–669. EDN: https://www.elibrary.ru/umsrli. DOI: https://doi.org/10.1093/joclec/nhab022

Larouche, P., de Streel, A. (2021). The European Digital Markets Act: A Revolution Grounded on Traditions. *Journal of European Competition Law & Practice*, *12*(7), 542–560. EDN: https://www.elibrary.ru/smrdtl. DOI: https://doi.org/10.1093/jeclap/lpab066

Lawton, T., Angwin, D., Dattée, B., Arregle, J. L., & Barbieri, P. (2024). Autonomy as a Strategic Dial: A Dynamic Framework for Managing Acquired Subsidiaries. *California Management Review*, *66*(3), 47–68. https://doi.org/10.1177/00081256241238054

Letina, I., Schmutzler, A., & Seibel, R. (2024). Killer acquisitions and beyond: policy effects on innovation strategies. *International Economic Review*, *65*(2), 591–622. EDN: https://www.elibrary.ru/szdhiw. DOI: https://doi.org/10.1111/iere.12689

Levy, N., Rimsa, A., & Buzatu, B. (2021). The European Commission's New Merger Referral Policy: A Creative Reform or an Unnecessary End to'Brightline'Jurisdictional Rules? *European Competition & Regulatory Law Review*, *5*, 364–379. EDN: https://www.elibrary.ru/jebcil. DOI: https://doi.org/10.21552/core/2021/4/5

Linneman, D. L. (2022). From Sherman to Shut down-Understanding Antitrust Legislation Targeting Big Tech. *Business, Entrepreneurship & Tax Law Review*, *6*, 118.

Manganelli, A., & Nicita, A. (2022). *Regulating Big Techs and Their Economic Power. In Regulating Digital Markets: The European Approach* (pp. 137–165). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-89388-0_6

Marinova, M. (2024). The UK's digital market regulation: the need for a proportionality principle in the CMA's new framework. *Journal of European Competition Law & Practice*, *15*(7), 491–497. EDN: https://www.elibrary.ru/vxktso. DOI: https://doi.org/10.1093/jeclap/lpae062

Marty, F., & Warin, T. (2023). Multi-sided platforms and innovation: A competition law perspective. *Competition & Change*, *27*(1), 184–204. EDN: https://www.elibrary.ru/scnhcl. DOI: https://doi.org/10.1177/10245294221085639

Mateev, M. (2017). Is the M&A announcement effect different across Europe? More evidences from continental Europe and the UK. *Research in International Business and Finance*, *40*, 190–216. https://doi.org/10.1016/j.ribaf.2017.02.001

Mendelsohn, J., & Breide, L. (2024). Considering the direction of innovation in EU merger control. *Journal of Responsible Innovation*, *11*(1). 2425120. https://doi.org/10.1080/23299460.2024.2425120

Nary, P., & Kaul, A. (2023). Private equity as an intermediary in the market for corporate assets. *Academy of Management Review*, *48*(4), 719–748. EDN: https://www.elibrary.ru/wirznm. DOI: https://doi.org/10.5465/amr.2020.0168

Nazzini, R. (2006). Article 81 EC between time present and time past: a normative critique of "restriction of competition" in EU law. *Common Market Law Review*, *43*(2), 497–536. https://doi.org/10.54648/COLA2006005

Nobrega, J. H. C., Sigahi, T. F., Rampasso, I. S., Minatogawa, V. L. F., Moraes, G. H. S. M. D., Ávila, L. V., & Anholon, R. (2024). Managing multi-sided platforms in an emerging country: challenges, critical success factors and contrasts with traditional companies. *Journal of Manufacturing Technology Management*, *35*(2), 247–267. EDN: https://www.elibrary.ru/aydrvo. DOI: https://doi.org/10.1108/jmtm-11-2022-0387

Norris, M. (2024). *Activating Anti-Trust Pinch Points: Microsoft's Activision Merger Conundrum and International Irregularities in Anti-Trust Law*. https://doi.org/10.2139/ssrn.4715559

Odrobina, A. (2023). The internationalisation of platform-based businesses–the case of GAFAM. *Central European Review of Economics & Finance*, *43*(2), 17–36. EDN: https://www.elibrary.ru/gjsrss. DOI: https://doi.org/10.24136/ceref.2023.007

Parker, G., & Van Alstyne, M. (2024). Platforms: Their Structure, Benefits, and Challenges. In: H. Werthner, et al., *Introduction to Digital Humanism* (pp. 523–542). Springer, Cham. https://doi.org/10.1007/978-3-031-45304-5_33

Parker, G., Petropoulos, G., & Van Alstyne, M. (2021). Platform mergers and antitrust. *Industrial and Corporate Change*, *30*(5), 1307–1336. https://doi.org/10.1093/icc/dtab048

Petrucci, C. F. (2023). Self-preferencing in the EU: a legal and policy analysis of the Google Shopping case and the Digital Markets Act. *Competition Law Journal*, *22*(1), 18–29. EDN: https://www.elibrary.ru/nhsmas. DOI: https://doi.org/10.4337/clj.2023.01.03

Pošćić, A. (2024). The Digital Markets Act: Ensuring More Contestability and Openness in the European Digital Market. *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations*, *11*(1), 269–288. https://doi.org/10.22598/iele.2024.11.1.12

Prado, T. S. (2022). Safeguarding Competition in Digital Markets: A Comparative Analysis of Emerging Policy and Regulatory Regimes. *Quello Center Working Paper*, 05. EDN: https://www.elibrary.ru/uovkiu. DOI: https://doi.org/10.2139/ssrn.4137588

Reddy, K. S. (2016). Regulatory framework of mergers and acquisitions: A review of Indian statutory compliances and policy recommendations. *International Journal of Law and Management*, *58*(2), 197–215. https://doi.org/10.1108/IJLMA-03-2015-0013

Redkina, A., Molodchik, M., & Jardon, C. (2023). Russian merger control: in favor of foreign companies? *International Journal of Emerging Markets*, *18*(10), 3802–3823. EDN: https://www.elibrary.ru/jfcgzd. DOI: https://doi.org/10.1108/IJOEM-01-2021-0109

Rikap, C., Lundvall, B. Å., Rikap, C., & Lundvall, B. Å. (2021). Alternative Futures and What is to Be Done. In *The Digital Innovation Race: Conceptualizing the Emerging New World Order*, 165–187. https://doi.org/10.1007/978-3-030-89443-6_8

Robertson, V. H. (2024). Digital merger control: adapting theories of harm. *European Competition Journal*, *20*(2), 437–459. https://doi.org/10.1080/17441056.2024.2307163

Saouma, R. E., Shelef, O., Wuebker, R., & McGahan, A. M. (2023). Incumbent Incentives In Response To Entry. *Rotman School of Management Working Paper*, *4122634*. http://dx.doi.org/10.2139/ssrn.4122634

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. *International Journal of Information Management*, *60*, 102331. EDN: https://www.elibrary.ru/lgmvsr. DOI: https://doi.org/10.1016/j.ijinfomgt.2021.102331

Shastitko, A., Markova, O. A., & Morozov, A. N. (2022). Deceptive evidence: The experience of product market definition for the purpose of competition law enforcement. *Russian Journal of Economics*, *8*(3), 255–275. EDN: https://www.elibrary.ru/lzymup. DOI: https://doi.org/10.32609/j.ruje.8.82144

Soni, M., & Kumar, R. (2024). Competition in Digital Markets in India and the Proposed Ex-Ante Regulatory Framework: A Legal Analysis of the Draft Competition Bill, 2024. *Cahiers Magellanes-NS*, *6*(2), 4887–4900. https://magellanes.com/index.php/CMN/article/view/776

Staab, P. (2024). Financial capitalism online. In *Markets and power in digital capitalism* (pp. 31–64). Manchester University Press. https://doi.org/10.7765/9781526172174.00008

Stephan, A. (2020). *The EU method of antitrust enforcement.* In *Research Handbook on Methods and Models of Competition Law* (pp. 391–413). Edward Elgar Publishing. https://doi.org/10.4337/9781785368653.00028

Tan, G., & Zhou, J. (2021). The effects of competition and entry in multi-sided markets. *The Review of Economic Studies*, *88*(2), 1002–1030. EDN: https://www.elibrary.ru/ruvvjf. DOI: https://doi.org/10.1093/restud/rdaa036

Tsyganov, A., Davydova, L., & Dokukina, A. (2023). Merger control in Russia: Review and perspectives. *Research Handbook on Global Merger Control*, 537–562. https://doi.org/10.4337/9781800378193.00035

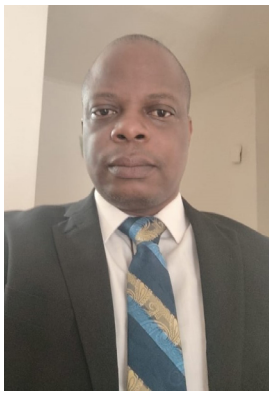
Tzanaki, A. (2023). *Dynamism and Politics in EU Merger Control: Appreciating the Gain and the Gap*. http://dx.doi.org/10.2139/ssrn.4574948

Xie, Y., & Wu, D. (2024). How does competition policy affect enterprise digitization? Dual perspectives of digital commitment and digital innovation. *Journal of Business Research*, *178*, 114651. EDN: https://www.elibrary.ru/mgtgdj. DOI: https://doi.org/10.1016/j.jbusres.2024.114651

Xu, H., & Deng, S. (2024). Digital Mergers and Acquisitions and Enterprise Innovation Quality: Analysis Based on Research and Development Investment and Overseas Subsidiaries. *Sustainability*, *16*(3), 1120. EDN: https://www.elibrary.ru/otwggn. DOI: https://doi.org/10.3390/su16031120

Ziermann, F. (2023). Assessing the World's Largest Gaming Acquisition under EU Competition Law. *Journal of European Competition Law & Practice*, *14*(4), 203–219. EDN: https://www.elibrary.ru/yotqhd. DOI: https://doi.org/10.1093/jeclap/lpad019

Сведения об авторе



Афувапе Колаволе – преподаватель, Школа права, Глобальный университет им. О. П. Джиндала
Адрес: Индия, 131001, Харьяна, г. Сонипат, район Джагдишпур, улица Сонипат Нарела
E-mail: afuwapekolawole@gmail.com
ORCID ID: https://orcid.org/0009-0001-5686-230X
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

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 – 26 декабря 2024 г.
Дата одобрения после рецензирования – 14 января 2025 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.

Research article
UDC 34:004:347:004.4
EDN: https://elibrary.ru/ujsqxf
DOI: https://doi.org/10.21202/jdtl.2025.14

Impact of the COVID-19 Pandemic on the Transformation of Judicial System in Nigeria: from Traditional to Digital Justice

Michael Chukwujindu Ogwezzy
Rivers State University, Port Harcourt, Nigeria

Keywords

access to justice,
court,
COVID-19 pandemic,
digital technologies,
digital transformation,
electronic justice,
judicial system,
law,
legislation,
virtual hearings

Abstract

Objective: to identify the key technological solutions implemented in the country's judicial system under quarantine restrictions and to assess their long-term impact on the administration of justice.

Methods: the study uses an integrated approach that includes an analysis of legal acts regulating the digitalization of the legal sphere in Nigeria. The work provides a comparative study of practical guidelines from federal and state courts for conducting virtual hearings, and a systematization of data on the introduction of electronic case management and trial management systems. The author uses a doctrinal method of analyzing court decisions and the practice of using digital technologies in various jurisdictions of the country.

Results: the author showed that the COVID-19 pandemic became a catalyst for the accelerated transition of the Nigerian legal system from traditional paper-based document management to digital platforms. The main technological solutions are identified: online case management systems, virtual courtrooms, electronic filing systems, and digital legal research tools. The article lists advantages of digitalization, including increased productivity, ensuring security when reviewing cases, as well as disadvantages associated with depersonalization of document management, threats to confidentiality and the potential loss of jobs.

Scientific novelty: the work presents a comprehensive analysis of the transformation of legal practice in Nigeria under the influence of the COVID-19 pandemic with a focus on the impact of digitalization on access to justice. The study contributes to understanding the peculiarities of adaptation of legal systems in developing countries to extraordinary

circumstances through the prism of technological innovations. The author developed the concept of the relationship between the judicial system's digital transformation and ensuring the constitutional right to a fair trial under the social distancing.

Practical significance: the study results can be used to improve the legal framework for the legal sphere digitalization in Nigeria and other developing countries. The conclusions are important for shaping policy in the field of modernizing judicial systems, developing ethical standards for virtual legal proceedings and creating effective mechanisms for ensuring access to justice in the digital age. Practical recommendations can be applied by judicial authorities to optimize the processes of administration of justice and to improve the quality of legal services.

For citation

Ogwezzy, M. Ch. (2025). Impact of the COVID-19 Pandemic on the Transformation of Judicial System in Nigeria: from Traditional to Digital Justice. *Journal of Digital Technologies and Law, 3*(2), 338–362. https://doi.org/10.21202/jdtl.2025.14

Contents

Introduction

The justice sector experienced a great revolution in the use of digital tools in dispensing justice by judges and legal practitioners who are plying their trade to earn a living. The emergence of the Covid 19 disease has plunged the entire world into a catastrophe of monumental proportion. Every aspect of human endeavour has been adversely affected by the pandemic. Economic, political, religious and social activities have been disrupted. However, many of the key players in these sectors have risen up to the challenges with pragmatic measures. The pandemic forced many professionals to consider digital options for service delivery including those practicing the practicing legal profession, lawyers, barristers and solicitors.

The legal system worldwide has become dependent on information technology, which has necessitated the transformation from the traditional usage of paper to the electronic recording and registration filing of legal documents and records. This development is not limited to other fields but extends to legal practice. In the current legal practice trend, many rely extensively upon digitization for information about cases, and the law is promptly accessible from estimators (Ufua et al., 2020). However, despite all that is happening digitally in current legal practice, Nigeria is still clinging to the ancient mode of justice administration by leaving out several aspects of digitalized practices.

The advent of the COVID-19 pandemic has necessitated the fast-tracking of the digitalization of legal practice globally. This is to enable the continuous provision of legal services via virtual and remote contact with clients and judicial officers. This paper examines the new approaches and technologies in legal practice as a result of the pandemic in Nigeria, defined by hybrid virtual court sittings, web-based communication applications, practice directions, and protocols for remote hearings. Virtual hearings, remote online witness conferencing and electronic and online filing of court processes are being deployed to replace physical courtroom hearings (Aidonojie, 2021).

This paper discusses the legal provisions, regulations, and guidelines at national and state levels on court-annexed and mediation schemes, legal aid providers and in-absentia hearings. The consequences of digitalization for legal practice and access to justice, such as overcrowded and unreliable internet connectivity in many parts of the nation, lack of computers, smartphones, modems, and cameras in legal aid offices and courts, the threat to privacy and cybersecurity due to lack of clear rules, potential hacking, and denial of service attacks, the heavy reliance on just one or two

international video-conferencing applications, data theft and manipulation, abuse and addiction to social media, etc., are also identified. The paper likewise underlines the importance of training and retraining of counsel, support staff and judicial officers in using new tools and provision of infrastructure facilities to facilitate the continuous digitalization of legal practice. The paper concludes by making suggestions on how digital legal practice in Nigeria can be optimized to guarantee the promotion of the rule of law and efficient delivery of the justice system.

During the pandemic, the courts in Nigeria had to embrace digital devices to promote the business of the courts and ensure access to justice by all those that needed and can afford it. The judicial sector and practicing lawyers adopted different digital tools in the administration of justice. This development could represent a turning point for the justice delivery and the judicial sector in Nigeria.

Nigeria, like other nations of the world, has embarked on efforts to contain the further spread of the Covid-19 pandemic by adopting policies and regulations targeted at social distancing and work from home, which involves digitalization of legal practice. Against this backdrop, a need arises to examine how the digitalization of legal practice and other contemporaneous legal aid services affect access to justice in Nigeria. Considering the complexity of the issues highlighted, this paper aims to establish the impact of the digitalization of legal practice on the judiciary in Nigeria.

1. Legal Framework for Digitalisation in Nigeria

At the bedrock of digitisation is the Nigerian Constitution 1999 which guarantees the right to privacy by providing in its section 37 that «the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected"[1]. This means that in all the digitization process, the privacy of persons involved or that may be affected must be considered at all times in order not to violate their fundamental human rights.

Also, the National Information Technology Development Agency Act 2007 (NITDA Act) establishes the National Information Technology Development Agency (NITDA which is an agency responsible for regulating all information technology matters in Nigeria. The NITDA is the main regulating body in Nigeria for online services that let users transmit text, photo, or video messages to one another via the internet. It is the organization in charge of overseeing internet platforms that permit both professionally and amateurly generated material to be created and shared. The NITDA Act gives NITDA the authority to create rules and guidelines for the advancement, supervision, assessment,

1 TNigeria Constitution 1999. https://clck.ru/3MBoND

and control of information technology practices, activities and systems in Nigeria, as well as any issues pertaining to or serving that objective[2]. NITDA is also empowered to develop guidelines for electronic governance and to monitor the use of electronic data interchange and other forms of electronic communication transactions[3]. NITDA also provides support for the development of local content and the growth of the ICT industry in Nigeria.

In furtherance of its mandate, in 2019, the NITDA issued the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019 with the objectives to protect the rights of natural persons to data privacy, to foster safe conduct for transactions involving the exchange of personal data and to prevent manipulation of personal data[4]. The NDPR governs all transactions involving the intended processing of personal data, regardless of the method used to process the data in relation to natural persons in Nigeria. It also applies to natural persons who live in Nigeria or to Nigerian citizens who live abroad. Nonetheless, no Nigerian or natural person is prevented from exercising their right to privacy under the NDPR from any law, rule, policy, or contract that is now in effect in Nigeria or in any other country. The NDPR sets out the rights of individuals with respect to their personal data and the obligations of organisations processing such data and it provides for the establishment of a Data Protection Commission to oversee compliance with the regulation. Also, the Cybercrimes (Prohibition, Prevention etc) Act was enacted in 2015 to tackle the menace of cybercrimes which are crimes carried out primarily by means of a computer on the internet.

As regards the legal practitioner and digitalization, the Legal Practitioners Act (LPA) provides that for requirements for the qualifications for the admission into the legal practice in Nigeria. Persons desiring to become legal practitioners in Nigeria are required to obtain a qualifying certificate from an accredited University after which they pass the Bar examinations and be called to the Nigerian Bar. The LPA empowers the Body of Benchers to make regulations or modify the qualifying requirements laid down in the legal profession of any category of legal service. It also establishes the Rules of Professional Conduct for the legal profession (Udemezue, 2022). Rapid digitization of law education and practice, unique as it is, has challenges as it offers opportunities. The ability of the lawyer to grasp the subject matter of his advice and of which he is speaking leaves him with great influence and access to power. By analogy to functional plasticity, the lawyer can pivot to play a radical role regarding changes to the justice system, arguing for a wider range of solutions than have traditionally been enculturated. This is an area that offers the

2 NITDA Act, section 6(a).

3 Ibid, section 6(c).

4 NDPR, paragraph 1.1.

opportunity of a wider role for digitisation in legal work. It is also an area which challenges the education of lawyers and there is room for much more focus on this in law schools (Bello & Ogufere, 2024).

Apart from these key legislations, the National Broadcasting Commission Act and the National Broadcasting Commission Code are relevant for the regulation of online platforms that deliver professionally produced editorial content to consumers in video and picture format.

It is clear from the foregoing that despite the global responses to legislations to incorporate digitisation into all spheres of life brought by the realities of the pandemic, Nigeria still has a lot to do in codifying these legislations and updating them to meet up with the minimum standards that could permit several services, including quality legal services to be delivered without physical presence. Given that not all the laws mentioned above recognise basic aspects of legal practice such as electronic signature, the implication of this for the Nigeria's legal system and other sectors is the limited scope of the legislations. Apart from the limited scope that may arise as a result of electronic signature, these laws were not tailored according to pressing matters inclusive to digital justice administration. The role of the laws in justice administration and legal practice may need further examination and amendment to respond to the society's need, including the possibility of voting in elections, access to justice, acting as a legal practitioner during a virtual hearing (Aidonojie et al., 2021).

This is not to say that Nigeria is entirely a stranger to digitized justice delivery system. Among the various digitization initiatives of the Nigerian justice administration are the Judiciary web portal, Judicial Performance Evaluation System, the E-justice Electronic Case Management System, Nigeria Case Management Software, Nigeria Electronic Filing Portal, and the e-filing. Furthermore, some Federal, State High, and customary Courts in Nigeria also have facilities to support video and teleconferencing for the hearing of matters. The National Industrial Court (NIC) in Nigeria recently piloted the remote/virtual hearing of its matters by its rules and guidelines issued in response to the COVID-19 pandemic (Ibekwe & Onwuatuegwu, 2021). However, there is a need to reinforce the importance of digitisation of the legal profession and practice in these laws.

2. Impact of Covid-19 on the Legal Sector

Like a recurring decimal, the Covid-19 pandemic disrupted societies. There was a disruption of every facet of society. People and organizations had to adjust to a new way of life predicated primarily on fancy technologies. This disruption was not only limited to the general population, but it also included professionals such as lawyers who traditionally have their print of foot obstructed by the law. All over the world, the pandemic ushered in an era of remote legal practice, supplemented by digital justice. Consequently, legal professionals who are notorious for being conservative and reluctant

to embrace digital technologies reluctantly embraced digital technologies to carry out legal practice. Consequently, a multitude of procedures and process were adapted into digital justice processes to accommodate virtual hearings and electronic filings during the pandemic (Karim, 2021).

The pandemic has also had several unintended effects on the Bar and Bench, affecting the furtherance of smooth justice delivery due to the non-implementation of statutory and functional responsibilities, especially the shutdown of the courts and the Bar from the public during the lockdown period (Arinze-Umobi, & Okonkwo, 2021). In the end, the impact of the pandemic has influenced access to justice with particular difficulty for disputant individuals and corporate entities and enforced a trial period for the legal system, in particular on matters that warrant urgent judicial decisions such as petitions for interim injunctions and police actions, long-term criminal and civil matters with inherent problems, among others (Olugasa & Davies, 2022).

With the change in lifestyle all over the world, there was invariable changes and adjustments in the modus operendi in Nigeria's justice sector. The Nigerian judiciary and the legal profession adopted some necessary adjustments to keep up with the times. This is where the deployment of information technology in the administration of justice has become a sine quanone.

In order to minimize the spread of the COVID 19 virus the Chief Justice of Nigeria (CJN), Ibrahim Tanko Muhammad on the 23rd of March, 2020, issued Circular No. NJC/CIR/HOC/11631. The essence of the directive was to initially suspend courts activities for an initial period of two weeks, save for urgent or time-bound cases. Furthermore on 6th April, 2020, His Lordship the CJN gave another directive, this time suspending court sittings sine die. His Lordship, however, noted again that courts were expected to sit particularly in respect of matters that are urgent, essential or time-bound.

In a bid to mitigate the dire consequences of the shutdown of the Courts, on the Nigerian justice system, notable voices in the legal profession made compelling and well-intentioned arguments for the courts to take advantage of the ease and efficiency offered by modern technology in order for the Courts to adopt virtual sittings. Subsequently the judiciaries of some states of the Federation started to issue some practice directions to introduce the practice of virtual hearing into the court proceedings. The Lagos State judiciary was among the initiators of this pragmatic innovation. The Chief Judge of Lagos State signed the "Lagos State Judiciary Remote Hearing of Cases (COVID-19 Pandemic Period) Practice Direction" which came into effect on the 4th of May, 2020. The essence of the Practice Direction is to make sure that hearing and determination of urgent and time-bound cases through digital platforms like Zoom, Skype or any other video and audio conferencing platforms approved by the Court.

Then, the Lagos State judiciary had its first virtual sitting in a criminal matter in line with the Practice Direction. The Borno State judiciary has also recorded its first virtual sitting wherein a Judge delivered a judgment in a criminal matter. The Federal High Court and some other State judiciaries have equally issued similar Practice Directions on virtual court proceedings and this is how the judicial sectors commence virtual court hearing and other forms of legal practice using the digital plat forms were adopted. It is imperative to note that the Nigeria evidence Act of 2011 was amended in 2023 for adopting electronic signature and other forms or processes through which legal documents can by authenticated and sent through a digital platform.

The legal consequences of the pandemic have led to innovative techniques for delivering legal services. The relevance of legal technology has received widespread acknowledgment at a level of importance commensurate with software developers and e-commerce entrepreneurs. Non-adoption or refusal to adopt relevant legal technologies risks dooming the legal profession to extinction. Consequently, there has been a tension of legal technology feeding on itself. Legal tech experts believe that more efficient, skillful, accurate, and affordable productions would be available through the outer limits of technology. Meanwhile, like offsetting colours, other stakeholders are pushing back and resisting such an embrace for reasons such as the value of human intervention, privacy concerns, unauthorized practice of the law, client access to lawyers, bandwidth issues, human touch in the decision-making process, technology cost effectiveness, and the real or perceived flaws in artificial intelligence algorithms (Eboibi & Mac-Barango, 2020).

In many ways, the Nigerian legal profession was in a state of suspended animation regarding its attitude to technology adoption in legal practice, i.e., until the advent of Covid-19, which forced many legal professionals to move work from the office to home. Thereafter, they had to embrace and use technology in their practice in no small measure. Such technologies were those that supported the efficient operation of judicial functions such as the remote appearance of legal counsel at court and the filing of court processes electronically, including enabling the court to entertain and deliver judgments in electronic format.

The pandemic has caused widespread disruption and pushed the legal industry into a massive, unpredicted transformation. The Bar and Bench are combating the effect of the pandemic head-on with the support of several Justice Sector partners by taking apparently quick steps to introduce virtual technology through webinar platforms, online meetings, remote working tools, etc., to ensure the safety and wellbeing of legal practitioners and staff. In Nigeria during the lockdown period, most law firms operate remotely while specific legal matters such as adjournment may be treated through remote video support, where possible. Thus, the legal industry has significantly accelerated its processes of digital transformation (Nwaiwu, 2021).

3. Technological Solutions for Legal Practice

Electronic exchange of judicial assistance documents and a bundle of electronic notices are some examples of digital capacity, in addition to judicial registries, designed to support, secure and enhance the new era of the legal profession, facilitating the conducting of business in a safe, flexible and contemporary digital context. Generally, it is expected that the investment in information technology can provide specific technology measures for procedural and organizational improvement. This section discusses specific interventions for technological advancement in legal practice and judicial activities in Nigeria.

3.1. Online Case Management Systems

In 2020, in response to the negative consequences of the pandemic on the administration of justice, various judges in Nigeria established individual virtual court sessions. For example, the Chief Judge of Lagos, which holds 117 of Nigeria's 255 non-Federal courts, issued guidelines setting out proceedings that could be conducted virtually, such as directions hearings, applications, and meetings in ongoing cases on the 'personally recorded' audio/video platform Zoom. Currently, both the High and Supreme Courts have individual virtual court appearances and some magistrates' and customary courts have held urgent matters via telephone and/or email. The Federal Courts also have ad-hoc or individual virtual hearings with limited provisions for court reporters, and limited security or enforceability of remote court orders where, being testimony, they cannot be cross-examined by opposing counsel (Olugasa & Davies, 2022).

There have been several attempts by private lawyers and public legal institutions in Nigeria to use digital technologies to improve litigation and case management in the courts. These include the launch of public access websites for the High and Supreme Courts, an online information portal for the justice sector produced through a World Bank-funded project entitled the 'Legal Information Management System' (LIMS), and the development of courtroom technology pilot projects, including the digitisation of case tracking, the installation of full audio-visual recording equipment, and electronic filing for bail. For example, Lagos has reported that some of its courts have prioritised urgent matters through virtual proceedings, conducted bail applications via email, and granted virtual marriage licences enabled through video calls (Nwebo, 2023).

3.2. Virtual Courtrooms

As opposed to the traditional court setting which is to have the judge, counsel, parties, witnesses, court officials, and audience in a physical courtroom, virtual courtrooms administers justice and trail processes online means and dispenses with the physical presence of these parties in the same place (Jimoh, 2021). The hearing is conducted through the format of a virtual conference. This is a digital procedure which enables

remote participants to access live online meetings and events from their computers across the globe. A virtual conference is hosted on the internet. Participants have no need to get together in a conference room in order to partake in deliberations at the conference. They can access the meeting through a conference website or video conferencing tools designed specifically for the virtual experience. In addition to the live events, virtual conference includes discussion forums, networking opportunities, a conference resource center, the ability to search for and chat with other conference participants, and other features. All of these are specifically designed to give virtual participants the same opportunity to get the same meeting experience as onsite attendees. The process is made easy by the adoption of witnesses' statements on oath, tendering of documents, presentation of argument and delivery of judgment are done electronically[5]. This method is known for its speedy trial, flexibility, effectiveness and adaptability to emergency situations (Jimoh, 2021).

It is important to note that in alternative dispute resolution cases, a virtual courtroom can simply be utilized in situations where the two disputing parties agree to meet online to settle a matter, as well as involve an impartial third party who will assist in mediating between the disputing parties with the aim of reaching a mutual understanding and/or settlement between them (Walker, 2020). Arbitration is another online dispute resolution mechanism that is utilized as a virtual courtroom. It is utilized when parties approach a neutral arbitrator to give an arbitral award, that is, a decision that is made by an arbitrator upon a disputed issue after considering the evidence provided by both parties. Disputes resolved through arbitration can be enforced in a similar manner to court judgments (Walker, 2020).

A virtual courtroom requires the following for effective virtual hearing:

1. A device you can access an internet connection (PC, MAC, Laptop, Smart Phone, Tablet, etc.);

2. The device must have a video conferencing software already installed.

3. A fast and stable internet connection.

4. A webcam or a built-in camera on your device that will allow the Judge to see you during the virtual hearing and a microphone to enable audio communication with other parties.

5. You must also have a valid email address to send and receive invitation links, meeting ID, password and other relevant details.

A virtual courtroom comprises online alternative dispute resolution services/means, which include mediation and arbitration. Mediation and arbitration are forms of ADR that provide the parties in a dispute with the opportunity to resolve their dispute without resorting to litigation. Furthermore, these mechanisms are effective, less costly, speedier, and confidential. Disputes conducted in these forums are usually resolved within weeks.

[5] Harris Scarfe v. Ernst and Young [2005] SASC 443.

The method selected by the parties to resolve a dispute determines if the method used is arbitration or mediation. If the decision is binding, it is referred to as arbitration, but if it is not binding upon the party, it is referred to as mediation (Arinze-Umobi, & Okonkwo 2021).

Virtual courtroom could be conducted in three major forms – video conferences, teleconference and web conference. A video conference allows participants to hear and see each other during a meeting with a computer video camera and microphone or the built-in camera of a mobile device. There are various kinds of video conference providers in the current market, such as Skype, Zoom, Webex and EzTalks. This type of virtual conference is often used for interviewing job candidates in faraway locations or delivering group online meetings for business. It is also used for meetings with employees who work at home and telecommute, as well as to connect to long-distance clients. Video conference is additionally beneficial in online training, for holding brainstorming sessions or for project-planning sessions.

A teleconference connects meeting participants via phone lines. This can be accomplished through landlines or cellular devices, which allows numerous people to connect simultaneously from multiple locations. The downside of teleconferencing is that there is no visual reference for meeting participants, and people have no access to identify who is speaking and cannot see each other. This format can be more effective if all teleconference participants are introduced beforehand, and if each person identifies himself before commenting.

Web conference is an umbrella term used to describe the process of using the internet and a web browser to connect individuals or groups together from separate geographic areas for educational or training webinars, collaborative online meetings, video conferencing, or live presentations in real time. Web conference allows real-time point-to-point communications as well as multi communications from one sender to many receivers. It offers data streams of text-based messages, voice, and video chat to be shared simultaneously, across geographically dispersed locations.

However, the constitutionality of virtual hearings have been questioned in the light of the right to public trial as required by section 36(4) of the Nigerian Constitution and this right has been upheld in a number of cases where trials were held in Judges' chambers[6]. It in unsure how decisions, especially in criminal cases, made virtually during the lockdown will stand appeal processes should such decisions be appealed to the Supreme Court. Although, the term 'public trial' was not expressly defined in the Constitution, it would suffice as public trail if members of the public have unhindered right of ingress and egress without the requirement of any special consent[7]. Scholars have

6 See the cases of Manakaya v. Manakaya (2001) 43 WRN 138; Oviasu v. Oviasu (1973) 1 ALL NLR 73; Edibo v. The State (2007) 13 NWLR (Pt. 1051) 306; Nuhu v. Ogele (2003) 18 NWLR (Pt. 852) 251.

7 Nigeria-Arab Bank Limited v. Barri Engineering Nig. Ltd (1995) 8 NW LR (Pt. 413) 257.

however argued that even if virtual trials are made open with the link to attend publicly available, it will still fail the test of the requirement of public trial because many Nigerians cannot afford the cost of internet and devices to enable them attend the virtual trials.[8] Apart from being able to afford the means of participating in virtual trials publicly, many Nigerians also lack the technical knowhow around virtual meetings. Should this then suffice as a reason to condemn virtual courtrooms which stands a chance to solve the challenge of slow justice dispensation in Nigeria? It is on this basis that it is pertinent to rule in the context of whether access to participate in virtual trials are made open without restrictions like passwords. Since the court has no business in how persons interested in attending proceedings in physical courtrooms get to the courtrooms, the burden of affordability and technical knowhow of virtual trials should not be placed on the court as well.

3.3. Legal Research

Legal practitioners, law students, researchers and judges' assistants can obtain pertinent statutes, case law, and regulations more quickly and accurately thanks to online databases and artificial intelligence. While sole reliance should not be placed on artificial intelligence, it helps in pointing the researchers in the direction to look in researching for a legal problem. This, in the end, saves a lot of time that would be spent in physical libraries and sourcing for information manually.

4. Merits and Demerits of Digitilisation of the legal practice in Nigeria

The digitilization of the legal practice has been met with mixed reaction with some embracing it and advocating for more digitalisation while others condemn it on the basis that the very nature of legal practice cannot make digitalisation to be an effective tool. It is noteworthy that the digitalisation of legal practice in Nigeria comes with advantages and disadvantages. This section outlines briefly the merits and demerits of digitalisation of legal practice in Nigeria.

4.1. Merits of Digitalisation of Legal Practice

The merits of digitalisation of legal practice includes among others: Increased productivity, enhanced clients service, decision in sensitive cases using zoom application, competitive advantage, improved work-life balance. These merits shall be expatiated hereunder:

---

[8] Benson, H. (2020, 8 May). COVID-19: The Legality of Virtual Court Proceedings in Nigeria. https://clck.ru/3M6CVy

4.1.1. Increased productivity

By streamlining processes using digital tools, legal professionals can complete tasks more efficiently and with fewer resources. Increased efficiency allows lawyers to focus on higher-value tasks, boosting their overall productivity. Also, the cost savings associated with reduced overhead expenses can be passed on to clients or reinvested into the firm to fuel further growth and innovation.

4.1.2. Enhanced client service

Clients will appreciate the cost effect of digitalising too and will come to embrace the cost savings and convenience technology creates. Through digitilisation, lawyers can provide clients easy access to documents, case updates and billing information. And by collecting and analysing data about clients, lawyers can offer customized solutions that meet their unique needs and preferences.

4.1.3. Decision in Sensitive Cases using Zoom application

The decision of courts in sensitive cases like election petitions that are usually accompanied by violence can be delivered virtually to ensure security of persons and properties. By so doing, the risk of large gatherings in and outside the courtrooms erupting in conflicts can be avoided.

4.1.4. Competitive advantage

Legal practitioners that harness the power of technology can offer innovative services, respond more quickly to market changes and differentiate themselves from competitors who are slow to adopt digital solutions. By staying at the forefront of legal tech, your firm will be better positioned to attract and retain clients who value speed, convenience and innovation. In the same way. Judges that embrace digitalisation can clear backlog of cases easily provide faster justice to the public.

4.1.5. Improved work-life balance

Legal professionals can use tools like video conferencing and cloud-based document storage to stay connected with colleagues and clients while working remotely. This offers opportunities to improve work-life balance and as a result, contribute to increased job satisfaction, stress reduction and overall improved well-being for your employees.

4.2. Demerits of Digitalisation of Legal Practice

The demerits of digitalisation of legal services includes: impersonal documents, threats to privacy, job displacement, regulatory challenges.

4.2.1. Impersonal Documents

It may be challenging for lawyers to develop a personal, emotional bond with their clients as a result of generic, impersonal records produced by automated document drafting and filing systems. In the African setting, it is expected that there is a level of involvement in the case that makes the client to be convinced that the lawyer has delivered. Digitalisation will rob the legal practice of this essence.

4.2.2. Threats to Privacy

The centralization of power over personal data exposes sensitive information of persons that seek legal services. There is the risk of losing control of assets when there is no guarantee of adequate safekeeping of information exchanged in the course of legal processes. Even though technology eliminates human mistake, humans are still in charge of ensuring that the data are not compromised. Giving up control to technology exposes legal practitioners and clients to cybercriminals such as hackers, whose destructive abilities are unknown.

4.2.3. Job Displacement

Automation and digitization have the potential to eliminate jobs since they make some tasks outdated or automatable. This may lead to job loss or the requirement that employees retrain for different positions.

4.2.4. Regulatory Challenges

Complex legal and regulatory issues pertaining to cybersecurity, online content, data protection, and intellectual property rights are brought up by digitization. Keeping up with changing legislation may be quite difficult for both individuals and corporations.

5. Access to Justice in Nigeria

Access to Justice means different things to different people. In its narrowest sense, it represents only the formal ability to appear in court. Broadly speaking, it engages the wider social context of our court system, and the systemic barriers faced by different members of the community. Access to Justice is concerned solely with the protection of human rights by ensuring easy and non-discriminatory access to courts of law, the transparency of judicial functionaries and the promotion of a worldwide jurisprudence on human rights. It is important to say that the use of different digital plat formats as explained in this paper allowed people access to justice despite the restrictions and lockdown in peoples' movement during the VOVID 19 Period in Nigeria. See Section 36 of the CFRN 1999 on fair hearing

This article does not aim to provide an extensive analysis of access to justice in Nigeria. Instead, it analyses the challenges and opportunities digitalization practices have represented for access to justice in Nigeria during and after the Covid-19 pandemic. This is known as technology-assisted litigation, which has permitted law firms, corporate legal departments, and courts to operate more effectively during the coronavirus pandemic. The digitalisation of the judicial process, also known as cloud court technology, has allowed the judicial process to continue mostly unimpeded even with courts physically closed and ensures disputes are still resolved within an acceptable timescale. However, reflecting on the merits and demerits of digitalisation of courtrooms and legal practices, it is essential to be mindful of the short-term and long-term challenges and opportunities these practices present for developing countries such as Nigeria, both in the context of the current pandemic and post-pandemic times (Otey, 2022).

Access to justice speaks of an open and transparent justice accessible to all. The phrase «access to justice» means access for everyone, without discrimination, at least cost, to a range of effective remedies (Adelakun-Odewale & Ogwezzy, 2016). The justice system is available; it avoids discrimination against vulnerable or disadvantaged individuals, and outcomes are predictable and consistent so that dispute processes are just, non-discriminatory, and fair. Access to justice is fundamental to the maintenance of the rule of law as it ensures adequate protection of rights of the citizenry. Access to justice is an integral element of a fair society, enabling the marginalized to have their voices heard and their rights enforced. Concerning Nigeria, to access justice for the citizens effectively and efficiently, there must be physical access to open, independent courtrooms, judicial officers, and support staff. To ensure continuous access to justice, Nigeria must also accelerate the adoption of digital technologies in courtrooms (Olugasa & Davies, 2022).

5.1. Role of Technology in Enhancing Access

Concurrency is required in suggesting the use of IT while simultaneously identifying and advising on the management of areas of concern that potentially escalate access to justice, though, at the detriment of some interests inherent in physical court appearances. It is pertinent to highlight at this juncture that, in the spheres of COVID-19 jurisprudence and legal practice, IT being an enabler for remote hearing is not an entirely new phenomenon; prior to the pandemic, judicial authorities in Nigeria had issued practice direction rules authorizing the hearing of certain categories of matters by teleconference and videoconference[9].

Access to justice has always been an issue both locally and internationally, long before the outbreak of COVID-19. Various impediments existed that hindered easy

[9] Schmitz, A., Shapiro, St., & Lalani, Sh. (2023, August 20). Arbitration Conversation No. 88. https://clck.ru/3MBp4k

access to the courts such as the nature of the courtrooms, financial implications, and so on. However, the issue has reached an astronomical level in Nigeria as a result of the COVID-19 pandemic. The suggestion is on the use of information technology as an enabler for enhanced access to justice in Nigeria is situated within the context and background of certain preexisting salient features of legal practice in Nigeria. It is suggested that the uptake of information technology in this manner would result in greater efficiency and effectiveness of the administration of justice in the legal system (Uwaegbute & Unachukwu, 2022).

6. Ethical and Regulatory Considerations

The integration of modern technologies by the legal community encourages the use of enterprise tools while simultaneously implying constraints and duties defined by a branch of regulation specifically designed to meet the peculiarities inherent in the profession: legal ethics. This area of regulation aims to guarantee that lawyers act within a framework aimed at ensuring the security requirements of citizens, the fairness of the judicial process, the general public interest, or that particular interest that requires the collaboration of a legal expert. The impact of these special provisions creates an interesting regulatory diversification scenario that requires a doctrinal, systematic and comparative legal approach in order to align the three legal elements that jointly govern the crucial role of the lawyer in his/her relationship with communication technology (Tabatabai, 2020).

The activities of legal practice are shrouded with official secrecy owing to the confidential nature of the information with which lawyers are entrusted by their clients. Similarly, lawyers must exercise high professional standards while upholding ethical principles. Thus, the introduction of digital platforms in legal systems appears to be faced with a degree of resistance. The major challenge of the addition of digitalisation to the legal landscape, aside from issues of cost, is the guarantee of protection of client-lawyer privilege in the face of further eavesdropping or e-interceptions by highly skilled computer hackers and third-party intruders. Leaning the foundation of digital applications in the legal sector upon secure platforms is vital to achieve end-to-end communication encryption (Purcell & Brook, 2022).

6.1. Data Privacy and Security

There is no doubt about the potential gains and, in some cases, existing gains to be made from the use of legal technology. However, ensuring that the growth of legal tech, particularly when technology becomes the new normal or a permanent part of the legal practice, is not only protected and secure but also compliant with legal and regulatory requirements is important. Other areas that must be looked at, particularly where legal tech targets the layman and not just the legal practitioner, would include consumer protection in legal tech products and services and legal malpractice as it relates to legal

technology. The interface between legal technology as it concerns the administration of justice and societal requirements and expectations is also important.

While the absence of enabling legislation is identified as a major factor preventing the growth of online legal practice, the increase in internet usage, a significant drop in the price of data, increased acceptability of online sessions, and technologically savvy younger generations appear to have propelled the growth of online legal services internationally. In the UK, where there are corresponding challenges around data privacy and security as it affects legal tech development, the security of data in the criminal justice system, data protection rights, and the combined effects of Brexit and the COVID-19 pandemic on data privacy and security in the legal tech sector cannot be overlooked. While the NDPR is aimed at regulating data privacy and security as a major legal framework of data protection enforceable directly in Nigeria, the law has been criticized for its lack of enforceability, lack of legal backing, and its overreaching provisions. Despite concerns about data privacy and security in Nigeria, a shift in data responsibility for cloud services and guidelines for using internet services effectively was proposed (Babalola, 2022).

6.2. Professional Conduct in Virtual Proceedings

One major challenge that professional conduct presents in virtual proceedings is the fact that the traditional methods used to obtain and maintain high levels of ethical and respectful behaviour, including various forms of policing and punishment, may not work as effectively in virtual space. In a physical courthouse, a judge can see, and if necessary, reprimand lawyers who are behaving badly. In a virtual courthouse, that same degree of visual monitoring may be difficult or impossible. Moreover, the physical isolation associated with most virtual proceedings could attenuate both the sense of community among the participants and the social constraints traditionally imposed by the physical presence of lawyers, judges, and clients in a real courtroom. This social and community constraints could also lead lawyers to adopt inappropriate informal tactics for courtroom advocacy, such as speaking more loudly, using contemptuous evidentiary objections, or acting inappropriately towards opposing counsel (Tiamiyu, 2022).

7. Future Directions and Recommendations

One of the significant impacts of the global health crisis hurried to our doorsteps at the speed of lightning of a thousand thunderbolts that revved the world into a frenzy was the pre-eminence of digitalisation. This paper recommends that in the event of future surges or pandemics, technological measures should be given pre-eminence in court registries not only as practicable contingency measures in addressing the safety concerns of litigants and legal practitioners, but also for the purpose of entrenching the objectives and reasonings behind digitalisation in court practice. All that this approach may lead

qualified officials in charge of court registries to do is to raise the antennae on the recurrent security and life-threatening hazards of individual technological solutions and conduct routine analyses on their ability to be integrated into the framework of our justice system.

The Covid-19 pandemic has only served to vindicate millennia of knowledge and wisdom enunciated by ancient Greek physicians. Epidemiologists have informed us thus far that the potential of a wider spread of Covid-19 is still far from abating. While there are already measures put in place for countries to mitigate the second wave of the Covid-19 pandemic, where is now the opportune time for legal practitioners to put in place some form of contingency plausibility measure so that litigants, particularly those seeking a day in a court of law, may not further have their means unwittingly snatched. The increasing use of digital technology and gadgets has been argued as integral to the access to justice project of conceptualising the meaning of «the court» to mean «any mode of dispute resolution» for litigants to have an outlet as disputes are always bound to come up from time to time.

Other follow-up discussions and implementations should include consideration of remote trial hearings using virtual Court Rooms, developing policy on deployment of E-filing protocols, secure videoconferencing, and the overall digital transformation of the criminal justice system. Key proactive policy changes and innovative measures such as those recently adopted during the pendency of the current pandemic must be further entrenched and sustained post-pandemic, which is where legislations and policy reforms come in. The advantage of timely coordinated measures such as those that have been recently adopted by a wide stakeholder audience in response to the Covid-19 pandemic is that potentially contentious issues such as the adoption and introduction of national, state, federal, and local law for use of technology in legal practices and across sectors were promptly debated, even if essentially at the level of moral suasion, rationale, and advisories. Consequently, when policies and laws are passed in Nigeria, there will hopefully be fewer hiccups in order for the legal practitioners to meaningfully contribute to sustainable development by exploiting the new digital tools of legal practice, performing effectively in the various sectors, as well as ensuring improved access to justice – economically for themselves and by extension society as a whole.

Furthermore, as the impact of access to telecommunication services cannot be overemphasized, training programs can also focus on advocacy, with the hope that legal professionals will encourage telecommunications providers to expand their coverage and reduce the cost of their services. Similarly, training sessions should be held for court registrars and personnel given the results that emerged with the digitalization of the judiciary. Such training can be carried out by government agencies, local non-governmental organizations, and international organizations, as these will not only help the judiciary system, but also enhance the image of the country as a fast-growing economy in Africa. Participants can be awarded certificates at the end of such workshops to encourage active participation and demonstrate the level of expertise.

Conclusion

It is an indisputable fact that the COVID 19 pandemic has changed the landscape of the entire world including legal practice in Nigeria through the use of digital technology. The protracted periods of lockdowns, social distancing and all forms of restrictions took a negative toll on all spheres of human endeavour. Digitalisation of legal practice in Nigeria has been accelerated due to the Covid-19 pandemic. This has resulted in a contactless environment where courts and other judicial bodies have been physically shut down. As a result, legal practitioners have had to find alternative ways to manage their work. While there are benefits to this digitalisation, there are also challenges. Initial discomfort and resistance to change are normal but can be addressed with the help of guidelines. Autonomy, integrity, familiarity, integration, trust, and quality are factors that contribute to the discomfort with new technologies and digitalisation.

These challenges pose new obstacles for the Nigerian legal profession and the implementation of legislation. The Nigerian Bar Association is therefore tasked to engage with stakeholders to find ways to mitigate these effects. But in the face of such rigid measures, we must be determined to forge ahead. There is the saying that when the going gets tough, the tough get going. These are extraordinary times and extraordinary times require extraordinary measures. We cannot insist on only physical court hearings at a time in summery Nigeria has come into terms with the use of digital technology in the practice of law where by the judges citing at the bench or the legal practitioners at the bar which includes their solicitorship jobs.

References

Adelakun-Odewale, O. S., & Ogwezzy, O. O. (2016). Access to Justice of Persons with Disabilities in Africa: The Nigerian Experience. *NOUN Journal of Jurisprudence and International Law*, *1*, 61.

Aidonojie, P. A., Ikubanni, O. O., Oyedeji, A. I., & Okuonghae, N. O. (2021). The Challenges and Impact of Technological Advancement to the Legal Profession in Nigeria given the COVID-19 Pandemic. *Kampala International University*, *6*(4), 5–19.

Arinze-Umobi, Ch. & Okonkwo, I. (2021). Alternative Dispute Resolution Practice in Nigeria and the Effect of COVID-19 Pandemic. *International Journal of Law and Clinical Legal Education*, *2*, 82–85.

Babalola, O. (2022). Data Protection Compliance Organizations (DPCO) Under the NDPR, and Monitoring Bodies under the GDPR: Two Sides of the Same Compliance Coin? *Global Privacy Law Review*, *3*(2), 98–106. https://doi.org/10.54648/gplr2022010

Bello, O. A., & Ogufere, C. (2024). The Emerging Artificial Intelligence Legal-Judicial System's Interface: Assessing the State of Nigeria's Judicial System's Readiness for a Revolution. *Commonwealth Cyber Journal, 2*, 6–24.

Eboibi, F. E., & Mac-Barango, I. (2020). Law and Judicial Application of Digital Forensic Evidence in Nigeria. *Journal of Law, Policy and Globalization*, *96*, 61–75.

Ibekwe, Ch. S., & Onwuatuegwu, Ch. (2021). ICT in the Administration of Justice: Challenges and Prospects for Labour and Productivity. *Nnamdi Azikiwe University Journal of Commercial and Property Law*, *8*(1).

Jimoh, M. A. (2020). Advancing Online Dispute Resolution in Nigeria: Current Opportunities, Legal Challenges and the Ways Forward. *Journal of Sustainable Development Law and Policy*, *11*(2), 407–431. https://doi.org/10.4314/jsdlp.v11i2.6

Karim, R. (2021). 9 The Importance of Legal Services During the COVID-19 Pandemic. In A. Trakic (Eds.), *COVID-19 and Business Law: Legal Implications of a Global Pandemic* (pp. 153–168). Berlin, Boston: De Gruyter 2021. https://doi.org/10.1515/9783110723694-009

Nwaiwu, F. (2021). Digitalisation and sustainable energy transitions in Africa: assessing the impact of policy and regulatory environments on the energy sector in Nigeria and South Africa. *Energy, Sustainability and Society*, *11*, 48. https://doi.org/10.1186/s13705-021-00325-1

Nwebo, O. E. (2023). Administration of Justice and Case Management in Imo State: A Case for Innovation. *Nigerian Journal of Legal Studies*, *12*.

Olugasa, O., & Davies, A. (2022). Remote Court Proceedings in Nigeria: Justice Online or Justice on the Line. *International Journal for Court Administration*, *13*(2), 2–17. https://doi.org/10.36745/ijca.448

Otey, B. S. (2022). The Disconnect: Reflections on the Virtual Connection between Lawyers and Clients. *Washburn Law Journal*, *62*(3), 617.

Purcell, Ch., & Brook, P. (2022). At Least I'm My Own Boss! Explaining Consent, Coercion and Resistance in Platform Work. *Work, Employment and Society*, *36*(3), 391–406. https://doi.org/10.1177/0950017020952661

Tabatabai, Sh. (2020). Simulations and Virtual Learning Supporting Clinical Education During the COVID 19 Pandemic. *Advances in Medical Education and Practice*, *11*, 513–516. https://doi.org/10.2147/AMEP.S257750

Tiamiyu, O. M. (2022). The Impending Battle for the Soul of ODR: Evolving Technologies and Ethical Factors Influencing the Field. *Cardozo J. of Conflict Resolution*, *23*(1), 75–142.

Udemezue, S. (2022). Resolving Conundrums Regarding Legal Profession Regulation in Nigeria (Part 1). *International Review of Law and Jurisprudence*, *4*, 113. https://doi.org/10.2139/ssrn.4313297

Ufua, D. E., Olujobi, O. J., Ogbari, M. E. et al. (2020). Operations of small and medium enterprises and the legal system in Nigeria. *Humanit Soc Sci Commun*, *7*, 94. https://doi.org/10.1057/s41599-020-00583-y

Uwaegbute, K. I., & Unachukwu, D. C. (2022). The Upsurge of Rape during the COVID-19 Lockdown in Nigeria and Its Effects on Survivors. *HTS Teologiese Studies*, *78*(3). https://doi.org/10.4102/hts.v78i3.6996

Walker, J. (2020). Courts in Lockdown: Lessons from International Arbitration. *International Journal of Procedural Law*, 10(2), 178–201. https://doi.org/10.1163/30504856-01002003

Author information

Michael Chukwujindu Ogwezzy – PhD, Full Professor of Human Rights Law, Faculty of Law, Rivers State University
Address: P.M.B 5080, Nkpolu-Oroworukwu, Port Harcourt, Nigeria
E-mail: michael.ogwezzy@ust.edu.ng
ORCID ID: https://orcid.org/0009-0002-2105-2136
Google Scholar ID: https://scholar.google.com/citations?user=_AOOR0YAAAAJ

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 6, 2024
Date of approval – October 27, 2024
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:347:004.4
EDN: https://elibrary.ru//ujsqxf
DOI: https://doi.org/10.21202/jdtl.2025.14

Влияние пандемии COVID-19 на трансформацию судебной системы Нигерии: от традиционного к цифровому правосудию

Майкл Чуквуджинду Огвеззи

Университет штата Риверс, Порт-Харкорт, Нигерия

Ключевые слова

виртуальные слушания,
доступ к правосудию,
законодательство,
пандемия COVID-19,
право,
суд,
судебная система,
цифровая трансформация,
цифровые технологии,
электронное правосудие

Аннотация

Цель: определение ключевых технологических решений, внедренных в судебную систему страны в условиях карантинных ограничений, и оценка их долгосрочного воздействия на отправление правосудия.

Методы: в исследовании применен комплексный подход, включающий анализ нормативных правовых актов, регулирующих цифровизацию правовой сферы в Нигерии, сравнительное изучение практических руководств федеральных судов и судов штатов по проведению виртуальных слушаний, систематизацию данных о внедрении электронных систем ведения дел и управления судебными процессами. Использован доктринальный метод анализа судебных решений и практики применения цифровых технологий в различных юрисдикциях страны.

Результаты: установлено, что пандемия COVID-19 стала катализатором ускоренного перехода нигерийской правовой системы от традиционного бумажного документооборота к цифровым платформам. Выявлены основные технологические решения: системы онлайн-ведения дел, виртуальные залы судебных заседаний, электронные системы подачи документов и цифровые инструменты правовых исследований. Определены преимущества цифровизации, включающие повышение производительности, обеспечение безопасности при рассмотрении дел, а также выявлены недостатки, связанные с обезличенностью документооборота, угрозами конфиденциальности и потенциальной потерей рабочих мест.

Научная новизна: проведен комплексный анализ трансформации юридической практики в Нигерии под воздействием пандемии COVID-19 с фокусом на влияние цифровизации на доступ к правосудию. Исследование вносит вклад в понимание особенностей адаптации правовых систем развивающихся стран к чрезвычайным обстоятельствам через призму технологических инноваций. Разработана

авторская концепция взаимосвязи между цифровой трансформацией судебной системы и обеспечением конституционного права граждан на справедливое судебное разбирательство в условиях социального дистанцирования.

Практическая значимость: результаты исследования могут быть использованы для совершенствования законодательной базы цифровизации правовой сферы в Нигерии и других развивающихся странах. Выводы работы имеют значение для формирования политики в области модернизации судебных систем, разработки этических стандартов виртуального судопроизводства и создания эффективных механизмов обеспечения доступа к правосудию в цифровую эпоху. Практические рекомендации могут быть применены судебными органами для оптимизации процессов отправления правосудия и повышения качества юридических услуг.

Для цитирования

Огвеззи, М. Ч. (2025). Влияние пандемии COVID-19 на трансформацию судебной системы Нигерии: от традиционного к цифровому правосудию. *Journal of Digital Technologies and Law*, *3*(2), 338–362. https://doi.org/10.21202/jdtl.2025.14

Список литературы

Adelakun-Odewale, O. S., & Ogwezzy, O. O. (2016). Access to Justice of Persons with Disabilities in Africa: The Nigerian Experience. *NOUN Journal of Jurisprudence and International Law*, *1*, 61.

Aidonojie, P. A., Ikubanni, O. O., Oyedeji, A. I., & Okuonghae, N. O. (2021). The Challenges and Impact of Technological Advancement to the Legal Profession in Nigeria given the COVID-19 Pandemic. *Kampala International University*, *6*(4), 5–19.

Arinze-Umobi, Ch. & Okonkwo, I. (2021). Alternative Dispute Resolution Practice in Nigeria and the Effect of COVID-19 Pandemic. *International Journal of Law and Clinical Legal Education*, *2*, 82–85.

Babalola, O. (2022). Data Protection Compliance Organizations (DPCO) Under the NDPR, and Monitoring Bodies under the GDPR: Two Sides of the Same Compliance Coin? *Global Privacy Law Review*, *3*(2), 98–106. EDN: https://elibrary.ru/qhzrdm. DOI: https://doi.org/10.54648/gplr2022010

Bello, O. A., & Ogufere, C. (2024). The Emerging Artificial Intelligence Legal-Judicial System's Interface: Assessing the State of Nigeria's Judicial System's Readiness for a Revolution. *Commonwealth Cyber Journal, 2*, 6–24.

Eboibi, F. E., & Mac-Barango, I. (2020). Law and Judicial Application of Digital Forensic Evidence in Nigeria. *Journal of Law, Policy and Globalization*, *96*, 61–75.

Ibekwe, Ch. S., & Onwuatuegwu, Ch. (2021). ICT in the Administration of Justice: Challenges and Prospects for Labour and Productivity. *Nnamdi Azikiwe University Journal of Commercial and Property Law*, *8*(1).

Jimoh, M. A. (2020). Advancing Online Dispute Resolution in Nigeria: Current Opportunities, Legal Challenges and the Ways Forward. *Journal of Sustainable Development Law and Policy*, *11*(2), 407–431. EDN: https://elibrary.ru/abgmvd. DOI: https://doi.org/10.4314/jsdlp.v11i2.6

Karim, R. (2021). 9 The Importance of Legal Services During the COVID-19 Pandemic. In A. Trakic (Eds.), *COVID-19 and Business Law: Legal Implications of a Global Pandemic* (pp. 153–168). Berlin, Boston: De Gruyter 2021. https://doi.org/10.1515/9783110723694-009

Nwaiwu, F. (2021). Digitalisation and sustainable energy transitions in Africa: assessing the impact of policy and regulatory environments on the energy sector in Nigeria and South Africa. *Energy, Sustainability and Society*, *11*, 48. EDN: https://elibrary.ru/kefrsz. DOI: https://doi.org/10.1186/s13705-021-00325-1

Nwebo, O. E. (2023). Administration of Justice and Case Management in Imo State: A Case for Innovation. *Nigerian Journal of Legal Studies*, *12*.

Olugasa, O., & Davies, A. (2022). Remote Court Proceedings in Nigeria: Justice Online or Justice on the Line. *International Journal for Court Administration*, *13*(2), 2–17. EDN: https://elibrary.ru/sqgkxk. DOI: https://doi.org/10.36745/ijca.448

Otey, B. S. (2022). The Disconnect: Reflections on the Virtual Connection between Lawyers and Clients. *Washburn Law Journal*, *62*(3), 617.

Purcell, Ch., & Brook, P. (2022). At Least I'm My Own Boss! Explaining Consent, Coercion and Resistance in Platform Work. *Work, Employment and Society*, *36*(3), 391–406. EDN: https://elibrary.ru/kgbjyl. DOI: https://doi.org/10.1177/0950017020952661

Tabatabai, Sh. (2020). Simulations and Virtual Learning Supporting Clinical Education During the COVID 19 Pandemic. *Advances in Medical Education and Practice*, *11*, 513–516. EDN: https://elibrary.ru/zprfkc. DOI: https://doi.org/10.2147/AMEP.S257750

Tiamiyu, O. M. (2022). The Impending Battle for the Soul of ODR: Evolving Technologies and Ethical Factors Influencing the Field. *Cardozo J. of Conflict Resolution*, *23*(1), 75–142.

Udemezue, S. (2022). Resolving Conundrums Regarding Legal Profession Regulation in Nigeria (Part 1). *International Review of Law and Jurisprudence*, *4*, 113. https://doi.org/10.2139/ssrn.4313297

Ufua, D. E., Olujobi, O. J., Ogbari, M. E. et al. (2020). Operations of small and medium enterprises and the legal system in Nigeria. *Humanit Soc Sci Commun*, *7*, 94. EDN: https://elibrary.ru/cxbynj. DOI: https://doi.org/10.1057/s41599-020-00583-y

Uwaegbute, K. I., & Unachukwu, D. C. (2022). The Upsurge of Rape during the COVID-19 Lockdown in Nigeria and Its Effects on Survivors. *HTS Teologiese Studies*, *78*(3). EDN: https://elibrary.ru/ncvxoj. DOI: https://doi.org/10.4102/hts.v78i3.6996

Walker, J. (2020). Courts in Lockdown: Lessons from International Arbitration. *International Journal of Procedural Law*, *10*(2), 178–201. EDN: https://elibrary.ru/jagrjy. DOI: https://doi.org/10.1163/30504856-01002003

Сведения об авторе

Огвеззи Майкл Чуквуджинду – PhD, профессор в области прав человека, факультет права, Университет штата Риверс
Адрес: Нигерия, Порт-Харкорт, Нкполу-Ороворукву, P.M.B 5080
E-mail: michael.ogwezzy@ust.edu.ng
ORCID ID: https://orcid.org/0009-0002-2105-2136
Google Scholar ID: https://scholar.google.com/citations?user=_AOOR0YAAAAJ

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 – 6 октября 2024 г.
Дата одобрения после рецензирования – 27 октября 2024 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.