Ius Humani
Revista de Derecho. Vol. 10 (II) (2021), pp. 87-100. ISSN: 1390-440X — eISSN: 1390-7794
Recepción: 24-10-2021. Aceptación: 4-12-2021. Publicación electrónica: 8-12-2021
https://doi.org/10.31207/ih.v10i2.288

EXPERIENCING PERSONAL DATA PROTECTION ON THE INTERNET AND ITS POSSIBILITIES OF RECOGNITION AND ENFORCEMENT IN UKRAINE

EXPERIMENTANDO LA PROTECCIÓN DE DATOS PERSONALES EN INTERNET Y SUS POSIBILIDADES DE RECONOCIMIENTO Y EJECUCIÓN EN UCRANIA

Petro Melnyk[*]
Oleksii Volodymirovich Kostenko[**]
Hanna Oleksandrivna Blinova[***]
Iryna Igorivna Shynkarenko[****]

Abstract: The purpose of this article is to find the most successful ways, forms and methods of personal data protection on the Internet among foreign countries for domestic political and legal realities. The following methods were used in the article: dialectical, logical-semantic, comparative-legal, documentary analysis, analytical, information-analytical. Issues related to the adaptation of the successful experience of a number of developed countries in the field of personal data protection on the Internet are brought up for discussion. Some options are covered and specified, which include effective methods and ways to implement an effective mechanism for

[*] Candidate of Law. Associate Professor. Deputy Director of the Kyiv Institute of Intellectual Property and Law of the National University «Odesa Law Academy» (Kiev, Ukraine). https://orcid.org/0000-0003-1928-9660. melnyk.petro@gmail.com
[**] Ph.D. Head of the Research Laboratory of Theory and Law of Digital Transformations of the Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine (Kiev, Ukraine). https://orcid.org/0000-0002-2131-0281. antizuk@gmail.com
[***] Doctor of Jurisprudence. Professor of the Department of Administrative Law, Process and Administrative Activity of Dnipropetrovsk State University of Internal Affairs (Dnipro, Ukraine). https://orcid.org/0000-0002-3320-585X. blinovahanna@i.ua
[****] Candidate of Jurisprudence. Associate Professor of the Department of Operative Investigative Activity and Crimes Investigation of the Kharkiv National University of Internal Affairs (Kharkiv, Ukraine). https://orcid.org/0000-0001-7136-3333. i_shinkarenko@ukr.net

personal data protection on the Internet in Ukraine. It is emphasized that the protection and proper confidentiality of personal data of individuals is one of the key tasks currently facing modern jurists. It is also added that the nature and specifics of the use and protection of personal data of individuals, including on the Internet, are extremely closely related to the institution of intellectual property. Emphasis is placed on the fact that the level of protection of personal data of individuals in a country is an indicator of the extent to which such a state meets the criteria of freedom, democracy, and the rule of law.

Keywords: Personal Data, Private Property, Legal Regulation, Confidential Information, Intellectual Property

---

Resumen: *El propósito de este artículo es encontrar las formas y métodos más exitosos de protección de datos personales en Internet entre países extranjeros en cuanto a sus realidades políticas y legales nacionales. En el artículo se utilizaron los siguientes métodos: dialéctico, lógico-semántico, comparativo-legal, análisis documental, analítico y de análisis informático. Se plantean para el debate cuestiones relacionadas con la adaptación de la experiencia exitosa de varios países desarrollados en el campo de la protección de datos personales en Internet. Algunas opciones están cubiertas y especificadas, incluyendo métodos y formas de implementar un mecanismo efectivo para la protección de datos personales en Internet en Ucrania. Se destaca que la protección y la debida confidencialidad de los datos personales es una de las tareas clave a las que se enfrentan actualmente los juristas modernos. También se agrega que la naturaleza y los detalles del uso y la protección de los datos personales, incluso en Internet, están extremadamente relacionados con la institución de la propiedad intelectual. Se hace hincapié en el hecho de que el nivel de protección de los datos personales en un país es un indicador del grado en que dicho Estado cumple los criterios de libertad, democracia y Estado de Derecho.*

Palabras clave: *Datos personales, propiedad privada, regulación legal, información confidencial, propiedad intelectual*

I. INTRODUCTION

The application of modern information and communication technologies is an indispensable factor in improving public safety. At the same time, the development of modern information and communication technologies has acted the complexity of security risks posed by such systems. On the other hand, citizens rightly expect an adequate response and protection mechanism from modern forms of endangering public safety and legally recognized freedoms and rights of citizens. Bearing this in mind, the basic task is to engage all the necessary resources starting from the collection of data and information, through assessment, processing and analysis. If such an answer is not forthcoming, we risk the trust of the citizens and the foundations of democracy itself. The challenge is great, because modern forms of endangering public safety are constantly changing, especially due to the accelerated development of information technology and means of communication **(**Gligorijević, *et al.*, 2020).

In modern realities, which govern the entire world community, it is impossible not to mention the importance of proper protection and confidentiality of the private sphere of people's lives. In particular, it concerns the personal data protection on the Internet, as it is well known that in the XXI century, which is rightly called "information", control over information, the ways of its collection and dissemination are a powerful element of political and economic influence.

Internet penetration in Ukraine annually increases by an average of 5%. In 2015, the figure was 49%. As of February 2016, 63% of households (excluding Crimea) are connected to the Internet in Ukraine. Regularly, once a month or more, 62% of families use the Internet (Chaikovska, 2016). According to the results of 2018, the number of Internet users in Ukraine is 70% of Ukrainians (compared to 63% as of December 2017). Factum Group research company claims that the number of Internet users in Ukraine reached 73% of the total number of Ukrainians in 2019, and the number of regular Internet users at the beginning of the 4th quarter 2019 was 22.96 million (Dubinskiy, 2019; Shymon, *et al.*, 2020).

The issues outlined in this article are quite deep and not fully explored. It is recognized that the study and substantive analysis of the nature and characteristic features of the processes associated with the proper respect for the safety and confidentiality of personal data of individuals on the Internet, should remain relevant for domestic and foreign scientific community. The issue of personal data protection on the Internet is available around the world. Thus, for example, an estimated 26 million American citizens per

year have been victims of an identity-based crime (Piquero, *et al.*, 2021). At the same time, it should be noted that in the developed countries of the West, the above processes of personal data protection are developing and improving much more dynamically than in Ukraine. That is why this article will focus on what specific methods and ways to develop the field of compliance and protection of personal data of individuals on the Internet can be adopted and further used in the domestic political and legal sphere.

II. METHODOLOGY

At present, any research should be based on the use of appropriate scientific methods, the application of which makes it possible to achieve the goal, scientifically substantiate the conclusions and propose appropriate solutions to the problem under study. The methodological basis is an interdisciplinary approach, in which the theoretical and methodological component is based on the fundamental provisions of the theory of law. The methodological base includes a set of general and specific methods of scientific knowledge. An objective analysis of the subject became possible due to the use of a complex of methods of general and special scientific knowledge.

In the study with the help of the dialectical method of cognition, as well as the logical-semantic method it was possible to define and reveal such theoretical concepts as "personal data", "personal data protection" and "the use of personal data". The experience of developed countries of the Western democratic world, in particular, such as the United States of America, Canada, Great Britain and the countries of the European Union, is studied using the comparative legal method.

When scientifically substantiating the theoretical conclusions of the author, the method of documentary analysis and the analytical method were used, in particular, it was concluded that the dynamic development of computer and digital technology requires constant supervision by the state in the field of personal data protection on the Internet. The most effective way to do this is to develop programs that make it possible to block pirated sites; identify persons who, using computer programs, interfere with the personal data of other persons, enterprises, organizations, etc.

The information and analytical basis of the scientific research was the legal framework governing relations in the field of personal data protection on the Internet, as well as the scientific achievements of Ukrainian and foreign scientists.

All of these methods are applied in interdependence and interrelationship. It's great and efficient that there exist methods of ensuring effective

protection of user's personal data from the internet, but this method continues to be questionable as they continue to be violations on personal data and services provided by the internet. Most people data are not secured and protected from the ills or criminal invasion of internet criminal. Our main concern here is to guarantee to personal users of the internet that their information and other activities are secured and protected. There is no use of putting in place methods and strategies were user rights and data will continue to be infringed and violated. It is there the responsibility of the State of Ukraine in ensuring the effective protection of personal data of its internet user, since they have the right to their individual privacy. Ensuring and following up the measure used become of prime importance.

III. RESULTS AND DISCUSSION

The democratic countries strictly adhere to the doctrine of privacy and private property, to the most radical approach in China. The settlement of any of the aspects does not mean the solution of the problem in the whole. The matter of its fundamental solution lies in the legal plane, and since organized crime in the context of global digitalization of the world community is becoming increasingly transnational in nature, it is primarily a field of international law. The complete solution of the problem has a complex character and should contain a number of normative and legal acts at the level of international and national law, as well as certain technical measures that ensure the legality of personal data collection procedures used by police in the most modern high-tech, toolmaking, analytical systems (Hnusov, Strukov & Mozhayev, 2021).

The expansion of the Internet and technologies based on it has enabled the development of the digital economy and the emergence of new and innovative business models. The Internet has transformed how goods and services have been produced, delivered and consumed. Using Internet platforms (such as eBay, Alibaba and Google Search) allows consumers to globally search, locate and buy goods from anywhere in the world. Simultaneously with the rapid development of technology, there was a need for regulatory intervention in various area of law, including the Intellectual Property Law. Increasingly diverse ways of using Intellectual Property works on the Internet have contributed to the frequency and extent of their abuse (Maltzer, 2016; Perišić, 2020).

The treatment of personal data of individuals solely in the spirit of the rule of law and on the basis of clear legal regulation is an important step towards the normalization of the functioning of intellectual property. Even

though with all these strategies and measures put in place in ensuring the effective use of personal data on the Internet, it's accessibility and protection has become problematic. Most users of the internet experience violations on their personal data, and this has affected the confidence bestow in the usage of the internet. The question one should be asking here is in verifying how secured the personal data of users of the internet are protecting their personal data. This has been a serious debate and deficiencies affecting users in aspects related to the internet.

It is very important today to understand that the parameter of data openness and accessibility is a fundamental vector for the existence of a modern information society. Open data, in this vein, should be studied from the standpoint of exclusively public information to which government authorities have provided online access to anyone who wishes. That is, the basic aspect is free access. Alternatively, such data can be found on the websites of ministries, various departments, state bodies of the region, cities, state registers, and platforms that have been created by activists and journalists (Shevchenko, *et al.*, 2020).

The Internet, the World Wide Web, and their successors are evolving rapidly into a global digital network, a "cybersphere" interrelating people and their activities through robust, albeit ubiquitous, computers, networks, and intelligent hardware and software. The internet has become an integral part of everyday life across diverse parts of society (Atkins, Duderstadt & Houweling, 2002; Pew Research Center, 2005). The Internet builds a parallel world from conversion of analog practices to new experimental spaces. Dissensus is an intrinsic feature of the cybersphere; difference not identity is its connecting work. Communicative activism potentially renders all practices, rules, and norms of practice controversial. Online activism feeds network change that serves the economic driven interests of the industry. Media oligopolies build out networks to reach audiences through filtering preferences that serve the ends of mass media (Thomas, 2016).

The present unbridled advancement in the field of information and communication technology has resulted in individuals being thrust at a crossroad, where refusing to sacrifice one's privacy would mean the denial of technological benefits. Concern for privacy begins once a child is born into this world where the right to privacy could now be argued needs to be considered as one of the basic human rights similar to other inalienable rights such as the right to life and liberties (Dhali, Zulhuda & Fadhilah, 2021).

Ukraine should definitely take lessons from Western Europe and North America in the development of systems related to the protection and secure storage of personal data. In particular, this can be explained by the fact

that in these countries, such as the United States, the first real steps in world history were taken to create systems and methods of personal data protection.

The United States is considered a "pioneer" in the introduction of confidential processing and storage of personal data on the Internet. Experts argue that the especially serious attitude of American society to the problems and issues, one way or another related to personal data protection, began somewhere in the middle of the XX century.

The prevention of identity theft requires the responsibility, cooperation, and actions of three major groups: individuals, businesses, and government. Individuals have the information that must be protected and need to take care to guard their personally identifiable information (PII). To help them do so, agencies such as the Federal Trade Commission recommend a plethora of preventive measures, such as shredding sensitive documents and regularly reviewing credit reports and credit card statements, which individuals are encouraged to undertake for their own protection (Piquero, *et al.*, 2021).

As we can see, without the effective and stable influence of public authorities and representatives of society (public organizations) on the quality of compliance in the country with all the necessary rules for the treatment of personal data will be considered impossible. In turn, the development of various data confidentiality programs, introduced and successfully operated under the administration of private entities and companies, is a good basis for the emergence of effective and consistent public policy in this area. Therefore, it is extremely important that there is a clear and long-term mutual cooperation (relationship) in society between government agencies, institutions and private commercial and non-commercial firms, as well as civil society organizations.

Experts in the field of cyber protection from the United Kingdom confidently state in their official reports that hacker cyberattacks are currently the most widespread and dangerous threat to the daily operation of servers that work with personal data. British experts emphasize that almost every piece of software of any institution or organization can become a potential target of a cyberattack. For example, according to a British report, in 2017 the computer servers of the United Kingdom National Health Service (NHS) were attacked. In particular, a criminal organization of hackers attacked more than two hundred thousand personal computers of representatives of the health service, which were located directly in the UK and other member countries of the British community.

Security officials, along with British police, found that the criminal computer attack was due to the using of the infamous hacking program «WannaCrypt» by cybercriminals. The criminal result of this attack on NHS

servers was the taking by cybercriminals of passwords and encryption keys of employees, including those in senior positions. As a result, criminals returned their access codes to UK health workers only after receiving significant amounts of money from them. It should be noted that this example is just one of many similar cyber-attacks that take place dozens of times a year.

Given these circumstances, British researchers, in our opinion, have come to the logical conclusion that even in the developed world, which includes the United Kingdom, it is essential to continue reforms and other significant changes. This is somehow related to ensuring the proper and secure day-to-day operation of systems that use personal data of individuals (Appleby Global Group, 2017, pp. 1-5). Such a negative example should serve as a "lesson" for the Ukrainian Government, since recently in our country electronic document management is being introduced more and more often, records in the form of an "electronic queue" and others are being introduced in public and private institutions. Of course, such virtual computer programs require a person to provide their personal data, and therefore must be effectively protected from outside interference. That is why private companies should be more careful about issues and processes related to the transfer (even temporary) of personal data or other information to third parties or organizations. Offshore companies and institutions that offer their services to other legal entities in the field of temporary or long-term storage of certain amounts of information, including personal data of employees of these legal entities, may act as such "third" organizations. Given that, offshore companies are a "tasty" target for illegal attacks by cybercriminals from around the world.

In order to significantly minimize the processes of transferring personal data to offshore companies, British experts suggest that legal entities increase their own scientific and technical potential, raise the general level of high technology in production and try to create a product or provide certain services based on their own capabilities and resources. Regarding the use of high-tech tools and implements, scientists recommend that all institutions, enterprises and organizations, regardless of their form of ownership or field of activity, gradually move to the use of blockchain technology in their daily work. This technology, according to experts, is a powerful tool in countering financial and computer crimes and fraud. It is clear that along with the introduction within the country of a number of the latest technological advances, steps should also be taken to ensure a proper law enforcement system, which should act to prevent hackers, cybercriminals, etc.

Nowadays, it is no less important to establish a proper regime of legal regulation in the country, which will ensure the effective storage of confidential information and personal data. To do that, it is necessary that the legislative body of state power (in Ukraine it is the Verkhovna Rada), adopt a number of legal acts that would adequately ensure effective and efficient legal regulation in the field of protection and promotion of personal data, including the Internet. In this context, both domestic and foreign legal experts point out that without a reliable system (mechanism) in a particular state of clear and unambiguous legal regulation of compliance with international standards and requirements to ensure the protection of personal data, it will be impossible.

A number of statements made by jurists and experts in cybernetics and computer technology from many developed countries should be identified as a separate point of view on this issue. This refers to the fact that the legal (legislative) regulation of such a specific and dynamic sphere of public relations as cybernetics, should be carried out exclusively at the national level, that is, at the State level. Instead, all other types of legal regulation, such as local or regional, are considered ineffective or even harmful. If such legal regulation is carried out by each region or each municipality separately, it will of course significantly slow down the quality and efficiency of public relations in the field of personal data protection on the Internet. It will also significantly harm both the development of computer technology and the development of the economy of a particular city, region or country as a whole. It is based on these logical statements; we note that regulation should take place at the State level.

III.1. The Necessity and Essence of Acquiring an Efficient Internet Platform in Ukraine

Developed and democratic states with true rule of law continue to be leaders and role models for other countries in further improving and developing the norms and principles of international law in the field of proper confidential treatment and protection of personal data on the Internet. To ensure the effectiveness of these processes, it is recommended that economically, culturally and politically developed countries help less developed countries to improve the efficiency of their state mechanism, as well as to create clearer, transparent and unambiguous legislation. In addition, it is appropriate for states to act together in an effort to improve the effectiveness of international legal norms and institutions, as it is known that the development of the Internet and computer technology is dynamic.

Considering the above opinion more broadly, we can argue that today the Internet is such that it is developing extremely rapidly (faster than other spheres of public life). Moreover, the peculiarity of the phenomenon of the Internet is that it is not only quite rapid, dynamic and rapidly evolving, but also significantly helps to progress and develop all other spheres of public life. In particular, the Internet and high technology have become an advanced part of societal progress. Therefore, through the rapid nature of the above phenomena, it can be noted that they should be subject to clear legal regulation.

State control over the relevance of national legislation in the field of personal data protection on the Internet should not be carried out through the creation of any new bodies or state commissions, while "inflating" the bureaucracy and creating an additional burden on the domestic state budget and government mechanisms. A much more useful solution may be the introduction of simplified procedures for changing or correcting the existing regulatory legal acts governing public relations in the field of personal data protection, as well as simplified and rapid procedures for the development and adoption of new legal acts.

We completely agree with this way of thinking, because it is clear that in the context of considering this issue there are two sides to a common problem. On the one hand, such a powerful and influential branch of public life as the Internet and the high-tech sector cannot be left unregulated by law (Kittichaisaree & Kuner, 2015, pp. 2-4). On the other hand, it can be argued that excessive legal regulation in this area or its slow introduction and implementation can significantly harm the whole mechanism of proper protection of private personal data, for example, artificially slowing down the natural dynamics of their development and functioning.

Economically developed countries should be considered as priority countries for cooperation and mutually effective exchange of experience and practical successful examples of work. This is explained by the fact that they have a high level of political and social culture, as well as have in their territory stable state institutions of power, which demonstrate their own stable efficiency for many years or even centuries (United Nations, 2013, Resolution No. 68/167). To date, several Western countries are subject to the characteristic requirements outlined above. In particular, among them the United States as the leading "superpower" of the modern world, which has the world's greatest influence and weight in politics, economics, culture, education and scientific and technological progress. Also, among the countries with which Ukraine can carry out fruitful cooperation, it is necessary to add the Member States of the European Union, which are extremely close to Ukraine in terms of common family, political and cultural values.

As is known, these countries follow the same principles and approaches in terms of protecting the privacy of every person as a subject of public relations. It is on the basis of these beliefs and convictions of Americans and representatives of Western European countries in the inviolability of property rights of each person, in respect for the confidentiality of their private life in general, as well as for certain, separate parts of confidential information about these persons or their lives, the appropriate legal regulation is formed.

III.2. Legislation of Ukraine on Personal Data Protection, Including on the Internet

It will be important to emphasize that the general content of legal regulation of personal data protection is based on such well-known international documents as the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966. The current legislation of Ukraine has been developed taking into account the requirements of these international documents, as they have been ratified by the Ukrainian Government (Verkhovna Rada) and are therefore binding. At present, the legislation on personal data protection consists of the Constitution of Ukraine, the Law of Ukraine "On Personal Data Protection", other laws and by-laws, international treaties of Ukraine which were approved as binding by the Verkhovna Rada of Ukraine.

The Member States of the European Economic Area, as well as the states that have signed the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, are recognized as ensuring an adequate level of protection of personal data.

Current regulations in the field of personal data protection regulate legal relations related to the protection and processing of personal data and are aimed at protecting fundamental human and civil rights and freedoms, in particular the right to privacy, in connection with the processing of personal data. The current legislation applies to the processing of personal data, which is carried out in whole or in part using automated means, as well as to the processing of personal data contained in the file or are subject to entering into the file, using non-automated means. If an international treaty of Ukraine, approved by the Verkhovna Rada of Ukraine, establishes rules other than those provided by the legislation of Ukraine, the rules of the international treaty of Ukraine shall be applied.

According to Art. 2 of the Law of Ukraine "On Personal Data Protection", personal data is defined as "information or aggregate information about a natural person who is identified or may be identified".

Meanwhile, in accordance with Part 1 of Art. 5 of this Law, personal data relating to the exercise by a person authorized to perform the functions of state or local government, official or service powers is not confidential information.

In our opinion, such a legislative interpretation of this concept is somewhat narrowed, as it includes only an indication of an individual, while neglecting the legal entity. At the same time, the owner of personal data may be both an individual and a legal entity, which determines the purpose of personal data processing, establishes the composition of these data and the procedures for their processing, unless otherwise provided by law. In addition, the legislator unjustifiably narrowed the concept of a subject of personal data, understanding it only as an individual whose personal data is processed. However, personal data of an individual can also be processed, as evidenced by the fact that nowadays all tax reports are submitted in electronic form, and for the current year of their activity, business entities submit appropriate declarations, which can be found in the public domain on the Internet.

The procedure for access of third parties to personal data possessed by the public information manager is determined by the Law of Ukraine "On Access to Public Information", except for data received from other bodies by the central executive body that ensures the formation and implementation of state financial and budgetary policy during the verification and monitoring of state payments.

It should be pointed out that the nature and content of legal norms protecting the confidentiality of personal data of individuals and their proper treatment are closely related to the institution of private property. In our opinion, this state of affairs can be explained by the fact that the personal data of individuals, as well as specific information about them, is their exclusive personal value, and therefore must be properly protected. The obtaining of personal data of individuals should be understood as a direct unlawful encroachment on personal freedoms, rights and interests of a person. It's a beautiful scenario that the country has put in place and enacted credible laws and legislation in ensuring the security and accessibility of its internet usage in depriving the violations of personal data rights. This is beautiful and laudable in all its initiation. The problem will be posing here is as to what use will this legislation be if effective methods and measures are not used to ensure its enforcement and application. It is one thing in enacting laws, and the other in ensuring it's application. The State of Ukraine can be credited in all its efforts in guaranteeing personal user's data, but more efforts still need to be done as this issue of internet crackers and hackers continues to be a serious threat affecting not only particular persons, but the entire Ukrainian system.

IV. CONCLUSIONS

1. The study showed that the nature and content of the processes of protection and proper provision of personal data on the Internet are closely linked with the institution of private property, as well as in general with the private part of life of individuals. However, there are some exceptions in this context, for example, some of the personal data is information that is socially important.

2. Given the many unique features of the Internet, as well as related computer and high-tech areas, the legal regulation of this area of public life is a difficult and responsible matter. In particular, the legal protection of personal data on the Internet should be carried out with the help of special "simplified" procedures for amending and adopting new legal acts. Instead, the creation of additional bodies or agencies to oversee the use of personal data of individuals is considered unnecessary and creates an excessive burden on the state system and budget.

3. The United States and the European Union Member States are the best role models for Ukraine in the field of proper protection and ensuring the confidentiality of personal data on the Internet, as these countries have common values regarding the priority of human rights, freedoms and interests of the individual over the State, as well as developed means of successful protection of these values.

REFERENCES

Appleby Global Group (2017). *Protecting Personal Data from Cyber-Attacks*. Appleby Global Group Services Limited.

Atkins, D. E., Duderstadt, J. J., & Houweling, D. V. (2002). *Higher Education in the Digital Age: Technology, Issues and Strategies for American Colleges and Universities*. Greenwood Press.

Chaikovska, V. P. (2016). E-Commerce in Ukraine: Current State and Trends. *Intelligence XXI*, *3*, 38-48.

Dhali, M., Zulhuda, S., & Fadhilah, S. (2021). The Digital Economy and the Quest for Privacy Protection in Bangladesh: A Comparative Legal Analysis. *IIUM Law Journal*, *28* (2), 567-596. Doi: https://doi.org/10.31436/iiumlj.v28i2.451

Dubinskiy, I. (11-X-2019). Internet Penetration in Ukraine: Research Methodology. *Factum Group*. https://bit.ly/3rznGjf

Gligorijević, M., Pećanac, M., Vulević, O., & Maksimović, A. **(**2020). Analysis of Aspects of Personal Data Protection Risk Assessment Using Modern Technologies in the Ministry of Internal Affairs. *International Scientific*

Conference "Archibald Reiss Days": Thematic Conference Proceedings of International Significance, *10* (1), 593-603.

Goodnight, G. T. (2016). Argumentation and the Cybersphere. In Ron von Burg (Ed.), *Windsor Studies in Argumentation* [Vol. III]. University of Windsor.

Hnusov, Y. V., Strukov, V. M., & Mozhayev, O. O. (2021). Problem of Harmonization of Legal Norms with the Needs of Police Investigations by Using High-Tech Instruments for Searching Information. *Law and Safety*, *80* (1), 78-85. Doi: https://doi.org/10.32631/pb.2021.1.11

Kittichaisaree, K., & Kuner, C. (14-X-2015). The Growing Importance of Data Protection in Public International Law. *Blog of the European Journal of International Law*. https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/

Meltzer, J. P. (2016). *Maximizing the Opportunities of the Internet for International Trade. E15 Expert Group on the Digital Economy - Policy Options Paper. E15 Initiative*. International Centre for Trade and Sustainable Development (ICTSD) & World Economic Forum.

Perišić, J. Ć. (2020). The Sale of Counterfeit Goods Via the Internet as a Contemporary Security Challenge – Legal Aspects. *International Scientific Conference "Archibald Reiss Days": Thematic Conference Proceedings of International Significance*, *10* (1), 195-203.

Pew Research Center (2005). *Internet: The Mainstreaming of Online Life*. http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf

Piquero, N. L., Piquero, A. R., Gies, S., Green, B., Bobnis, A., & Velasquez, E. (2021). Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders. *Victims & Offenders*, *16* (3), 444-463. Doi: 10.1080/15564886.2020.1826023.

Shevchenko, V., Dosenko, A., Iuksel, G., Synowiec, A., & Valentyna, D. (2020). Use of Open Data in Ukraine: Some Important Aspects. *Revista San Gregorio*, *42*, 319-329. Doi: http://dx.doi.org/10.36097/rsan.v1i42.1564

Shymon, S., Baliuk, I., Kykot, P., Shatalova, L., & Harust, Y. (2020). Administrative and Legal Bases of Consumer Rights Protection on the Internet. *Gênero e Direito*, *9* (5), 72-92.

United Nations (1948). *Universal Declaration of Human Rights*. United Nations General Assembly Resolution 217A (III).

United Nations (1966). *International Covenant on Civil and Political Rights*. United Nations General Assembly Resolution 2200A (XXI).

United Nations (2013). *The Right to Privacy in the Digital Age*. United Nations High Commissioner for Human Rights.