Ius Humani
Revista de Derecho. Vol. 10 (I) (2021), pp. 167-183. ISSN: 1390-440X — eISSN: 1390-7794
Recepción: 8-8-2020. Aceptación: 22-2-2021. Publicación electrónica: 12-4-2021
https://doi.org/10.31207/ih.v10i1.240

JURISDICTIONAL ISSUES IN THE DIGITAL AGE

CUESTIONES JURISDICCIONALES EN LA ERA DIGITAL

Yulia Razmetaeva[*]
Hanna Ponomarova[**]
Iryna Bylya-Sabadash[***]

Abstract: The article addresses some aspects of the key challenges for legal reality and legal systems in the digital age with a focus on jurisdictional issues in special attention to cyberspace, given its independent value and self-regulatory nature. The article suggests that regarding issues through the prism of a universal human rights approach could be a pillar for resolving existing and potential digital conflicts, prevent cybercrimes. The general legal framework in light of this approach is proposed here. The article discusses scenarios for solving jurisdictional problems: (i) global—focuses on the idea that a single worldwide legal framework and a universal regulation mechanism are possible; (ii) fragmented—partly considers the possibility of a single legal framework (or a set of agreements) and rely mainly on regional mechanisms; and (iii) national—each legal system is capable of providing and effective response to the threats of the digital age and aligns its legislation and judicial practice with the latter. Finally, it is suggested to focus on the prevention and mitigation of negative consequences of the activities of all subjects of law.

[*] Ph.D., Associate Professor of the Department of Theory and Philosophy of Law, Yaroslav Mudryi National Law University (Kharkiv, Ukraine). https://orcid.org/0000-0003-0277-0554. yulia.razmetaeva1@gmail.com
[**] Ph.D., Associate Professor of the Department of History of State and Law of Ukraine and Foreign Countries, Yaroslav Mudryi National Law University (Kharkiv, Ukraine). https://orcid.org/0000-0003-4940-1406. hanna.ponomarova@gmail.com
[***] Ph.D., Associate Professor of the Department of Theory and Philosophy of Law, Yaroslav Mudryi National Law University (Kharkiv, Ukraine). https://orcid.org/0000-0001-7069-9708. i.o.bylya8@gmail.com

Keywords: Cybercrimes, Cyberspace, Digital Age, Human Rights, Jurisdiction

Resumen: *El artículo aborda algunos aspectos de los desafíos clave que enfrenta la realidad jurídica y los sistemas legales en la era digital con enfoque en las cuestiones jurisdiccionales, prestando especial atención al ciberespacio, dado su valor independiente y su naturaleza autorreguladora. El artículo sugiere que abordar los problemas a través del prisma de los derechos humanos universales podría ser un pilar para resolver los conflictos digitales existentes y potenciales, así como prevenir los delitos cibernéticos. A la luz de este enfoque, aquí se propone un marco legal general. El artículo discute escenarios para resolver los problemas jurisdiccionales: (i) global, el cual se centra en la idea de la posibilidad de un marco legal mundial único y un mecanismo de regulación universal; (ii) fragmentado, que en parte considera la posibilidad de un marco legal único (o un conjunto de acuerdos), basado principalmente en mecanismos regionales; y (iii) nacional, en el que cada sistema jurídico nacional es capaz de proporcionar una respuesta eficaz a las amenazas de la era digital y alinea a esta su legislación y práctica judicial. Por último, se sugiere centrarse en la prevención y mitigación de las consecuencias negativas de las actividades de los sujetos de derecho.*

Palabras clave: *Ciberdelitos, Ciberespacio, Era digital, Derechos humanos, Jurisdicción*

I. INTRODUCTION: KEY CHALLENGES FOR LEGAL SYSTEMS IN THE DIGITAL AGE

In the digital era, fundamental changes are taking place –in legal reality, in society as a whole, and in the life of every person, in particular–. A significant part of the activities of all subjects of law occurs in cyberspace or is closely related to the use of information technologies. Today's technologies are the product of a reality digitalization and often the usability process is made possible thanks to telecommunications systems and

computer networks. Therefore, such an interconnection exposes individuals to potentially adverse consequences for their human rights, caused by the behaviors of people operating within other jurisdictions (Coccoli, 2017).

Extremely serious challenges are jurisdictional problems, in particular, resolving the interrelation between international and national jurisdictions, cross-border activities and extraterritorial consequences, bringing both natural and legal persons to legal liability. The information in the form of data, which is the key to any activity in the digital age, does not just run in the virtual space, it is connected with physical storage that are territorially located in the jurisdiction of a particular state. However, there are several obstacles to determining the exact jurisdiction and effective legal regulation in general. First of all, it should be borne in mind that information is routed through the territory of several states. It should also be borne in mind that the technical capabilities of regulating activities in cyberspace are limited both objectively and subjectively.

Objective limitations are expressed in such aspects as an extremely large amount of information, the digital divide, and the technological leadership, the rapid and unpredictable emergence of new digital tools. Subjective limitations are expressed in such aspects as the unwillingness of states to carry out the respective territorial control, organizations and businesses from different countries to agree on specific rules for providing their business activity, the desire to take advantage of the lack of effective regulation, and law degree of control over the online environment. It is also about sharing responsibility for activities conducted or mediated by natural or legal persons online. Theoretically, the subjects of such responsibility are primarily states, individuals and legal entities. But to determine the subjects of responsibility in a particular case, the degree to which they should bear it, and the applicable law is becoming increasingly difficult, as due to global activity, when giant corporations have mother, domiciled, joint companies in countries with different legal systems, and because of identification issues. Considering different models of identification and authentication in some states, Jozef Andraško (2018) writes about the rapid transition to cyberspace of all aspects of electronic governance, which raises security issues that could potentially become even more problematic, given the potential for joint identification.

There are acute questions about balancing human rights and protecting them online in the digital era. Moreover, actions in cyberspace affect all actors, and the consequences of such actions are hard to predict. This applies to indirect and delayed impacts, such as algorithmic discrimination, widening global inequality due to the digital divide, radicalization of views due to online hate speech or self-restriction from participating in online

democratic processes due to numerous privacy violations (for example, the sale of personal data). This also applies to direct harmful influences, such as cyberattacks and cybercrimes. Numerous discussions are underway to evaluate these direct harmful effects, in particular cyberattacks, since "the threat landscape of cyberattacks is rapidly changing and the potential impact of such attacks is uncertain" (Agrafiotis, *et al.*, 2018), as well as cybercrimes, for the evaluation of which traditional sources such as police-recorded statistics and direct observation of criminal activities work poorly (Riek & Böhme, 2018), the growing threats from cybercrime and the need for global security for business (Moskowitz, 2017).

In the digital age, the question of applicable law also raises sharply, both in connection with the correlation of national and international law, and in connection with doubts about the admissibility of applying international law as such to activities in cyberspace. Zhixiong Huang and Kubo Mačák (2017) manifest that "most cyber operations do not cross the use of force threshold and must be analyzed through the prism of peacetime international law" (p. 310), but this does not exclude all the above problems of legal regulation of cyber operations. With regard to the law of war, the issue is even more complex, in particular due to the uncertainty of what can be defined as cyberattacks and cyber conflicts. Therefore, many points to the need for careful study and careful application of armed conflict laws to cyberspace (see Xinmin, 2016; Mačák, 2017). The last but not least, it is necessary to consider the presence of technical, legal and, no less important, political difficulties when applying the norms of international law in relation to cyber operations (Pipyros, *et al.*, 2016).

In these conditions, states seek to expand their jurisdiction, both on online activities, and on controversial issues of the application of law in situations related to the development of digital technologies. There are many attempts to expand national jurisdictions, for instance, direct extraterritorial reach of the legislature or impose national laws and regulations on private actors, which has direct transboundary impacts on all foreign users (La Chapelle & Fehlinger, 2016, p. 9). At the same time, the decentralized nature and flexible structure of cyberspace are contrary to methods of strict legal regulation. The priority of freedom over security and the dynamism of cyberspace are reflected in all legal relationships in the modern world, where networks have become an important part of everyday life and political, social, and economic development. In the digital age, the infrastructure of such networks is becoming more global and more dependent on shared resources and joint solutions.

This article addresses the abovementioned aspects of the key challenges for legal reality and legal systems in the digital era with a focus

on jurisdictional issues and a particular focus on cyberspace. The article suggests that considering these issues through the prism of a universal human rights approach could be a pillar for resolving existing and potential conflicts. To conduct the research, we used methods such as dialectic and hermeneutic approaches as a general philosophical basis for studying problematic issues in their development and interpretations. We have also applied methods of system analysis, dogmatic and comparative legal methods, primarily to consider jurisdictional theories, scenarios for solving jurisdictional problems, legal regulation used in different countries. In addition, we refer here to a series of significant decisions by authoritative courts to illustrate the practical application of the bottlenecks of jurisdictional theories and some possible scenarios for resolving jurisdictional problems.

II. MATERIALS AND METHODS TO RESEARCH THE JURISDICTIONAL ISSUES

The theoretical and methodological basis of the work is the general scientific methods of research and special methods based on modern scientific foundations of economics, law and related sciences. The methods used are: (i) economical and statistical, to analyze the current state cyberspace problems; (ii) complex and systematic analysis, for the study of literary sources, normative-legal acts in the studied sphere; (iii) abstract-logical, for theoretical generalization and formation of conclusions; and (iv) analysis and synthesis, for module research.

III. WORLD JURISDICTIONAL THEORIES AND CYBERSPACE PROBLEM

The digital age can be described as an era where every aspect of human life or activities are mainly information based (Pathak, 2016, p. 18). But the important thing here is not only the informational component of any life or activity, but also the fact that, firstly, information in the form of data in huge and uncontrolled volumes is stored, transmitted, used and modified, and secondly, much of this happens in cyberspace.

The development of cyberspace is not based on physical boundaries or the location of subjects. At the same time, legal regulation and jurisdictional theories are somehow attached to states and other subjects of law having a geographical location or moving in physical space. Obviously,

a jurisdictional problem arises. This discussion is not new, but so far it has not advanced significantly. In addition, difficulties also arise with what exactly is considered a problem. As noted, "partly because of this failure to map the precise nature of the jurisdictional problem, regulation of the Internet is commonly seen as either empirically unfeasible or normatively illegitimate" (Perloff-Giles, 2018, p. 192). Moreover, opinions about a possible solution change as the landscape of the online environment and its perception in the world transform. A decade ago, proposals were made to make cyberspace the fourth international space, similar in regulation to Antarctica, outer space and the open sea, that is, spaces where there is no territorial jurisdiction (see Menthe, 1998, pp. 101-102; Wilske & Schiller, 1997, p. 175). Despite the fact that territorial jurisdiction is the most fundamental and commonly accepted method of exercising jurisdiction, the development of decentralized cyberspace could shift this paradigm, and, as Jean-Baptiste Maillart (2019) point, call into question the territorial dogma in the digital age (p. 376). Besides, unlike these spaces, cyberspace, according to Ma Xinmin (2016), "per se does not have any territory or boundary, it is a man-made virtual space based on the interaction and intertwinement of human cyber activities supported by cyber infrastructures" (p. 125).

Nevertheless, cyberspace essentially diminishes the significance of the physical location, because, as Denis T. Rice (2000) wrote, "transactions in cyberspace, strictly speaking, do not take place in any particular geographic location or jurisdiction" (p. 585). At the same time, if we cast aside the somewhat romantic view of cyberspace as virtual nowhere, the questions that arise before the law are not that online interactions occur nowhere. As Dan Jerker B. Svantesson (2004) sagaciously noted, "what causes the difficulties is that Internet interactions potentially occur everywhere and come under the jurisdiction and laws of multiple legal systems" (p. 72). Therefore, modern ideas about applying jurisdictional theories to cyberspace could be focused on the fact that it has a value of its own and a self-regulatory character. The independent value of cyberspace makes us think about how not to harm human rights and the legitimate interests of subjects of law while trying to solve jurisdictional problems. The self-regulatory nature determines the style of problem solving based on autonomy and the use of non-traditional legal instruments. However, neither traditional legal instruments nor the most daring theories can keep pace with the development of technology, especially when it comes to digital technologies.

Regardless of what cyberspace is—nowhere virtual, a special space that is fully or partially tied to territorial or other physically applied objects—a scenario in which subjects of law are able to agree on a single

applicable jurisdictional scheme does not look too real. It is almost impossible to agree on a common understanding of the standards and develop a mechanism for their application with such a variety of relevant national laws and approaches to the regulation of cyberspace, especially given its ever-growing value for any activity. However, there is some hope that humanity has at least one universally agreed framework of activity—human rights.

IV. THE HUMAN RIGHTS APPROACH AND BALANCING

Human rights may become the yardstick of justice and a criterion for jurisdiction in cyberspace. Considering a human rights-based approach in the context of privacy, Marko Milanovic (2015) writes that "human rights treaties do apply to all or the vast majority of foreign surveillance activities, including the bulk collection of the communications and personal data of millions of ordinary people" (p. 140). If we take an approach based on human rights as a basis, then the contradictions can be resolved using an approximate framework that would focus on the following questions: (i) How does legal regulation within a specific legal system affect universal fundamental rights? (ii) Does it protect human rights online as well as offline? (iii) How are the requirements of fundamental rights taken into account when choosing the applicable law and jurisdiction? (iv) In case of a jurisdictional dispute, will a particular choice of jurisdiction contribute to the protection of rights or, conversely, create a threat of their violation? (v) How do applicable legal instruments ensure respect for human rights by non-state actors?

Simultaneously, to apply this framework one should consider the problem of conflict of rights, which require dynamic balancing. Classical clash of rights, originating from the contradiction of freedom and security, is particularly acute in the digital age. Several rights that are equally protected as human rights may conflict with each other. For example, freedom of expression may conflict with privacy or the prohibition of discrimination. And if the understanding of these rights varies in different legal systems, then this balance is even more complicated.

If we take an example of the legal regulation of hate speech, including online statements or their dissemination in cyberspace, then the conditional American and European approaches will differ significantly. The American approach supports the view that the exclusion of such a speech from the legal field does not allow proper discussion and study of problematic issues, intolerance in expression, although harmful, is the price that society pays to

ensure freedom of speech. The European approach advocates the need for reasonable and proportional restrictions on freedom of expression for the sake of equality, non-discrimination and coexistence in a multicultural society.

In the laws of the United States of America, most forms of hate speech are protected, and attempts to impose restrictions on it are usually rejected by the Supreme Court of the United States. This kind of speech must cause violence or harm before it is considered a crime. Supporters of the special protection of freedom of speech are convinced that, for example, racist statements must be fought with the help of combating racism and banning them as a hate speech can hit innocent people. In particular, the Supreme Court of the United States (2011) in the case "Snyder v. Phelps" concluded that the religious community of Westboro Baptist Church had the right to picket holding hateful posters in the public place, in front of the cemetery where the soldier's funeral was held. This caused a wide discussion, as a result of which a part of society took the position that punishment for the actions of the picketers would mean an encroachment on fundamental freedoms and that protection should be provided even for offensive statements in connection with discussion of socially significant issues in order not to limit open discussion or not to drown it.

In a dispute between the American company *Yahoo!* and the French organization *Ligue Internationale Contre le Racisme et l'Antisémitisme* (International League Against Racism and Anti-Semitism) which fights intolerance and xenophobia, the United States Court of Appeals for the 9th Circuit has ruled that the French orders are not enforceable in the United States because such enforcement would violate the First Amendment to the United States Constitution (United States Court of Appeals for the 9th Circuit, 2006). The French side in this case demanded that *Yahoo!* banned users from accessing an Internet auction for the sale of Nazi paraphernalia, which was organized on the *Yahoo!* site in France. Thus, while the content was downloaded and viewed in France, from the American perspective, it was not subject to French legislation banning online hate speech.

European laws contain different language regarding hate speech, and generally stipulate more stringent liability. In addition, there are some topics in many legal systems in which the balance of rights becomes a sensitive issue. For instance, in the case of "Garaudy v. France" (2003) the European Court of Human Rights (ECHR) has confirmed that Holocaust denial is a form of speech that has no protection of the right to freedom of expression, that is, protection in accordance with article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. Roger Garaudy wrote a book in which he contested some of the historical facts about the Holocaust and crimes against humanity. The ECHR concluded that this was

not a historical investigation in search of truth, but an appeal against crimes against humanity, and that is one of the most severe forms of racial slander and incitement to hatred of Jews. The ECHR considered that the denial or rewriting of this type of historical fact is a serious threat to public order, incompatible with democracy and human rights.

When we deal with online speech, the spread of hate speech in cyberspace, as well as with their discussion, it becomes even more difficult to measure their negative impact on human rights. It should be noted that the Internet does not forget anything, and that the opinions disseminated there can have a huge audience, and that commercially tuned search engine algorithms can contribute to biases. Equality, which is both a requirement and a fundamental feature of human rights, is under attack. The requirements for justice and non-discrimination are formally fulfilled, but in fact they are not. The digital divide exacerbates inequality, in particular, globally, and the actions of non-state actors such as powerful corporations deepen the divide. In particular, companies can regulate content or activities in cyberspace using corporate policies, successfully maneuvering between legislation and judicial practice of different legal systems, including by citing the inapplicability of jurisdiction. For example, in many African countries, according to Nir Kshetri (2019), cybersecurity is considered a luxury, and cyberattacks originating from these countries have a worldwide impact, which is why companies from industrialized countries classify online transactions as risky. Scam emails from Nigeria that end up in your spam folders and promise a win or an inheritance have become the talk of the town. Has this changed the way Internet users view Nigeria? It is quite possible that yes.

Today, it is difficult to predict what delayed or indirect negative impact many actions in cyberspace will have. At the same time, many issues in the digital age are becoming global in nature due to the interconnectedness of the modern world, the emergence of new social relations and constructs, and the change in the degree of influence of such non-state subjects of law as companies and organizations. Therefore, the abovementioned negative effects can be global. This is well illustrated by direct malicious impacts such as cybercrimes.

V. THE CYBERCRIMES AS GLOBAL ISSUE IN DIGITAL AGE

The cybercrimes have recently been a subject of burgeoning interest last years. And the wider digitalization becomes the more common the problem gets.

Despite the fair assertion that every state, regardless of the type of legal system, "should have sufficient legislative and judicial capabilities to combat cybercrime and such laws must be harmonious among different countries; since they protect the common interest" (Al-Hait, 2014, p. 83), in reality many contradictions arise. They are a consequence of such problems as a lack of global consensus on the definition of cybercrime and the types of behavior it covers, a lack of synchronized mechanisms and procedures, international treaties and acts on mutual extradition, joint investigations and other cooperation that would respond to the specific of cybercrime and keep pace with the dynamics in such an undoubtedly complex area. In addition, obstacles arise as a result of attempts by governments to exercise transboundary influence and extend national jurisdictions to disputed cases. This does not always happen as a purposeful extraterritoriality. After all, the very nature of cyberspace, as rightly noted, "constitutes an affront to easy determination of jurisdiction in relation to the prosecution of Internet crimes" (Oraegbunam, 2015, p. 63).

There is no consensus on approaches to understanding and regulating cybercrime problems, but it is clear that the very nature of such crime and, in general, activities using predominantly digital tools and/or conducted online do not fit into the traditional framework of understanding and regulation. Even those authors who hold the position that traditional jurisdictional bases can be applied to cybercrime, note that this will lead to conflict of jurisdictions and numerous claims and acknowledge that "cybercrime may sooner look at the location of the effect or the location of the perpetrator or victim" (Brenner & Koops, 2004, p. 44), which again brings us back to questions of location. More radical views on the solution of jurisdictional problems of cybercrime include proposals to apply the universal jurisdiction and the extra criminal justice principle (see Jiménez, 2015; Ajayi, 2016), given the transnational, as well as the significant harm from this type of crimes.

It is also proposed to act at the level of the international community. In particular, within the United Nations, which should take the lead "not only encouraging member states to formulate national laws in this crucial area but also come out immediately with a model law to facilitate such a move and bring about uniformity in national laws covering cyber jurisdiction" (Kush, 2017, p. 102). Looking ahead, we can see this as part of global approaches to solving jurisdictional problems, which often focus on the UN and the legal framework proposed at this universal level of regulation.

The complexity of fighting this type of crime in today's world and the effectiveness of the potential legal framework reflect the key challenges of the digital age. In particular, a new threat, potentially having a global

dimension, is advanced tools and automation that have filled the gap with the lack of highly qualified specialists needed for unpunished cyber hacking and invasions. Therefore, today in order to exploit the vulnerability of digital tools only other digital tools are needed, not information technology professionals. In a review of new directions in cybercrimes research Adam M. Bossler and Tamar Berenblum (2019) emphasize that the focus of cybercrime research today has shifted to examining whether the theoretical causes and correlations of traditional crimes are equally applicable to cybercrimes. Markus Riek and Rainer Böhme (2018) highlight the difficulty of estimating the costs of cybercrimes, also because they are designed to track attack trends, not impact. Often, theoretical constructs are useless when applied to cybercrime because: (i) it is a special type of crime based on the use of digital tools; (ii) it is cross-border and/or related to information impacts in cyberspace; and (iii) it fully meets the characteristics of unpredictability and uncertainty of development that we see in the digital era.

Returning to the theses about direct and indirect harm, difficult-to-predict and long-term consequences from activities carried out or mediated online, all possible approaches to potential problem solving should be considered.

VI. THE SCENARIOS FOR SOLVING JURISDICTIONAL ISSUES

Scenarios for solving jurisdictional and cross-border problems in the digital age look rather abstract, they contain calls for greater independence and, at the same time, cooperation of all parties.

Part of the responsibility is proposed to be shifted to those who use cyberspace resources. In particular, it is proposed to put forward demands to the cyber-community, which "as a whole should become more responsible for monitoring what is being proliferated over the system" (Gilden, 2000, p. 159). This meets the hopes for autonomous regulation, self-regulation of cyberspace and interactions mediated by digital tools.

According to Michael Gilden (2000), "efforts must be made to continue: (i) creating uniform international laws pertaining to the Internet; (ii) increase self-regulation by hosts and users; and (iii) better educate law makers of how the Internet and World Wide Web function" (p. 160). As the difficulties of managing the online space have become systemic and since we know that tensions will most likely grow, it is noted that such tools should continue to be used: "multilateral efforts, bilateral agreements, and informal interactions between public and private actors across borders" (La Chapelle & Fehlinger, 2016, p. 10). In any case, what we call cyberspace is

becoming increasingly dependent on shared resources and efforts, acquires a global structure and a ubiquitous character, and therefore will require flexible regulation and fruitful interaction. In addition to legal solutions, to successfully address threats to human rights, the values of democracy and the rule of law, and any wrongdoing, we will need political solutions and educational efforts.

The approaches to solving jurisdictional problems in the digital age could be roughly divided into global, fragmented and national. Global approaches focus on the idea that a single legal framework and a universal mechanism are possible. An example would be attempts to regulate cyberspace at the UN level. In particular, Ma Xinmin (2016) proposes the UN-centric approach as the core governance model in the global cyberspace, because "cyberspace is a *sui generis* domain, with dual characteristics of reality and virtuality and also dual attributes of sovereignty and global commons" (p. 125). In the long run, it would be great to have a common understanding of the fundamentals that are important in the digital age. However, it is incredibly difficult to come to new working mechanisms at the UN level in the conditions of super-rapid development of technologies, on the one hand, and opposing interests of many influential actors, on the other.

Fragmented approaches partly take into account the possibility of a single legal framework (or a set of agreements) and rely mainly on regional mechanisms. Such approaches imply mutual cooperation, which can be based on political, economic interests, cultural ties and geographic location. The collapse of regulation initiatives of cyberspace at the UN level, as Anders Henriksen (2019) rightly notes, is likely to lead to a shift away from ambitious global initiatives towards regional agreements between "like-minded states" and, at the same time, to the emergence of a fragmented international normative structure on information and communication technology. Fragmented approaches may imply a somewhat forced cooperation, as parties understand that the formation of universal international legal mechanisms and global agreement has never been easy or quick.

National approaches hold on to the idea that each legal system is capable of providing an effective response to the threats of the digital age and, accordingly, shaping the legislative framework and judicial practice. However, the vulnerability of these approaches lies not only in the different degrees of development of national legal systems and differing technological power of states, but also in the fact that inventing a unique adapter for a charger, if it connects perfectly to the standard ports of the device, is inappropriate. Some universalization in the digital age is inevitable, including the universalization of law in connection with the regulation of the use of information technology and activities in cyberspace.

It should be said that none of the approaches prevails—they all have pros and cons, are burdened not only by legal and ethical considerations, but also cannot be translated into reality without revision on the go, which is primarily due to very fast and unpredictable development of technologies.

So far, the regulation and application of law in relation to the use of information technology and activities in cyberspace resemble a careful balancing act. For instance, the European Union's data protection regulation, at first glance, has a distinctly extra-territorial nature in relation to the right to be forgotten. But the decision in the case "Google LLC, successor in law to Google Inc. v. Commission Nationale de l'Informatique et des Libertés" (Court of Justice of the European Union, 2019) on the inapplicability of this right outside European jurisdiction clearly shows that this is not the case.

Many disputes with a jurisdictional component promise to be sharp, but in reality, they end in nothing. An illustrative example of a decision without a decision is the case of "United States v. Microsoft Corp" (Supreme Court of the United States, 2018), known as Microsoft's email privacy dispute, which was expected to redefine some jurisdictional issues. The controversy arose around the use of data in cloud storage and, in particular, its transfer abroad. During the consideration of the case by the Supreme Court of the United States, 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, which is vital for both parties—the state and the corporation—was not resolved substantively, and the trial was dropped.

These same cloud storage facilities may involve storing sensitive medical data overseas. Side by side, even if a powerful corporation, possessing technological and economic resources, cannot always ensure the security of data constituting a trade secret, the resources of the public health sectors can be much more vulnerable. That being said, cyber interference in life support systems can have immediate dire consequences. Moreover, in a connected globalized world, everything can hit everyone, as the fresh lesson of the COVID-19 pandemic has shown.

Therefore, regardless of the approaches used, the efforts of all parties should be aimed at preventing and mitigating the negative consequences of the activities of subjects of law in the digital era. First of all, we are talking about activities that take place in cyberspace or are closely related to the use of information technologies. Discussion of strategies and the development of specific recommendations for prevention and mitigation of consequences can be the subject of further research in this area.

VII. CONCLUSIONS

1. Thus, jurisdictional issues, such as cybercrime, resolving the interrelation between international and national jurisdictions, cross-border activities and extraterritorial consequences, bringing both natural and legal persons to legal liability, in the digital era are becoming a matter of special jurisdictional interest at the international level as the negative impact. This is due to the contradictory application of traditional law that has not contemplated the world-wide technological advance existing at the present time.

2. The other factor are the peculiarities of the activities of subjects of law in cyberspace or the close connection of such activities with the use of information technologies and digital tools. Direct and indirect harmful influences today have an all-encompassing and unpredictable effect, and the degree of negative consequences may increase due to the global nature of the online environment and the general interconnectedness of the world, as well as the redistribution of the influence of state and non-state actors. A human rights-based approach and an associated universal legal framework can provide a basis for resolving existing and potential conflicts.

3. Regardless of the type of scenario for solving jurisdictional problems based on approaches: (i) global (focuses on the idea that a single worldwide legal framework and a universal regulation mechanism are possible); (ii) fragmented (partly considers the possibility of a single legal framework (or a set of agreements) and rely mainly on regional mechanisms); and (iii) national (each legal system is capable of providing an effective response to the threats of the digital age and aligns its legislation and judicial practice with the latter).

4. The efforts of stakeholders should be focused on preventing and mitigating the negative consequences the activities of subjects of law, considering the trends towards the proliferation of the digital environment.

REFERENCES

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

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

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

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

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

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

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-phrg-2017-2-4

Court of Justice of the European Union (2019). Case "Google LLC, successor in law to Google Inc. v. Commission Nationale de l'Informatique et des Libertés", Judgment of the Court of Justice of the European Union (Grand Chamber) of 24-IX-2019, C-507/17, ECLI:EU:C:2019:772.

European Court of Human Rights (2003). Case "Garaudy v. France", Decision of the European Court of Human Rights, nº 65831/01, ECHR 2003IX.

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

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

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

Jiménez, W. G. (2015). Rules for Offline and Online in Determining Internet Jurisdiction. Global Overview and Colombian cases. *International Law, Revista Colombiana de Derecho Internacional*, *26*, 13-62. DOI: http://dx.doi.org/10.11144/Javeriana.ill5-26.rood

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

Kush, K. (2017). Emergence of Cyber Crimes: A Challenge for the New Millennium. *Bharati Law Review*, 2017 (2), 86-103.

La Chapelle, B., & Fehlinger, P. (2016). Jurisdiction on the Internet: How to Move Beyond the Legal Arms Race. *CyFy Journal*, *3*, 8-14.

Mačák, K. (2017). From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law. *9th International Conference on Cyber Conflict*, 1-14. DOI: 10.23919/CYCON.2017.8240333.

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

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

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

Moskowitz, S. (2017). *Cybercrime and Business: Strategies for Global Corporate Security*. Butterworth-Heinemann.

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.

Pathak, J. P. (2016). Digital Age 2.0 and Its Challenges on Media Ethics. *Journal of Humanities and Social Science*, *21* (1), 18-24. DOI: 10.9790/0837-21111824

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

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and International Humanitarian Law: A review of Obstacles in Applying International Law Rules in Cyber Warfare. *Information & Computer Security*, *24* (1), 38-52. DOI: https://doi.org/10.1108/ICS-12-2014-0081

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.

Riek, M. & Böhme, R. (2018). The Costs of Consumer-Facing Cybercrime: An Empirical Exploration of Measurement Issues and Estimates. *Journal of Cybersecurity*, *4* (1). DOI: https://doi.org/10.1093/cybsec/tyy004

Supreme Court of the United States (2011). Case "Snyder v. Phelps", Decision of the Supreme Court of the United States, 2-III-2011, 562 US 443.

Supreme Court of the United States (2018). Case "United States v. Microsoft Corp.", Appeal to the Supreme Court of the United States, 584 US__, 138 S. Ct. 1186.

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

United States Court of Appeals for the 9th Circuit (2006). Case "Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme", Declaratory Judgment of 12-1-2006, 433 F.3d 1199.

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

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/S2377740016500068