YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

Analysis Of The Jurisdictional Challenges In The Realm Of The Digital Age

Dr. G. Mallikarjun, Associate Professor of Law, NALSAR University of Law

Published on: 12th July 2025

Abstract

The digital age has revolutionized human interaction, legal systems, and the exercise of sovereign authority, resulting in complex jurisdictional dilemmas. As cyberspace transcends physical borders, traditional notions of territorial jurisdiction are rendered inadequate. This paper explores the multifaceted legal challenges of regulating actions and data flows in cyberspace, with particular attention to extraterritoriality, cybercrimes, surveillance, and digital sovereignty. It critically analyzes how international law, often grounded in territorial frameworks, struggles to address issues involving non-state actors, multinational corporations, and cross-border cyber operations. The study underscores the need to align digital governance with universally accepted human rights principles, proposing a normative framework where privacy, equality, and security are not compromised. Theoretical models like dialectical, hermeneutic, and comparative legal methods are used to examine existing gaps and propose adaptive legal strategies. The paper also evaluates the emergence of cybercrime as a global threat and the limitations of current international cooperation mechanisms. It concludes by recommending multilateral, human rights–driven legal reforms to navigate jurisdictional uncertainty in the digital sphere.

Key Words: *cyberspace jurisdiction, digital sovereignty, international law, human rights in cyberspace, cybercrime regulation, extraterritoriality*

1. INTRODUCTION

Every aspect of society, including the law, and every individual's life is undergoing a profound transformation due to the advent of the digital age. The vast majority of all legal matters involve some kind of interaction with information technology, and much of that activity takes place online[1]. Modern technology is a by-product of digitisation, with the help of telecommunications and computer networks enabling the usability process. Consequently, people's human rights could be violated as a result of the actions of individuals in other countries due to this interconnectivity[2]. Particularly difficult are issues of jurisdiction, such as how to resolve conflicts between different national and international courts, the extraterritorial effects of cross-border actions, and the potential legal culpability of both natural and legal entities. The data that is essential to everything digital does not merely exist in cyberspace; it is also linked to physical storage facilities that are situated inside the borders of a specific state. Nonetheless, identifying the precise jurisdiction and, more generally, effective legal regulation presents numerous challenges[3]. Before anything else, one must note that data travels through multiple states. Keep in mind that there are objective and subjective limitations to the technical capacities of cyberspace regulation. Extremely huge amounts of data, the digital gap, technological leadership, and the sudden and unexpected appearance of new digital tools are all examples of objective constraints. An example of a subjective limitation would be the reluctance of states to exercise their respective territorial control, the difficulty for international organisations and businesses to reach a consensus on a common set of rules for conducting business, the ambition to profit from the absence of effective regulation, and the lack of legal control over the internet[4]. Additionally, it pertains to the division of responsibilities for actions taken or mediated by individuals or entities on the Internet. In theory, states, persons, and legal entities are mainly considered to be the subjects of such accountability. Due to globalisation, identification problems, and the fact that multinational corporations often have mother, domiciled, and joint companies in countries with different legal systems, it is becoming more and more difficult to identify who is liable, how much of a burden they should bear, and which laws apply[5]. With various identity and authentication models in different states, all parts of electronic government are quickly moving online, posing security risks that could grow worse with the possibility of joint identification. Finding a middle ground between violating and safeguarding human rights in the digital age raises serious concerns. There is no way to

[1]Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A Taxonomy of Cyber-Harms: Defining the Pmpacts of Cyber-Attacks and Understanding How They Propagate. Journal of Cybersecurity, 4 (1). DOI: https://doi.org/10.1093/cybsec/tyy006

[2] Ajayi, E. F. G. (2016). Challenges to Enforcement of Cyber-Crimes Laws and Policy. Journal of Internet and Information Systems, 6 (1), 1-12. DOI: 10.5897/JIIS2015.0089

[3] Al-Hait, A. A. S. (2014). Jurisdiction in Cybercrimes: A Comparative Study. Journal of Law, Policy and Globalization, 22, 75-83.

[4]Andraško, J. (2018). Identification and Authentication of Persons in Cyberspace in Selected States. International and Comparative Law Review, 18 (1), 199-216. DOI: https://doi.org/10.2478/iclr-2018-0032

[5] Brenner, S. W. & Koops, B.-J. (2004). Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, 4 (1), 2-46.

know what will happen as a result of an action in cyberspace as it impacts everyone. This is true of long-term effects like algorithmic bias, growing inequalities around the world as a result of the digital divide, radicalisation of opinions as a result of hate speech on the internet, and people avoiding online democratic processes as a result of privacy breaches, such as the selling of personal data[6]. Directly detrimental influences, such cyberattacks and cybercrimes, also fall under this category. Cybercrimes and cyberattacks are two examples of these direct harmful effects that are currently the subject of much debate. Cybercrimes, in particular, pose a growing threat to businesses around the world, and traditional methods of assessing these threats, such as police-recorded statistics and direct observation of criminal activities, are inadequate. There are two main concerns with the applicability of international law to cyberspace: first, how national and international laws relate to one another; and second, whether or not international law can be applied to cyberspace at all. Most cyber operations do not include the use of force, hence they are analysed through the lens of international law during times of peace. However, more is needed to eliminate the aforementioned issues with the legal regulation of cyber operations. Cyber attacks and cyber conflicts are difficult to define, adding another layer of complexity to the problem from a legal perspective. Hence, there is much evidence that online armed conflict regulations require more research and careful application. Finally, when applying international law standards to cyber activities, it's crucial to keep in mind that there are technical, legal, and, equally significant, political hurdles[7]. As a result, governments are trying to get a bigger hand in regulating internet use and deciding how to apply the law to contentious cases involving new digital technology. There have been numerous efforts to increase the scope of national authorities, such as the legislature's direct extraterritorial reach or the imposition of national rules and regulations on private actors, both of which affect users beyond international borders. Strict legal regulation is at odds with cyberspace's decentralised structure and inherent flexibility. Networks have grown integral to modern life and political, social, and economic development; as a result, all legal connections reflect the dynamic nature of cyberspace and the prioritisation of freedom over security[8]. The digital era has made such networks' infrastructure more global and reliant on collaborative solutions and shared resources. With an emphasis on jurisdictional concerns and cyberspace in particular, this article discusses the aforementioned elements of the major difficulties facing legal reality and legal systems in the digital age. According to the authors, a universal human rights perspective on these matters could provide a solid foundation for ending current and future conflicts. The present research is generally based on general philosophical

[6] Bossler, A. M. &Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42 (5), 495-499. DOI: https://doi.org/10.1080/0735648X.2019.1692426

[7] Coccoli, J. (2017). The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era. Peace Human Rights Governance, 1 (2), 223-250. DOI: https://doi.org/10.14658/pupj-phrg2017-2-4

[8] Gilden, M. (2000). Jurisdiction and the Internet: the «Real World» Meets Cyberspace. ILSA Journal of International & Comparative Law, 7, 149-160.

frameworks for understanding the genesis and interpretation of complex topics, such as dialectic and hermeneutic approaches. One has also used system analysis, dogmatic, and comparative legal methodologies to investigate jurisdictional theories, potential solutions to jurisdictional challenges, and international legal regulations. To further demonstrate the actual application of jurisdictional theories' bottlenecks and to provide some potential scenarios for resolving jurisdictional concerns, one also cite several vital decisions made by authoritative courts.

2. THEORETICAL APPROACHES TOWARDS JURISDICTIONAL CHALLENGES IN THE DIGITAL ARENA

Every facet of modern human existence is increasingly dependent on digital technologies. Not only is information essential to every aspect of existence, but it is also stored, communicated, used, and altered in vast and unregulated quantities—data—and most of this takes place in cyberspace. Neither physical borders nor the whereabouts of individuals have any bearing on the expansion of cyberspace. Also, states and other legal subjects actual locations or motions are somehow linked to notions of jurisdiction and legal control. A jurisdictional problem emerges, as one might expect. Although this topic has been discussed before, it has not made much progress thus far. Also, there are issues with defining what constitutes a problem. Many people believe that regulating the Internet is either theoretically impossible or morally wrong, partly because the exact nature of the jurisdictional problem has not been adequately mapped[9].

In addition, as the internet and its perception evolve, so do people's views on potential solutions. As with Antarctica, outer space, and the open sea—all areas devoid of territorial jurisdiction—proposals were made a decade ago to classify cyberspace as the fourth international space.[10]Although territorial jurisdiction is the most basic and often used form of exercising jurisdiction, the rise of decentralised cyberspace has the potential to change this paradigm and put territorial doctrine to the test in the modern era. Also, unlike these places, cyberspace is entirely man-made and devoid of physical borders; it is a vast, interconnected network of computer networks that facilitates online human communication and business transactions. Cyberspace makes physical location less important since, technically speaking, no specific geographic location or jurisdiction is required for cyber transactions.[11]. But suppose one is intended to consider the idealised picture of cyberspace as a virtual wasteland. In that case, the issues that come up in legal proceedings are not about the lack of physical location of online exchanges. The

[9] Henriksen, A. (2019). The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. Journal of Cybersecurity, 5 (1). DOI: https://doi.org/10.1093/cybsec/tyy009

[10] Huang, Z. &Mačák, K. (2017). Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. Chinese Journal of International Law, 16 (2), 271-310. DOI: https://doi.org/10.1093/chinesejil/jmx011

[11] Maillart, J.-B. (2019). The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime. ERA Forum, Journal of the Academy of European Law, 19, 375- 390. DOI: https://doi.org/10.1007/s12027-018-0527-2

fact that conversations on the Internet could happen anywhere and be subject to the laws of different countries makes things complicated. Since cyberspace has inherent worth and the ability to self-regulate, recent proposals for expanding jurisdictional theories to it may centre on these features. While attempting to resolve jurisdictional issues, one must keep in mind the inherent worth of cyberspace and not infringe upon human rights or the legitimate interests of persons subject to the law. The self-regulatory character defines the method of resolving issues, which depends on individual agency and non-conventional legal tools. The problem is that technology is progressing at a faster rate than any theoretical framework or conventional legal tool, particularly in the realm of digital technologies. Cyberspace may be nothing more than a virtual place with no actual physical connection to any one location; however, the prospect of legal topics reaching a consensus on a single jurisdictional scheme does not appear promising. With so many different national laws and approaches to cyberspace regulation, it is nearly complicated to come to a common understanding of the standards and create a mechanism for their application[12]. This is particularly true in light of the fact that cyberspace's worth is always increasing for any activity. Nevertheless, human rights provide a glimmer of optimism as a globally recognised paradigm for human conduct.

3. HUMAN RIGHTS APPROACH TOWARDS JURISDICTIONAL PROBLEMS

Human rights may soon become a measure of fairness and a criterion for cyberjurisdiction. All or almost all foreign surveillance operations, including the mass collection of communications and personal data of millions of ordinary people, are subject to human rights treaties when seen through the lens of a privacy-based human rights perspective.[13]In this context, it is rightly said that protecting privacy rights as human rights should be a criterion for cyberspace jurisdiction. Thus, treaties on human rights apply to all foreign surveillance activities, including the bulk collection of the communications and personal data of ordinary people, if an approach emphases human rights as a basis[14] An approximation framework centered on the following issues can help us address the discrepancies if one has to adopt a human rights-based approach: (i) How does legal regulation within a particular legal system impact Universal Fundamental rights? (ii) Is human rights protection available both online and offline? (iii) When deciding on the law and jurisdiction to apply, how are the needs of fundamental rights considered? (iv) In the event of a disagreement over jurisdiction, will a specific choice of jurisdiction help to safeguard rights or put them at risk of infringement? (v) How can non-state actors be guaranteed to respect human rights

[12]Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22 (2), 77-81. DOI: https://doi.org/10.1080/1097198X.2019.1603527

[13] Menthe, D. C. (1998). Jurisdiction in Cyberspace: A Theory of International Spaces. Michigan Telecommunications and Technology Law Review, 4, 69-103.

[14]Adeyoju, A. (2022). State Surveillance, the Right to Privacy, and Why We May Need a New International Instrument. https://core.ac.uk/download/559449204.pdf.

by relevant legal instruments? The issue of conflicting rights, which necessitates constant rebalancing, must be considered simultaneously in order to implement this system[15]. The classic conflict of rights, stemming from the tension between liberty and safety, is more pronounced in the information era. There may be incompatibilities between multiple rights that are both equally protected and recognised as human rights. For instance, privacy protections and anti-discrimination laws could clash with the right to free speech. This delicate equilibrium will become much more so if the interpretation of these rights differs between jurisdictions[16]. For instance, the conditional approaches in the United States and Europe will be very different in the case of hate speech. This includes both online utterances and their diffusion in cyberspace. Society pays a price to guarantee freedom of speech, and the American approach supports the concept that excluding such speech from the legal field prevents appropriate discussion and study of critical subjects[17]. Intolerance in expression is destructive but necessary. The European perspective stresses the importance of proportional and reasonable limitations on free speech to promote equality, non discrimination, and harmonious cohabitation in a multi-ethnic society.

It is already challenging to quantify the harmful effects of online speech and the dissemination of hate speech in cyberspace without adding the complexity of their discussion. It should be remembered that anything can be found on the Internet, that thoughts shared here can reach a large audience, and that biases can be introduced into search engine algorithms through commercial tuning. There is a pushback against equality, a basic right and an essential human rights component. The spread of hate speech in cyberspace would result in a negative impact on human rights. The internet remembers everything, the opinions disseminated there can have a vast audience, and commercially tuned search engine algorithms can contribute to biases. Equality, a requirement and a fundamental feature of human rights, is under attack[18]. The requirements for justice and non-discrimination are formally fulfilled, but they are not, in fact. The digital divide exacerbates inequality, in particular, globallyand the actions of non-state actors such as powerful corporations deepen the divide.The formalities of justice and non-discrimination have been met. Still, the reality is otherwise. Particularly on a global scale, the digital gap and the activities of non-state actors, including large businesses, intensify inequality. Particularly, businesses can use corporate policies to control online material or actions, navigating the laws and court decisions of several jurisdictions (e.g., by claiming inapplicability of jurisdiction) with relative ease.

The immediate or indirect detrimental effects of many cyberactions are still hard to foresee.

[15] Stitching the Digital Fabric: The.COMMUNITY Domain Extension – DN.org. https://dn.org/stitching-the-digital-fabric-the-community-domain-extension/

[16] Milanovic, M. (2015). Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. Harvard International Law Journal, 56 (1), 82-146.

[17] Andrew Altman, Freedom of Expression and Human Rights Law: The Case of Holocaust Denial,https://doi.org/10.1093/acprof:oso/9780199236282.003.0002, 2012, Pages 24–49

[18]Kshetri, N., Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22, 2, 2019, 77-81. DOI: https://doi.org/10.1080/1097198X.2019.1603527

Concurrently, many problems in the digital era are taking on a more global character as a result of the increased connectivity of the contemporary world, the rise of novel social structures and interactions, and the shifting power dynamics within non-state entities subject to legal regulation, such as businesses and nonprofits[19]. Hence, the aforementioned detrimental consequences may have an international scope. Directly harmful effects, such as cybercrimes, are a good example of this.

4. CYBER CRIME AS AN EMERGING FORM OF THREAT IN DIGITAL SPACE

In recent years, there has been a growing interest in cybercrimes. The problem is becoming more widespread as digitalisation spreads. In spite of the reasonable claim that all states, irrespective of their legal systems, ought to possess adequate legislative and judicial powers to tackle cybercrime, and that these laws ought to be compatible with one another, safeguarding the common good, numerous inconsistencies emerge in practice. Inadequate international treaties and laws on mutual extradition, joint investigations, and other forms of cooperation that would address the unique aspects of cybercrime and stay up with the ever-changing dynamics of this undeniably complex field are to blame[20]. Another issue is the absence of a universally accepted definition of cybercrime and the kinds of conduct it encompasses. Government's efforts to exert transboundary influence and expand national domains to contentious issues also create problems. Intentional extraterritoriality is not always the case. The sheer essence of cyberspace, as pointed out correctly, makes it extremely difficult to establish jurisdiction for the purpose of prosecuting crimes committed on the Internet. The fundamental character of cybercrime and, more generally, actions involving primarily digital tools and/or conducted online does not conform to the conventional paradigm of comprehension and regulation. Yet, there is no agreement on methods for comprehending and controlling such issues. Authors who argue that cybercrime can be tried using traditional jurisdictional bases are quick to point out that this will cause many disputes and disputes over who gets to decide who gets sued. They also concede that cybercrime cases may soon focus on where the victim or perpetrator is located, bringing up the issue of location again[21]. Given the global nature of cybercrime and its substantial harm, more extreme perspectives on resolving jurisdictional issues surrounding this crime include using the extra criminal justice principle and universal jurisdiction. It is also intended to take action on a global scale. Specifically, the UN should spearhead efforts to have member states enact cyber jurisdictional rules and should publish a model law to help other countries do the same. This is an extremely important topic for international law. This fits in with future plans to

[19]Oraegbunam, I. K. E. (2015). Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea from International Law? Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 6, 57-65.

[20] Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. The Yale Journal of International Law, 43, 191-227.

[21] Rice, D. T. (2000). Jurisdiction in Cyberspace: Which Law and Forum Apply to Securities Transaction on the Internet? University of Pennsylvania Journal of International Economic Law, 121 (3), 585-657

address jurisdictional issues on a global scale, with an eye on the United Nations and the planned legal framework at this level of regulation[22]. The primary issues of the digital age are the effectiveness of the prospective legal framework and the complexity of fighting this form of crime in today's society. The fact that sophisticated automation and technologies have stepped in to compensate for the shortage of highly trained professionals, allowing for impunity in cyber attacks and invasions is particularly concerning. This new danger may even be global in scope. Thus, in today's world, information technology experts no longer need to take advantage of the weaknesses in digital tools; all that is required are other digital tools. It should be stressed that current cybercrime studies are more concerned with testing the hypothesis that cybercrimes share the same theoretical underpinnings as more conventional crimes. Cybercrime cost estimates are notoriously difficult to come by, in part because such tools are primarily intended to monitor attack patterns rather than actual damage. Theoretical frameworks do not always work when applied to cybercrime for three reasons: (i) it is a distinct kind of crime that relies on digital tools, (ii) it can affect people all over the world and has an effect on information in cyberspace, and (iii) it perfectly exemplifies the characteristics of development uncertainty and unpredictability that we witness in the digital age. Considering all possible avenues for problem-solving is essential when returning to the theses on direct and indirect harm, difficult-to-predict outcomes, and long-term effects of online activities and mediation.

5. POLICY SUGGESTIVE FOR ANALYSING THE JURISDICTIONAL CHALLENGES

More clarity is needed regarding the potential future for addressing jurisdictional and cross-border challenges in the digital era. These potential futures include calls for increased autonomy while encouraging all stakeholders to collaborate.[23] Users of cyberspace resources may be asked to take for some of the responsibility. More precisely, it is urged that demands be made of the cyber-community, which collectively ought to assume greater responsibility for monitoring what is spreading throughout the network. This is something that should be done. This fulfils the requirements for interactions that are mediated by digital technology, as well as the self-regulation and autonomous control of cyberspace systems. Maintaining efforts to (i) establish consistent worldwide regulations for the Internet, (ii) encourage more self-regulation on the part of hosts and users, and (iii) educate policymakers on the underlying workings of the Internet and the World Wide Web are all important goals that should be pursued. One must continue using multilateral efforts, bilateral agreements, and informal exchanges between public and commercial entities across borders. This is due to the fact that the difficulties associated with controlling the online realm have become systemic, and tensions are sure to intensify.

[22] Svantesson, D. J. B. (2004). An Introduction to Jurisdictional Issues in Cyberspace. Journal of Law and Information Science, 15, 50-74.

[23] Wilske, S. & Schiller, T. (1997). International Jurisdiction in Cyberspace: Which States May Regulate the Internet? Federal Communications Law Journal, 50 (1), 117- 178.

The fact that no one technique has emerged as the most viable alternative in cyberspace should be kept in mind regardless of the circumstances. All of these options come with their own set of benefits and drawbacks, are weighted down by ethical and legal considerations, and, most crucially, cannot be put into reality without on-going iteration to accommodate the highly unexpected speed of technology innovation. Until this point, regulating and enforcing laws belonging to cyberspace and information technology has been analogous to juggling many different goals that conflict with one another[24].

When the right to be forgotten is taken into consideration, the data protection regulation of the European Union has a clearly extra-territorial character. This is just one example. A significant number of disagreements, although their jurisdictional aspects appear to be insurmountable, eventually fail to produce any results that are meaningful. The case of United States v. Microsoft Corp[25]is an example of a case that did not result in a decision being reached. This case was expected to redefine certain jurisdictional concerns, but instead, it was referred to as Microsoft's email privacy conflict. Computing in the cloud and, more significantly, the export of data that has been stored were the first sources of contention. During the time that the case was being examined by the Supreme Court of the United States, law enforcement agencies were given further jurisdiction, and new legislation was introduced that addressed the use of data from cloud storage. Since the critical issue of cross-border digital evidence collecting, which is a problem that affects both the state and the corporation, needed to be appropriately addressed, the trial was ultimately withdrawn. With these same cloud storage services, storing confidential patient information in nations outside of the United States is possible. At the same time, the resources of the public health sector may be significantly more vulnerable than those of a large corporation, which may have the ability to possess both economic and technological capabilities but cannot guarantee the protection of data that becomes a trade secret. On the other hand, if cyber actors were to undermine life support systems, there may be immediate and devastating consequences. In addition, as the recent COVID-19 pandemic lesson has revealed, in our interconnected and globalised society, everything can potentially touch everyone.

Thus, all stakeholders must work together to minimise or at least lessen the impact of the unwanted outcomes induced by the acts of law subjects in the digital age. To clarify, we are referring to everything related to the use of information technology or that occurs in cyberspace. Any additional study conducted in this field may concentrate on addressing strategies and generating specific recommendations for minimising and managing the effects of the impacts[26].

6. CONCLUSION

[24] Michael A. Geist, Is There a There There? Toward Greater Certainty for Internet Jurisdiction, 16 Berkeley Technology Law Journal . 1345, 1356 (2001).

[25]United States of America v. Microsoft Corporation - 253 F.3d 34

[26] Wilske, S. & Schiller, T. (1997). International Jurisdiction in Cyberspace: Which States May Regulate the Internet? Federal Communications Law Journal, 50 (1), 117- 178.

The adverse effects of the digital age are making jurisdictional concerns, such as cybercrime, the resolution of the interrelationship between international and national jurisdictions, cross-border activities and extraterritorial consequences, and the exposure of both natural and legal persons to legal liability, a topic of particular interest at the international level and national level. Thus, the ways to solve jurisdictional issues in this digital age are complex and multifaceted primarily, issues can be divided into global and national-level issues. The global approach, focusing on a single legal framework and universal mechanisms, presents a complex landscape. The national-level approach, which partly considers the possibility of a single legal framework (or a set of agreements) and relies mainly on regional mechanisms, adds another layer of complexity. Such approaches imply mutual cooperation, which can be based on political and economic interests, cultural ties, and geographic location. Global approaches imply a somewhat forced cooperation, as parties understand that forming universal international legal mechanisms and global agreementshas never been easy or quick. National approaches hold on to the idea that each legal system can effectively respond to the threats of the digital age and, accordingly, shape the legislative framework and judicial practice[27].

It is important to note that none of the approaches will solve jurisdictional issues. They have pros and cons, and legal and ethical considerations burden them. The dynamic nature of the digital age necessitates ongoing revision of these approaches. So far, the regulation and application of law regarding the use of information technology and activities in cyberspace have resembled a careful balancing act.

Many disputes with a jurisdictional component promise to be sharp, but in reality, they end in nothing. Controversy arose around the use of data in cloud storage and, in particular, its transfer abroad. During the consideration of the case by the United States Supreme Court, new legislation was passed that included the issue of using data from cloud storage and provided law enforcement agencies with some new powers. As a result, the issue of digital evidence collected across borders, vital for both parties—the state and the corporation—was not resolved substantively, and the trial was dropped[28].

The beginning is to discuss strategies and develop specific recommendations for preventing and mitigating consequences of jurisdictional challenges. The complexity and importance of jurisdictional issues in the digital age make them ripe for further research and exploration. The advent of the digital era has given rise to problems over jurisdiction. Traditional legal laws, which still need to consider the rapid technological innovation that is taking place on a global scale, are applied in a manner that contradicts one another.

Another aspect is the distinctive nature of legal subjects' online actions or the interconnection of those

[27]Razmetaeva, Y., Ponomarova, H., &Bylya-Sabadash, I. (2021). Jurisdictional Issues in the Digital Age. Ius Humani. https://doi.org/10.31207/ih.v10i1.240

[28] ibid

acts with IT and digital resources. The worldwide nature of the internet, the overall interconnection of the world, and the redistribution of power between states and non-state actors mean that both direct and indirect negative influences today have far-reaching and unpredictable effects and that the severity of these consequences may grow.[29]A worldwide legal system based on human rights is one conceivable foundation for settling present and future problems.

Regardless of the type of scenario for solving jurisdictional problems based on approaches: (i) global, which focuses on the idea of a single worldwide legal framework and a universal regulation mechanism; (ii) fragmented, which partly considers the possibility of a single legal framework and relies on regional mechanisms; and (iii) national, which aligns legislation and judicial practise with the idea that each legal system can effectively respond to the threats of the digital age.

In light of present trends pointing towards the expansion of the digital environment, those who have a stake in the matter ought to make an effort to prevent or, at the least, diminish the negative impacts caused by the activities of the subjects of law.

[29] Xinmin, M. (2016). Key Issues and Future Development of International Cyberspace Law. China Quarterly of International Strategic Studies, 2 (1), 119-133. DOI: https://doi.org/10.1142/S237774001650006

Reference

- I Agrafiotis and others, 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate' (2018) 4(1) *Journal of Cybersecurity* https://doi.org/10.1093/cybsec/tyy006
- EFG Ajayi, 'Challenges to Enforcement of Cyber-Crimes Laws and Policy' (2016) 6(1) *Journal of Internet and Information Systems* 1 https://doi.org/10.5897/JIIS2015.0089
- AAS Al-Hait, 'Jurisdiction in Cybercrimes: A Comparative Study' (2014) 22 *Journal of Law, Policy and Globalization* 75
- J Andraško, 'Identification and Authentication of Persons in Cyberspace in Selected States' (2018) 18(1) *International and Comparative Law Review* 199 https://doi.org/10.2478/iclr-2018-0032
- SW Brenner and B-J Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4(1) *Journal of High Technology Law* 2
- AM Bossler and T Berenblum, 'Introduction: New Directions in Cybercrime Research' (2019) 42(5) *Journal of Crime and Justice* 495 https://doi.org/10.1080/0735648X.2019.1692426
- J Coccoli, 'The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era' (2017) 1(2) *Peace Human Rights Governance* 223 https://doi.org/10.14658/pupj-phrg2017-2-4
- M Gilden, 'Jurisdiction and the Internet: the "Real World" Meets Cyberspace' (2000) 7 *ILSA J Intl & Comp L* 149
- A Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5(1) *Journal of Cybersecurity* https://doi.org/10.1093/cybsec/tyy009
- Z Huang and K Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches' (2017) 16(2) *Chinese Journal of International Law* 271 https://doi.org/10.1093/chinesejil/jmx011
- J-B Maillart, 'The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime' (2019) 19 *ERA Forum* 375 https://doi.org/10.1007/s12027-018-0527-2
- N Kshetri, 'Cybercrime and Cybersecurity in Africa' (2019) 22(2) *Journal of Global Information Technology Management* 77 https://doi.org/10.1080/1097198X.2019.1603527
- DC Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 *Mich Telecomm & Tech L Rev* 69

- A Adeyoju, 'State Surveillance, the Right to Privacy, and Why We May Need a New International Instrument' (2022) https://core.ac.uk/download/559449204.pdf
- *DN.org*, 'Stitching the Digital Fabric: The .COMMUNITY Domain Extension' https://dn.org/stitching-the-digital-fabric-the-community-domain-extension/
- M Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56(1) *Harvard International Law Journal* 82
- A Altman, 'Freedom of Expression and Human Rights Law: The Case of Holocaust Denial' in *Freedom of Expression and Human Rights Law* (OUP 2012) 24–49 https://doi.org/10.1093/acprof:oso/9780199236282.003.0002
- IK Oraegbunam, 'Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea from International Law?' (2015) 6 *NAUJILJ* 57
- A Perloff-Giles, 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges' (2018) 43 *Yale J Intl L* 191
- DT Rice, 'Jurisdiction in Cyberspace: Which Law and Forum Apply to Securities Transactions on the Internet?' (2000) 121(3) *UPenn J Intl Econ L* 585
- DJB Svantesson, 'An Introduction to Jurisdictional Issues in Cyberspace' (2004) 15 *Journal of Law and Information Science* 50
- S Wilske and T Schiller, 'International Jurisdiction in Cyberspace: Which States May Regulate the Internet?' (1997) 50(1) *Federal Communications Law Journal* 117
- MA Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction' (2001) 16 *Berkeley Tech LJ* 1345
- *United States v Microsoft Corp*, 253 F.3d 34 (DC Cir 2001)
- Y Razmetaeva, H Ponomarova and I Bylya-Sabadash, 'Jurisdictional Issues in the Digital Age' (2021) *Ius Humani* https://doi.org/10.31207/ih.v10i1.240
- Xinmin Ma, 'Key Issues and Future Development of International Cyberspace Law' (2016) 2(1) *China Quarterly of International Strategic Studies* 119 https://doi.org/10.1142/S237774001650006