ISSN : 1984 - 9729

The Law, State and Telecommunications Review

Volume No. 16

Issue No. 1

January - April 2024

ENRICHEDPUBLICATIONSPVT.LTD

S-9,IIndFLOOR,MLUPOCKET,
MANISHABHINAVPLAZA-II,ABOVEFEDERALBANK,
PLOTNO-5,SECTOR-5,DWARKA,NEWDELHI,INDIA-110075,
PHONE:-+(91)-(11)-47026006

ISSN : 1984 - 9729

The Law, State and Telecommunications Review

Aims and Scope

The Law, State and Telecommunications Review publishes two annual issues released on May and October since 2018 and one annual issue released on May uninterruptedly since May 2009. The journal mission is to publish legal and interdisciplinary analyses on telecommunications and communications focused on policy and regulation of communications services, telecommunications services, Internet-based services and rights, such as the right to communicate, to publish, to private exchange, to design communication platforms, and other related topics, such as privacy, intellectual property, universal access, convergence, satellite and spectrum regulation, telecommunication licensing and regulatory design, independent agencies, deregulation, e-commerce, big data, net neutrality, and so forth, with emphasis on national and foreign experiences through the lenses of legal and regulatory theories. It accepts submissions in English, Spanish, and Portuguese. It does not charge for processing, submission, or publishing the articles. Authors are allowed to hold the copyright of their paper without restrictions. We welcome paper submissions all year round. They will undergo rigorous peer review process by anonymous refereeing of independent expert referees. The Law, State and Telecommunications Review is a journal maintained by the University of Brasilia and edited by the Telecommunications Law Research Group of the School of Law Center on Law and Regulation. The journal adopts structured abstracts with clear indication of purpose, methodology/approach/design, findings, practical implications, and originality/value of the papers. Keywords should depict the actual content of the article and be limited to five, according to the ABNT NBR 6028 standard. The journal adopts the ABNT NBR (Brazilian Association of Technical Standards) citation

The main goal of the University of Brasilia Law, State, and Telecommunications Review is to put together high quality legal analyzes and interdisciplinary research on telecommunications focused on regulation, technology, policy and legal framework. We invite authors to submit papers on any relevant topic related to telecommunications policy and regulation, such as but not limited to infrastructure, broadband, broadcast, telecommunication services, universalization, interconnection, consumer rights, privacy, right to communicate, and Internet. We also accept papers focused on telecommunications regulatory approach from the viewpoint of environmental law, antitrust law, labor law, tax law, consumer protection and urban law.

ISSN : 1984 - 9729

ISSN : 1984 - 9729

The Law, State and Telecommunications Review

(Volume No. 16, Issue No.1, January - April 2024)

Contents

Legal Regulation of Electronic Money Turnover: Global Trends

Kamshat T. Raiymbergenova*Gulnar T. AigarinovaSaltanat K. Atakhanova***Bakhytzhan Zh. Saparov****Makhabbat K. Nakisheva*****

A B S T R A C T

[Purpose] *To analyse the existing trends in the turnover of electronic money, and their relationship with the conventional cash turnover on the territory of the Eurasian Economic Union (EEU), in particular, in the legal system of the Republic of Kazakhstan (RK).*

[Methodology/Approach/Design] *Deduction, content analysis, comparative analysis, and other general and special research methods were used.*

[Findings] *As a result, the existing problems in the functioning of the type of money considered in this study were analysed. The study includes recommended measures to introduce amendments to legislation aimed at removing barriers to the functioning and circulation of electronic money, which will benefit the economic system of the given state.*

[Practical Implications] *The information presented in this article can be useful material for representatives of public authorities in the implementation of reforms to modernise the economic system, for a wide range of readers interested in the development of digital technologies and their impact on the commercial activities of subjects of the economic life of society.*

Keywords: Currency. Payment System. Economy. Financial Organisation. Bank.

INTRODUCTION

Electronic money is a de facto prepaid payment product, which is positioned as a payment service with limited functions. Electronic money performs many functions, namely: this type of money acts as a starting financial product for people who previously had no access to financial services; electronic money is needed to increase the availability of financial services due to a lower entry threshold (that is, reduced requirements for customer identification and their level of financial literacy); it performs the role of infrastructure and is the basis for other innovative projects, which include, for example, the issuance of cards (banking or transport), and online lending (NEKHAICHUK et al., 2019; POIER et al., 2022).

Electronic money can be characterised as a relatively new phenomenon present in the financial market. The consequence of this is the fact that the supervision of their turnover is still in the process of development. The above can be evidenced, for example, by the fact that there is no single, generally accepted definition of the phenomenon considered in the article, namely electronic money. Nevertheless, in modern conditions, the role of this type of money is becoming increasingly important

since it is one of the unique forms of money evolution in the digital economy (PANOVA, 2018; PATASHKOVA et al., 2021). Based on the results of examining the information scope from various studies, it can be stated that, in the scientific literature, the issue of electronic money has been considered sufficiently. Notably, the previous studies were aimed at considering the purely technical aspects of the functioning of electronic money, while the aspects of legislative, and legal regulation of electronic money were not fully covered. Furthermore, a more detailed consideration of the history of the development and legislative consolidation of the functioning of this type of money in the context of the Eurasian Economic Union (EAEU), in particular in the legal system of the Republic of Kazakhstan (RK) has not been conducted (AYUDYA and WIDOWO, 2018; VOZNIUK et al., 2020).

To address these shortcomings, within the framework of this study, the main emphasis is placed on the analysis of the role of electronic money in the EAEU member states, in particular, the history of the development, functioning, and legislative consolidation of electronic money in the Republic of Kazakhstan will be covered. The theoretical consideration of the studied phenomenon is also included, identifying the most important and key features of electronic money circulation, and correlating it with classical, cash circulation. In the course of transferring the analysis to the state level, the regulatory framework of the Republic of Kazakhstan is considered in the framework of the study, in particular, specific laws regulating the sphere of functioning of electronic money systems are provided. Furthermore, the study identifies reasons for the insufficient distribution of this type of money in the Republic of Kazakhstan, based on which practical recommendations will be developed for the introduction of many adjustments to the current Kazakh legislation and the economic policy of the state to provide wider opportunities for the functioning of electronic payment systems. The above will increase the activity in the field of online commerce, resulting in the improvement of the economy and the creation of a more developed economic system (LASME and MAKOTO, 2020; SARSEMBAYEV, 2021; BLAHUTA et al., 2019).

The purpose of the article is to analyse the existing trends in the turnover of electronic money, and their relationship with the conventional cash turnover on the territory of the Eurasian Economic Union. Firstly, attention will be focused on the Republic of Kazakhstan

MATERIALS AND METHODS

In reviewing the existing and functioning electronic money circulation system on the territory of the Eurasian Economic Union and the territory of the Republic of Kazakhstan, in the development of methodological recommendations for the modernisation of the legislative framework of the republic and its economic policy, many general and special research methods were applied. With the use of a set of methods in this study, it was possible to identify the key provisions that determine the scientific perception of electronic money, to discover the main characteristics of approaches to building regulatory

mechanisms for this type of financial transaction, which is especially important when creating a scientific theoretical, legal foundation on which, in the future, the actions of individual states will be based on, regarding the creation and implementation of national legislation or other mechanisms that will be aimed at preventing and countering crimes that have already been committed in the field of electronic money circulation by certain criminal entities. The development of electronic money in the legislative field was also disclosed, the ratio of classical, cash, and electronic money turnover was considered, the main areas of the development and functioning of the phenomenon considered in the framework of the study were identified, synthetic conclusions were formulated, together with the prospects of further research.

For example, upon using the deduction method, a description of existing, in particular in the legislative system of the Republic of Kazakhstan, adopted, and relevant regulations that introduce electronic payment systems into the legal field was compiled, while the inductive method allowed structuring and generalising the publicly available scope of information directly related to electronic money. It should also be noted that other research methods were used in the course of the study. For example, the use of content analysis in the framework of this study allowed identifying key conclusions regarding the further recommended area of implementation of reforms. The use of comparative analysis allowed identifying the differences in the existing fundamental approaches to the definition of electronic money, considering how to fully fulfil one of the key advantages of the type of money under consideration, namely, very high competitiveness due to the expansion of the number of entities directly connected and interacting with electronic money.

The methodology generalisation used in the framework of this study allowed the creation of the most complete picture, which represents, firstly, modern and relevant features of the functioning of electronic money systems on the territory of the EAEU member states and the territory of the Republic of Kazakhstan, drawing conclusions regarding the prospects for the use of these technologies, formulating effective and usable methods of modernisation of the economic system and financial policy of this state.

This study was conducted in three stages. In the first stage, guided by the scientific literature and the theoretical achievements formulated in it, the issues of the establishment and development of electronic payment systems on a global scale and the scale of the EAEU member states, the main approaches to scientific comprehension and perception of the phenomenon considered in the framework of the study were disclosed. In the second stage, a descriptive characteristic of the currently implemented economic and legal policy regarding electronic money circulation at the national level (in particular, in the Republic of Kazakhstan) is formed, and an analysis of current regulations in this area is also conducted. In the third stage, the recommended measures that, if implemented, can remove barriers to the full functioning of electronic money, which will have a very beneficial effect on the national economy of Kazakhstan are offered.

RESULTS

Money, acting as a payment instrument, determines the development of the economy at the international level and on the scale of a separate state, the society living on its territory. They provide for universal exchange between owners of a variety of goods and services to ensure the operation of the credit and financial systems of the state (WULANDARI et al., 2016). Regarding the history of the development of electronic payment systems at the modern level, the following should be noted. After computers began to gain popularity, the first area of application of new computing power was the conversion of calculations and accounting into electronic format. Interbank settlements, which previously required direct physical transportation of banknotes, are now almost totally carried out electronically. Electronic payment instruments, which include card payments and electronic bank transfers, have gradually replaced cash and paper checks in retail payments, even though paper money is still in large circulation as, in some cases, a convenient means of paying for small-volume settlements and services. In the 1990s, there was a surge in the power of electronic computing machines (computers), moreover, new generations of computer technologies allowed investing in personal computers. The development of the Internet has also created a demand for the exchange of intangible goods and services in electronic form (KOVALENKO and SHERNIN, 2018; BLAHUTA et al., 2020). This trend has led to the emergence of a new payment instrument, namely electronic money.

Despite the relatively recent entry into the daily life of electronic money, the active and dynamic development of this area of economic activity can be observed. The “electronic money” in the framework of this study refers to a variety of payment instruments that are based on innovative technological and digital developments. Currently, it can be stated that there is no single, practically supported, and stable definition of this phenomenon. Regarding the currency, a number of its fundamental features and the duties that it must fulfil can be outlined. Thus, for example, they include the need to make payments (i.e., to facilitate the circulation of the money supply within the state and internationally), to serve as a recognised equivalent of value, and to be used as a unit of account for certain economic transactions (LESKOVA, 2017). It is possible to distinguish two main characteristics inherent directly in electronic money, the presence of which allows asserting that electronic payment systems belong to electronic money. In particular, electronic payment systems are capable of performing the function of money, serving as an alternative to conventional currency instruments, moreover, existing in electronic form, electronic money differs from conventional bank accounts and securities.

An important factor, which, depending on its state, hinders or stimulates the development of electronic money circulation in the state economy, is the technical subsystems and the level of informatisation of the state under consideration. As an opportunity for modernisation, in this case, attention should be paid to the prospects for the implementation of the functions of the international payment system operating on the territory of the EAEU member states (KHACATURYAN, 2016). Even though the functions of the

international payment systems on the territory of different countries and the mechanisms of turnover of the countries of the Eurasian Economic Union are approximately the same, the volume of services provided by the international payment system will depend on the technical capabilities of each country. The lack of high-quality Internet communication in all regions of the Eurasian Economic Union may pose a real threat to the mechanisms considered in the study. It seems that without proper development of electronic interaction channels, it is impossible to ensure acceptable interaction of financial and commercial organisations, their clients, and government agencies within national economic systems or a single integrated platform. Regarding the above, the Kyrgyz development of 2020 deserves consideration. A draft concept for the development of digital payment technologies in the period 2020-2022 has been formed in the Kyrgyz Republic (AMNAZHOLOVA, 2018).

As an opportunity to open prospects for the development of electronic payment system mechanisms, the possibility of using simplified customer identification mechanisms within the state economy should be considered. The absence of these platforms in the EAEU space may limit the number of commercial business enterprises that can be maintained through existing remote service channels. The National Bank, which is the main body and an important part of the national mechanism of circulation of electronic payment systems, is interested in promoting the development of electronic money circulation and payment methods. Considering the above, national regulatory authorities should be interested in stimulating the development of the national economy and, as a result, integrating the mechanisms of circulation of electronic payment systems. It seems that for the effective and safe development and functioning of the digital payment space, coordination measures are required at the level of all participants along with supervision corresponding to the modern technologies by national central banks, which are the main body of the electronic payment system turnover mechanism. On the one hand, it will maintain the stability of the payment system,and protect the rights and interests of consumers, on the other hand, it will contribute to the development and introduction of digital innovations.

DISCUSSION

The imperfect legal framework of the EAEU member states (especially the Central Asian states) in terms of using innovative digital payment technologies and products and the lag in the adoption of regulations for innovative payment technologies and products on the territory of the EAEU member states directly hinder the development of electronic payments (AFANASYEVA, 2020). Therewith, the introduction and improvement of measures aimed at coordinating the elements of the electronic payment system turnover mechanism provide the EAEU member states with additional opportunities for the development of these systems. The low level of use of digital channels by customers should be considered a threat when interacting with the participants of the payment system. This threat is caused by the lack of a high-quality Internet connection and a low level of financial awareness of consumers of

payment services. Thus, despite the presence of certain theoretical developments aimed at modernising the legislative framework in the field of functioning of the phenomenon under consideration, the level of development and use of this tool in such states as Belarus, Kyrgyzstan, Armenia, and Kazakhstan is still at a low level (ABRAMOVA et al., 2020). In addition, the functioning of electronic payment systems should be considered to resolve the existing problem of creating a collective, single currency, which is relevant for the countries of the Eurasian space. All decisions of the financial authorities of these countries emphasise the need to use their national currencies for interaction between the countries of the Eurasian Economic Union. Even though the Eurasian Economic Union is currently working on the introduction of a single currency, the question of which currency should be introduced into the EAEU as a single currency has not yet been resolved. Among the available options, the possibility of using the Russian rouble as the strongest currency in the region is being considered (the alternative is to create a new currency). Thus, international experience shows that the development of electronic payments, especially electronic money, reduces the cost of cash turnover and, as a result, accelerates economic growth. Electronic money can also contribute to the development of new sectors of the economy and e-commerce. However, the development of the electronic money market largely depends on legal supervision (DOSTOV et al., 2020). If the relevant rules are not flexible enough, innovations in the field of electronic payments cannot be implemented at a high level.

With the adoption of the Law of the Republic of Kazakhstan No. 466-IV "On amendments and additions to certain legislative acts of the Republic of Kazakhstan on electronic money issues" (2011), electronic money was recognised at the legislative level as a legal instrument for payments and settlements. Furthermore, this concept was introduced into circulation from the Law of the Republic of Kazakhstan No. 11-VI "On payments and payment systems" (2016). The pioneer of issuing electronic currency in Kazakhstan is the joint-stock company "Eximbank Kazakhstan", which became the first issuer of electronic currency "e-kzt" in 2012, in its activities this bank relies on the Kazakhstan Interbank Settlement Centre of the National Bank of the Republic of Kazakhstan. The introduction of electronic money is aimed at developing alternative methods of non-cash payments. Electronic money, in its essence, is similar to paper money, yet payments are made in a non-cash form. This is how ordinary people perceive electronic money in everyday life. Nevertheless, this does not seem quite correct. Upon analysing the legislative framework, many differences in electronic money can be observed, the most important of which will be discussed below. The first considerable difference between electronic money and paper money is the form of issue. According to Law of the Republic of Kazakhstan No. 11-VI "On payments and payment systems" (2016), the currency of Kazakhstan can exist in cash (in the form of paper money and coins) and in non-cash form (in the form of bank account records), therewith, the type of money in question can exist only in electronic form, not in the form of a bank account record (AYUDYA and WIBOWO, 2018).

Thus, the fundamental difference between electronic money and currency is in the form of existence. The form of non-cash currency is a type of bank account, its concept and exhaustive classification are determined by the legislation of Kazakhstan (DZHAKSYBEKOVA and NAMZHUDINOVA, 2020). Bank accounts cannot be a form of electronic money, that is, an unconditional and irrevocable monetary obligation of electronic money issuer, which is stored in electronic form and accepted by others as a means of payment in electronic money. This is due to many differences between electronic money and paper money, which are a condition for issuing money. For example, according to Law of the Republic of Kazakhstan No. 2155 "On the National Bank of the Republic of Kazakhstan" (1995), the issue of banknotes and coins, the organisation of their circulation, and withdrawal from circulation in the Republic of Kazakhstan is carried out only by the National Bank of the Republic of Kazakhstan. Following the provisions of the legislation of the Republic of Kazakhstan on payments, only second-tier banks can issue electronic money on the territory of the country. The following directly arises from the above-mentioned difference. For example, since the issuer of ordinary currency is the National Bank of the Republic of Kazakhstan, which is an affiliate of the country, the obligations on money issued by the National Bank of the Republic of Kazakhstan are guaranteed by the assets of the National Bank of the Republic of Kazakhstan (ZHIENDINOVA, 2016). Therefore, in any case, the person who owns paper money has the right to make claims to the state under the authority of the National Bank of the Republic of Kazakhstan in respect of this type of money, while the obligations on electronic money are secured solely by the issuer of specified electronic money.

Therefore, the owner of electronic money has the right to make requests only to the issuer of electronic money, including for the redemption of the above type of money. The exception is that if the issuer's functions in the electronic money system are performed by several secondary issuing banks, between which netting agreements have been concluded, then these issuers will be jointly and severally liable for the likely risks. Moreover, in this case, the rules related to the circulation of the corresponding electronic money system and the agreements signed between the issuer and the owner of electronic money should explicitly provide for the possibility of filing a claim against any issuer of the electronic money system. A considerable difference between electronic money and conventional money is in the sphere of circulation, which is why their versatility and turnover possibilities also differ. An ordinary currency is a universal way of paying for certain economic services. Therefore, the owner of a regular currency can use it to pay for any goods or services in Kazakhstan, and the seller (or supplier) will be obliged to accept the specified currency unconditionally. Electronic money is not as universal as paper money since it can only be used to pay for goods and services presented in the electronic money system in circulation. The Law on Payments provides for the possibility of exchanging electronic money for other types of money, but this also does not violate their universality.

According to Law of the Republic of Kazakhstan No. 11-VI "On payments and payment systems"

(2016), the possibility of exchanging electronic money for other electronic money is fixed. However, this does not endow this type of money with universality, since they can be exchanged for electronic money of another system, or they can be used solely to pay for goods and services that are available in a particular system of electronic money circulation. Thus, the electronic currency issued by secondary banks of Kazakhstan is the so-called non-fiduciary currency. According to publicly available information, fiduciary money became widely used after its introduction into scientific circulation at the beginning of the 18th century, in parallel with the Bank of England's issuance of banknotes that were not backed by an equivalent amount of gold. Currently, the term fiat money borrowed from American economists is more commonly used, the meaning of which is determined by the Latin word fiat (that is, decree, order). The literal translation of the word fiat is "let it be done". Currently, most of the national currency is legal tender, including tenge, rouble, United States dollar (USA), euro, and other currencies. In general, a fiduciary currency is a paper currency, and its solvency is determined by national legislation. When the economic and political power of the state falls, and trust in it decreases, the value of such money in this country will change. Its value depends on nominal value – the number indicated on the banknote, while the production price of paper money and coins is much lower than their nominal value (MAKHALINA and MAKHALIN, 2019).

When issuing such money, the state solved two tasks – to minimise the costs of issuing currency symbol carriers, while protecting it from counterfeiting to the fullest degree. There is also non-fiduciary money, an example of which can be modern units of value, widely used in electronic payment systems on the Internet. Notably, states and their institutions are in no way responsible for the obligations of electronic money on the Internet. Another difference between conventional currency and electronic money is that the regulator has special restrictions on the owner of electronic currency, while there is no such function for owners of conventional currencies. Electronic currency can be used only by individuals for settlements, individual entrepreneurs and legal entities can accept it only as payment for goods and services that they provide (in the case of services) or sell (in the case of goods). According to the established rules for the issuance, use,and return of electronic money, and the requirements of issuers of electronic money and electronic money systems in the Republic of Kazakhstan, holders of electronic money are divided into two types: identifiable and unidentifiable. Owners of electronic currencies set restrictions on transactions. Unidentified owners of electronic currencies cannot conduct transactions with electronic currencies, which, in terms of their volume, exceed a hundredfold size of the monthly calculation index set for a particular financial year according to the law of the republican budget (ASHIM and OMAROVA, 2017; GHARAIBEH et al., 2012).

In this case, the issuer is obliged to verify the identity of the specified person following the Law of the Republic of Kazakhstan No. 191-IV "On counteraction of legalisation (laundering) of incomes received by illegal means, and financing of terrorism" (2009). In addition, according to the policy of the

regulatory body, in any case, regardless of how much the owner of electronic money owns, they must be of legal age. Therefore, a person under the age of 18 cannot become the owner of electronic money. To conclude, it should be noted that the legal approaches to control the turnover of electronic money are fundamentally different from the approaches to control regular, classical money circulation. In particular, electronic money is not a universal payment method, there are many restrictions for owners and issuers of electronic money, and legislators impose certain obligations on issuers of electronic money to ensure the safety of the electronic money system. It can be stated that the above factors do not contribute to the widespread use of electronic money in the Republic of Kazakhstan. Nevertheless, with the improvement of the legislative framework and the development of online payments, the use of the type of money considered in the framework of this study as a means of payment for goods and services provided will gradually be able to gain the trust of consumers, gain more popularity than now and have a beneficial effect on the economy of the Republic of Kazakhstan.

Above, there was a discussion of the expansion of the use of electronic money in an integral context, that is, as a means of uniting the economic systems of the EAEU member states based on a single currency. It was confirmed that the development of electronic money should be analysed as a factor that creates additional risks for individuals and the entire financial system of the country. The studies mentioned above have shown that the introduction of electronic money systems in economically highly developed countries took place amid two trends in the development of monetary circulation, namely, the reduction of cash turnover and its subsequent replacement with non-cash payments. Moreover, it is necessary to note the replacement of a cash paper loan with a non-cash loan, and the varieties of the methods of state supervision over electronic money in different countries can be explained by the hope of the management to find the most acceptable solution to the "efficiency/risk" dilemma. Regarding the existing barriers to the full functioning of the turnover of electronic money, many problems can be observed, the elimination of which will entail active development. Notably, the phenomenon considered in the framework of this study should not be considered unique and peculiar to the Kazakh economy exclusively. Firstly, such problems include a low level of trust in electronic money on the part of private consumers and commercial enterprises. Secondly, it is possible to note the existing problems and imperfections of the electronic money systems themselves.

To increase consumer confidence in electronic money and expand its use in Kazakhstan, it is necessary to take a number of the following measures:

(1) It is necessary to supplement the composition of electronic currency issuers with financial organisations that have a license from the National Bank of the Republic of Kazakhstan to use the electronic currency for transactions, since this, undoubtedly, will stimulate competition between issuers and improve the quality of the system and services, which will be facilitated by the spread of electronic money.

(2) In addition to activities for the direct issuance of electronic money, it is necessary to formulate and legislate a list of those operations that can be performed by financial institutions-issuers of electronic money.

(3) It is necessary to carry out minimal, but clear and strict supervision of the issuing institution, which is based on tracking the activities of this type of organisation (namely banks and financial organisations).

(4) It is necessary to increase the transparency of the activities performed by issuers of electronic currencies, for example, to require them to provide a wide range of people with information about the financial condition of the issued electronic currency and the number of obligations assumed, which includes the repayment of electronic money.

(5) To solve the problems arising from the interaction of various electronic money systems, is required to create a single integrator that allows using and accepting electronic money in one system operating in parallel with other systems.

CONCLUSIONS

Electronic money can be characterised as a relatively new phenomenon present in the financial market. The consequence of this is the fact that the supervision of their turnover is still in the process of development. In particular, electronic money considered in the framework of this study is a very promising and actively developing field. Further forecasts regarding the popularisation of the use of this type of finance seem very optimistic, especially considering rapidly developing digital communication technologies and the much higher level of convenience of using electronic money. The consequence of these processes should be considered the growth of online commerce, which will contribute to the development of small and medium-sized businesses, whose activities will have a very favourable and improving effect on the economic system of a particular state, including the economy of the Republic of Kazakhstan considered in the study.

The material offered for review in this article may arouse the interest of specialists in the development of information technologies, for example, to introduce innovations and modern technologies into commercial processes.Furthermore, it will also be of interest to a variety of experts and consultants who, indirectly or personally, influence the decision-making of private or public structures in the field of informatisation of their activities. Notably, many problems were identified during the study. In particular, a very interesting area for further research is to study to what extent different interpretations and definitions of electronic money affect economic processes, and to what extent this factor can influence the growth of this sector in different states. In addition, researchers can focus their attention on further analysis of the generally accepted characteristics of electronic money, which have been considered in this article. In particular, the practical aspect of this issue should be analysed based on unbiased and real statistical information that could illustrate the level of development of the electronic money market in a particular country.

REFERENCES

Abramova, M. A; Dubova, S. Y; Krivoruchko, S. V. (2020). Factors of the development of electronic cash and payment turnover in the EAEU space. Economics, Finance, and Production Management, Vol. 3: 3-13.

Afanasyeva, M. A. (2020). Interstate cooperation of the EAEU countries in the digital economy. Effective Governance: Scientific Almanac in Memory of Professor M. I. Panov, Vol. 1: 29-41.

Amnazholova, B. A. (2018). Legal regulation of cryptocurrency in the world.Education and Law, Vol. 5: 56-69.

Ashim, A. A; Omarova, A. A. (2017). Prospects for the development of the electronic money market: International experience and its use in Kazakhstan. Problems of Science, Vol. 3: 16-32.

Ayudya, A. C.; Wibowo, A. (2018). The intention to use e-money using theory of planned behavior and locus of control. Journal of Finance and Banking, Vol. 22, Issue 2: 335-349.

Blahuta, R. I; Blikhar, V. S; Dufeniuk, O. M. (2020). Transfer of 3d scanning technologies into the practice of criminal proceedings. Science and Innovation, Vol. 16, Issue 3: 84-91.

Blahuta, R. I; Kovalchuk, Z. Ya; Bondarchuk, N; Kononova, O; Ilchenko, H. (2019). Financial resources and organizational culture as determinants for competitive strategy of enterprises. International Journal of Economics and Business Administration, Vol. 7, Issue 4: 471-482.

Dostov, V. L; Shust, P. M; Alekseev, G. V; Krivoruchko, S. V. (2020). Approaches to regulating the electronic money market in the EAEU: A comparative analysis. Financial Journal, Vol. 5: 89-119.

Dzhaksybekova, G. N; Namzhudinova, A. F. (2020). Main trends in the development of new banking products in the republic of Kazakhstan. Eurasian Union of Scientists, Vol. 4, Issue 73: 21-29.Gharaibeh, B; Al-Refaie, A;

Goussous, J; Shurrab, M. (2012). Effect of CCMS on customer satisfaction and loyalty in Jordanian banks. Information (Japan), Vol. 15, Issue 12 C: 6227-6237.

Khacaturyan, M. V. (2016). On the problem of managing the risks of integration of the EAEU countries. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia, Vol. 1: 166-168.

Kovalenko, S. B; Shernin, P. G. (2018). Foreign exchange operations of Russian commercial banks: Current state, problems and ways of development. Bulletin of the Saratov State Social and Economic University, Vol. 2: 136-143.

Lasme, M; Makoto, K. (2020). Financial inclusion, mobile money, and individual welfare: The case of Burkina Faso. Telecommunications Policy, Vol. 44, Issue 3: 49-66.

Law of the Republic of Kazakhstan No. 11-VI. (2016). "On payments and payment systems". Available at: https://online.zakon.kz/Document/?doc_id=38213728#pos=3;-106.

Law of the Republic of Kazakhstan No. 191-IV. (2009). "On counteraction of legitimization (laundering) of incomes received by illegal means, and financing of terrorism". Available at:

Law of the Republic of Kazakhstan No. 2155. (1995). "On the National bank of the Republic of Kazakhstan." Available at: https://online.zakon.kz/Document/?doc_id=1003548.

Law of the Republic of Kazakhstan No. 466-IV. (2011). "On amendments and additions to certain legislative acts of the Republic of Kazakhstan on electronic money issues." Available at: https://adilet.zan.kz/rus/docs/Z1100000466.

Leskova, I. V. (2017). Electronic currency: Opportunities for use in the EAEU. Archon, Vol. 1: 18-35.

Makhalina, O; Makhalin, V. (2019). Digitalization of the cryptosphere of the EAEU countries: State and prospects. Vestnik Universiteta, Vol. 6: 143-149.

Nekhaichuk, D. V; Nekhaichuk, Yu. S; Budnik, S. A. (2019). On the issue of introducing electronic means of payment and electronic money as modern innovative banking technologies. Bulletin of the Altai Academy of Economics and Law, Vol. 3, Issue 2: 122-128.

Panova, G. S. (2018). Modern money: Cash and non-cash. Scientific works of the Free Economic Society of Russia, Vol. 213, Issue 5: 125-131.

Patashkova, Y; Niyazbekova, S; Kerimkhulle, S; Serikova, M; Troyanskaya, M. (2021). Dynamics of Bitcoin trading on the Binance cryptocurrency exchange. Economic Annals-XXI, Vol. 187, Issue 1-2: 177-188.

Poier, S; Nikodemska-Wołowik, A. M; Suchanek, M. (2022). How higher-order personal values affect the purchase of electricity storage—Evidence from the German photovoltaic market. Journal of Consumer Behaviour,Vol. 21, Issue 4: 909-926.

Sarsembayev, D. M. (2021). International legal currency regulation in the framework of Eurasian integration (on the issue of a single currency). Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan, Vol. 1, Issue 64: 294-303.

Vozniuk, A. A; Savchenko, A. V; Tarasevych, T. (2020). Electronic money and payments as mean of committing crimes. Academic Journal of Interdisciplinary Studies, Vol. 9, Issue 4: 150-159.

Wulandari, D; Soseco, T; Narmaditya, B. S. (2016). Analysis of the use of electronic money in efforts to support the less cash society. International Finance and Banking, Vol. 3, Issue 1: 68-83.

Zhiendinova, S. B. (2016). Legal nature of electronic money in Kazakhstan: Comparison with the legal nature of money. Questions of Modern Jurisprudence, Vol. 2: 53-72.

The Right to be Forgotten as a Special Digital Right

Tereziia Popovych*,Mariia Blikhar,Svitlana Hretsa***Vasyl Kopcha****. Bohdana Shandra*****

A B S T R A C T

[Purpose] *The purpose of this study is to investigate aspects of digital law in Ukraine and other countries of the world in the context of the right to be forgotten.*

[Methodology/Approach/Design] *To achieve the objective, induction, deduction, and comparative analysis were used, both the proximate topics and aspects of the legal framework of different countries together with the legal information provided by online services were considered.*

[Findings] *The study identified the main features of the right to be forgotten in different countries, the impact of the European Union Court of Justice and European Court of Human Rights on it and the little-studied intricacies of the legal aspect of this mechanism.*

[Practical Implications] *This paper can be of interest both as introductory material and as a basis for further study because there is a growing human need to be able to control personal data in the face of the expanding phenomenon of globalization and digitalization.*

Keywords: Law. Digital Law. Search Engines. Internet Law. Information.

INTRODUCTION

The right to be forgotten implies the right of a person in certain specific situations to demand the deletion of data about their personal or family members. The establishment of the right to be forgotten is caused by the ability to find information about individuals in search engines at any time, regardless of the time frame for its placement. In its current form, it means the right to demand the exclusion from search engines of URLs (uniform resource locator) that were legally posted on the network, including by a person independently, due to their obsolescence or changing circumstances (DOVGAN, 2018). According to E.A.Voynikanis (2016), the attention of the European community to the right to be forgotten takes place in connection with the existing belief that the Internet, as a technology that allows storing a potentially unlimited amount of information, is a threat to privacy. In the context of this problem, the right to be forgotten is perceived as a certain additional means of controlling the personal data subject over the processing of their personal information in an online environment. At the same time, the researcher notes that the information stored on the network is not just indestructible, capable of infinite replication, but also closed in the eternal present, because due to its technical characteristics, the Internet is an environment within which it is impossible to disappear and within which a "digital dossier" for each user is actually stored (FILATOVA, 2020; SPASIBO-FATEEVA, 2019).

According to Yu.S. Razmetaeva (2018), the right to be forgotten is not fully covered by the right to privacy. The latter protects information about a person that they do not want to make publicly known,

for a certain time and preventing access to it for others. The right to be forgotten refers to truthful or once-true information that interferes or negatively affects a person's life or destroys their reputation in society. Researchers of the right to be forgotten generally believe that the "locomotive" for the further legal regulation of this right was the decision of the European Union (EU) Court of Justice in the case "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (2014). In its decision, the court ordered Google to remove information about Spanish citizen Mario Costech Gonzalez regarding the forced sale of real estate, which took place in connection with his social security debt ten years ago. The court also concluded that the right to be forgotten can be granted to an individual only when there is no interest of the Internet community in information about a particular person, and when the person does not play a particularly significant public role.

The main question before the Court of Justice in the Mario Costeja Gonzalez case was whether it was possible to consider search engines as data controllers, and hence whether they should provide users with tools to make changes or delete false personal data. The conclusions reached by the court were as follows:

(1) Firstly, search engines should be considered data controllers, because they process personal data;

(2) Secondly, search engines, as data controllers, are required to remove from the list results that are displayed after a search performed based on links to a person's name on web pages published by third parties, and that contain information about this person, even if the latter is legitimate;

(3) Thirdly, when analysing the request of the personal data subject for the removal of links to search results, the authorities must balance the interests of the subject under the Convention for the Protection of Human Rights and Fundamental Freedoms, the economic interests of the service provider, and the role of the personal data subject in public life and the public interest in accessing information (GUADAMUZ, 2017; PETRYSHYN and HYLIAKA, 2021).

The right to be forgotten in the system of digital human rights today is a very promising area of legal research, because it follows from the need to ensure the privacy of a person on the Internet, and is also the latest addition to the right to privacy and the right to protect personal data. In Ukraine, research on the right to be forgotten remains insignificant. Among the researchers who have investigated certain aspects of this phenomenon, the following can be noted: O.M. Kalitenko (2019), Yu.S. Razmetaeva (2018), A.A. Antopolsky (2019), N.V. Varlamova (2019), E.A. Voynikanis (2016). But above all, the right to be forgotten is the object of interest and analysis in international legal doctrine, as evidenced by the works of such researchers as A. Guadamuz (2017). The study reviewed and compared the results of court cases on the exercise of the right to be forgotten between Google divisions and various individuals or states. In the course of the study, a comparative analysis was carried out, and conclusions were developed using deductive and inductive approaches, considering the specifics of each of the situations, the importance of the case in the eyes of the court and the public, and a retrospective aspect in the context of the specifics

of each of the situations, the importance of the case in the eyes of the court and the public, and a retrospective aspect in the context of the specifics of the state structure, information control, and the legal system of different states.

INTERNATIONAL PRACTICE OF APPLYING THE RIGHT TO BE FORGOTTEN

The consequences of the decision taken by the Court of Justice of the European Union are of interest. Thus, to minimise possible lawsuits, Google has created a special online application form, through which a person can apply to the company to delete certain personal information. As of 2018, according to Google, it received more than 860 thousand requests to delete information from the search engine, as a result of which more than 3.4 million links were deleted. Based on the analysis of completed requests to delete information from the Google search engine, O.M. Kalitenko (2019) determines the following grounds for deleting information: the statute of limitations of circumstances that are the content of information (on the example of the case of Spanish citizen Mario Costech Gonzalez, which refers to ten years); unreliability or irrelevance of information about a person; public interest in information about a person. The last of these aspects is the most difficult because it shows the confrontation between the interests of an individual and the interests of society regarding information about a particular person. Therefore, the main focus here is directly on the subject of the request to delete information. This includes several types of such subjects:subjects that do not play a significant role in public life; subjects that play a significant role in public life (political or public figures, religious leaders, “stars”of show business, sports; subjects that play a limited role in public life (civil servants, individual officials) (LUKIANOV et al., 2021; UVAROVA, 2020). At the same time, as it becomes clear, the main criterion for the possibility of removing information about a person from a search engine is the public significance of the relevant information. Accordingly, information about the first category of persons may be deleted, about the second – not, about the third –deleted depending on its content and significance for society.

In the case of M.L. and W.W. v Germany. (2018), the European Court of Human Rights dismissed a complaint lodged by the applicants (who had been convicted of murder) concerning the commission by anonymous of severalmaterials in the Internet archive given: the public interest and the wide visibility of the case; the objective and reliable nature of the publications; the lack of intent to damage the applicants' reputation. N.V. Varlamova (2019) points out that the EU Court of Justice imposes on search engine operators the obligation to remove links to web pages published by third parties and containing information about a person from the list of search results made based on the name of the interested person, if such information has lost its relevance, but causes harm to it. The right to delete such information, according to the EU Court of Justice, must prevail over the economic interests of the search engine operator and the public interest in obtaining access to the relevant information about a person, except in cases of the special situation and role of the personal data subject in public life, which make the

interference with their rights justified.

The right to be forgotten, as defined by A.M. Boyko (2018), is a human right that allows a person to demand, under certain conditions, the removal of their personal data from public access through search engines, that is, links to those data that, in their opinion, can harm the person. This refers to outdated, inappropriate, incomplete, inaccurate, or redundant data or information, the legal grounds for storing which have disappeared over time. Therefore, it is important to note that it is not information about a person that is deleted but only links to this information on the Internet since the Internet is by its very nature a space where it is impossible to completely delete information. It remains on the servers of one resource or another. Therefore, the exercise of this right means that links to certain information about a person are removed from the search results so that the relevant information becomes inaccessible to public access users for their search queries. The URL must be removed from the search engine index, after which it becomes invisible to the user when executing a search query, but the source data remains available in the original source (VARLAMOVA, 2019).

Thus, the applicants M.L. and W.W. were found guilty of committing a crime against a famous actor in 1993 and sentenced to life in prison. However, in August 2007 and January 2008, they were released on probation from serving their sentences. However, in 2007 the applicants first brought a claim against the Deutschlandradio radio station in the Hamburg court to make anonymous personal data in the documentation about them, which was posted on the radio station's website. The Hamburg court and subsequently the court of appeals upheld the claim of applicants M.L. and W.W. However, the Federal Court overturned the decision of the appeal in the case, arguing that the radio station has the right to freedom of expression, as well as the public's interest in awareness.

In its conclusions, the European Court of Human Rights drew attention, first of all, to the importance of striking a balance between the applicants' right to respect for private life, the radio station's right to freedom of expression, and the public's right to be informed (BARABASH and BERCHENKO, 2019). In addition, the court pointed out that the indication in media reports, for example, of the name of a certain person (as was the case with M.L. and W.W.) there is an important aspect of the work of the press, especially when covering information about criminal proceedings that have attracted considerable public attention. Attention was focused on the increased public interest in the applicants in view of the public outcry that they had committed the murder of a famous actor. As it turned out, during their conviction, the applicants themselves repeatedly turned to the media to cover their case before the public. This factor further reinforced the court's reasoning as to the rejection of claims by M.L. and W.W. The German Federal Court of Justice and the European Court of Human Rights also noted that the veracity of the information about the applicants publicly posted online was not disputed, and the media did not intend to offend M.L. and W.W. or damage their reputation. Dissemination of information about the latter was limited because itwas carried out through a paid subscription. In addition, the applicants

did not provide information that they applied to search engine operators to restrict the tracking of information about them. Ultimately, the European Court of Human Rights concluded that there had been no violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950) in relation to the applicants M.L. and W.W. (JUDGMENT M.L. and W.W. V. GERMANY, 2018).

Therefore, as the above-mentioned decision shows, the court in the case of finding the truth must find a fair balance between the right of a person to privacy (through which the right to be forgotten is implemented) and freedom of expression and the right of the public to be informed. At the same time, as the case of M.L. and W.W. v Germany. (2018), the search for such a balance of interests is not an easy case, because at different levels of judicial instances, there were different interpretations of the courts of the essence of the dispute, and, accordingly, different decisions from each other. According to O.M. Kalitenko(2019), the debatable and problematic nature of the right to be forgotten lies in the fact that it is on the verge of two personal non-property rights of a person – the right to information (open access, lack of censorship) and the right to privacy (respect for private and family life, protection of personal data).

Resolution of the European Parliament and the Council No. 2016/679 "On the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (2016) provides for the right of the personal data subject to correct and erase (the "right to be forgotten") their personal data by their controller. In the sense of erasure, personal data may be deleted by the control at the request of the subject, if: they are not necessary from the standpoint of the purposes for which they were collected or processed; consent to their processing is revoked or objected to processing; they were processed illegally, etc. At same time, there are exceptions – cases where the rule on erasure of personal data cannot be applied: for the purpose of exercising the right to freedom of expression and information; considering the public interest in public health; for achieving goals of public interest, scientific, historical research, statistics; for the purpose of forming, implementing, or protecting legal claims.

In Argentina, the case of a 30-year-old model, singer, and actress Da Kunha v. Yahoo and Google, where the key question was raised about the responsibility of search engine operators for information that is provided to users in the search result. Thus, according to the plot of the case, Da Kunha, who published various kinds of photos on her website and social networks, including herself in short shorts, swimsuits, T-shirts, etc., filed a lawsuit against Yahoo Google, because photos with her in search results appeared on websites sexual, pornographic nature, as well as related to sex trafficking. The applicant submitted that such information had damaged her career as a singer and actress. In addition, her appearance on this type of website does not correspond to her personal beliefs and professional activities. She demanded compensation for property and moral damage in the amount of 200 thousand Argentine pesos. The court granted Da Kunha's claim, ordering Yahoo and Google to filter out all links to pornography and sexual services from search results. The key issue for the court's resolution was the conflict between freedom of

of expression and a person's right to control the use of their image (the right to privacy). This refers to the need to obtain permission to use images of a person in public space. In turn, the federal civil appeals court, at the request of representatives of Yahoo and Google, overturned the decision of the court of the first instance, releasing the applicants from certain obligations for them. The court's arguments were based on the fact that search engine operators cannot be held responsible for the damage caused to Da Kunha by Internet users through the placement of her photos on pornographic and sexual websites. The fact that Yahoo and Google catalogued relevant sites and provided links to websites is not sufficient to determine the causal relationship of Da Kunha's harm (CARTER, 2013).

A similar aspect of the liability of search engine operators (information intermediaries) was the subject of Google India Pvt. Ltd. v. Vinay Rai & Anr when an appeal was filed by the aggrieved party before the Delhi High Court over a breach of privacy caused by a third party seeking to hold even Google liable. However, the court dismissed the complaint on the grounds that for the Resolution of the Parliament of India No. 21 "On digital technologies" (2000), the intermediary (search engine operator) is not responsible for the content of information to which users are granted access. Exceptions here may be cases where: the transfer of information was initiated by an intermediary; the information was selected or modified by the intermediary; the intermediary colluded, facilitated, or encouraged the transfer of information; the intermediary cannot promptly delete or prohibit access to information after receiving actual knowledge or notification to the government that the data or communication line that takes place in a resource controlled by the intermediary is used to commit an illegal act (CHAKRABORTY, 2019). Thus, the issue of liability of search engine operators remains controversial in judicial practice, requiring proof of the positions of the parties. The latter, at the request of interested parties, can remove the demonstration of certain information about a person from the search results, but they should not be responsible for the content of certain personal data about a person posted on the Internet.

PRACTICE OF THE EUROPEAN COURT OF HUMAN RIGHTS IN THE CONTEXT OF THE RIGHT TO BE FORGOTTEN

From the standpoint of the practice of the European Court of Human Rights, the solution of problematic aspects of the implementation of the right to be forgotten is carried out by establishing by the court the presence or absence of a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), which protects the right to respect for a person's private and family life.

For example, in one of the European Court of Human Rights cases, Khelili v. Switzerland (2011), the right to respect Sabrina Khelili's private life was upheld. According to the plot of the case, during a police check in Geneva in 1993, the applicant was found to have business cards that read: "A pretty, beautiful woman in her 30s, would like to meet a man to have a drink together or go outside from time to time. Phone number ...". The police wrote her name on their records as a "prostitute", despite Khelili's

insistence that she was never one. In turn, the police referred to the cantonal law on personal data, which allegedly allowed them to keep records of personal data to the extent necessary for the performance of official duties. On this basis, in November 1993, the Federal Office of Foreignersissued a two-year ban on Khelili's residence in Switzerland. In 2001 two criminal complaints were lodged against the applicant for threatening and abusive behaviour. In 2003, from a letter from the Geneva police, she learned that the word “prostitute” in relation to her name still appears in police cases. Subsequently, in 2005, the Geneva police chief told Khelili that the word for her profession had been replaced by “tailor”. However, after learning from a telephone conversation that in 2006 the word “prostitute” still appeared in the police's computer files, Khelili asked to delete the relevant information again and asked the Geneva police to delete data on criminal complaints filed against her, among which the word “prostitute” was included. However, in this request, the applicant was refused on the grounds that such information should be kept as a preventive measure, given her past offences.

In its conclusions, the European Court of Human Rights determined that the word “prostitute”, which is kept in the police records, can damage the reputation of Khelili and make her daily life more problematic because this data can be passed on to the authorities. The problem situation is compounded by the fact that such data is subject to automatic processing, which facilitates access to it and its distribution. The court also drew attention to the vagueness of Khelili's allegations of unlawful prostitution and to the insufficient proximity of the link between the retention of the word "prostitute" and the applicant's conviction for threatening and abusive behaviour. Thus, the court concluded that the retention of false data in the police records violated Khelili's right to respect for her private life, and in particular the word “prostitute” – neither justified nor necessary (KHELILI V. SWITZERLAND, 2011).

It is important to note that the right to be forgotten in its implementation must have its limits. This, in particular, is confirmed by the decision of the EU Court of Justice in Google v. France in September 2019 in its decision, the Court indicated that the right in question applies only to the version of the search engine in the EU, but not outside it. The essence of the dispute between Google and France was that the National Commission for Informatics and Freedom of Franceasked Google to completely remove information that was granted the right to be forgotten from search results. The company did not comply with the National Commission for Informatics and Freedom of France request but only used geo blocking. In other words, the information was displayed in the search results, but not in the EU. The National Commission for Informatics and Freedom of France imposed a fine of 100 thousand euros on Google. Therefore, the company appealed to the French Council of State to cancel this decision. The latter sent the dispute to the EU Court of Justice. Despite the arguments of France that geoblocking does not give proper results, because the search results can be circumvented via a virtual private network (VPN), the EU Court of Justice did not take them into account. At the same time, the court took into account Google's position that if states were given the opportunity by law to perform actions similar to

those required of the search engine by the National Commission for Informatics and Freedom of France, in the future this would allow censoring the Internet network (ANDROSCHUK, 2021).

A frequent area of implementation of the right to be forgotten is associated with the removal of information about a person's past experience in criminal activities from search engines. Thus, this refers to protecting the right of a person to rehabilitation. Thus, for example, in September 2014, the Kyoto District Court (Japan) rejected a person's claim against Google Japan, which asked to remove information about their arrest in the past from search results. At the same time, the court determined that such actions should be performed by the parent company, not the subsidiary. Consequently, in October 2014, the Tokyo District Court ordered Google to remove headlines and snippets on websites that reveal the name of a person who claimed that their privacy rights were violated due to articles hinting at past criminal activity. In addition, in June 2015, the Saitama District Court in Japan ordered Google to remove from search results details of an arrest that took place three years ago for violating child prostitution laws, saying that the crime was relatively minor and had no historical or social significance (VOSS and CASTETS-RENARD, 2016).

CONCLUSIONS

Thus, the exercise of the right to be forgotten is one of the modern forms of protection of privacy and personal data on the Internet, which has gained its significance due to the practice of the EU Court of Justice and the European Court of Human Rights. At the heart of this right is the freedom of a person to handle personal information about them, which a person, in particular, wishes to remove from public access. At the same time, it is not about deleting information directly, but about links to it contained in search engines. The study found that there is a contradiction in the exercise of the right to be forgotten, namely in maintaining a balance between ensuring private and public interests (in terms of access to information).

In addition, it is worth noting that in the light of the exercise of the right to be forgotten, it is necessary to discuss two main legal obligations: the first –established – concerns search engine operators who must remove links to information about a person on their request, which is outdated, inaccurate, unreliable, etc.; the second – concerns the obligation to obtain the consent of a person to place information about them on the network. Given the specific nature of the Internet, obtaining such consent is necessary, because in the future it would allow avoiding situations in which a person will contact search engine operators to delete information about them placed without their consent. An exception here may be information about public or socially significant persons, or certain personal data of civil servants and individual officials.

REFERENCES

Androschuk, G. (2021). EU Court: Google has won the dispute over the right to forget. Available at: https://cutt.ly/cZmrs10.

Antopolsky, A. A. (2019). Human rights and the Internet: the case law of the European Court of Human Rights. Proceedings of the Institute of State and Law of the Russian Academy of Sciences, 14(2), 171-172.

Barabash, Y. & Berchenko, H. (2019). Freedom of Speech under Militant Democracy: The History of Struggle against Separatism and Communism in Ukraine. Baltic Journal of European Studies, 9(3), 3-24.

Boyko, A. M. (2018). The right to forget: some aspects of theory and practice. Journal of Eastern European Law, 48, 124-131.

Carter, E. L. (2013). Argentina's right to be forgotten. Emory International Law Review, 27, 25-31.

Chakraborty, S. (2019). Right to be forgotten – the most recent dispute in data protection. International Journal for Legal Developments & Allied Issues, 1, 86-87.

Convention for the Protection of Human Rights and Fundamental Freedoms. (1950). Available at: https://zakon.rada.gov.ua/laws/show/995_004#Text.

Dovgan, E. F. (2018). Human rights in the age of information technology. Journal of the O.E. Kutafin University, 5, 109-125.

Filatova, N. (2020). Smart contracts from the contract law perspective: Outlining new regulative strategies. International Journal of Law and Information Technology, 28(3), 217-242.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. (2014). Available at: https://eur lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

Guadamuz, A. (2017). Developing a right to be forgotten. EU Internet Law:Regulation and Enforcement, 59-76. Cham: Springer.

Judgment M. L. and W.W. v. Germany (2018). Available at: https://cutt.ly/xZn4Rpz.

Kalitenko, O. M. (2019). The right to be forgotten: a European or a global achievement? Journal of Civilization, 35, 60-64.

Khelili v. Switzerland. (2011). Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-345%22]}.

Lukianov, D. V., Hoffmann, T. & Shumilo, I. A. (2021). Prospects for recodification of private international law in Ukraine: Do conflict-of laws rules require a new haven? Journal of the National Academy of Legal Sciences of Ukraine, 28(2), 198-210.

Petryshyn, O. V. & Hyliaka, O. S. (2021). Human rights in the digital age: Challenges, threats and prospects. Journal of the National Academy of Legal Sciences of Ukraine, 28(1), 15-23.

Razmetaeva, Y. S. (2018). Formation of new human rights under the influence of IT. IT law: problems and prospects of development in Ukraine. Lviv: Ivan Franko National University of Lviv.

Resolution of the European Parliament and the Council No. 2016/679. "On the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". (2016). Available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Resolution of the Parliament of India No. 2. "On digital technologies". (2000). Available at: https://uk.upwiki.one/wiki/Information_Technology_Act,_2000.

Spasibo-Fateeva, I. (2019). Implementation and Protection of the Right to Freedom of Expression in Ukrainian Civil Law: Modern Problems. Baltic Journal of European Studies, 9(3), 205-223.

Uvarova, O. (2020). Business and human rights in times of global emergencies: A comparative perspective. Comparative Law Review, 26, 199-224.

Varlamova, N. V. (2019). Digital rights – a new generation of human rights? Proceedings of the Institute of State and Law of the Russian Academy of Sciences, 14(5), 9-46.

Voss, W. G. & Castets-Renard, C. (2016). Proposal for an international taxonomy on the various forms of the "right to be forgotten": a study on the convergence of norms. Available at: https://cutt.ly/SZmthCh.

Voynikanis, E. A. (2016). The right to be forgotten: legal regulation and its theoretical understanding. Jurisprudence, 3, 70-89.

Autonomous Robots and Their Legal Regime in the Context of Recodification of Civil Legislation

Yurii Khodyko*

ABSTRACT

[Purpose] *The issues of understanding what a robot is as an object of civil legal relations and the civil law regime that must be applied to ensure effective legal regulation of relations related to the use of robotics require legal solutions. Special attention should be paid to the study of liability for damage caused by robotics to a person or their property.*

[Methodology/Approach/Design] *The main methods on which this work was based are the method of systematization and the method of analysis. The article summed up various basic materials related to robots as objects of civil legal relations, as well as the impact of their existence on the current development of the world.*

[Findings] *Considering the purpose of robotics in the modern world, it is proposed to carry out legal regulation of robotics relations using an approach of the extension of civil law regulation applied to things. This does not exclude the introduction of special rule s that will apply exclusively to robots as objects.*

Keywords: Object of Civil Legal Relations. Autonomous Robot. Legal Regime. Concept Of Robot. Liability For Damage Caused by Robot.

INTRODUCTION

The development of technology and the desire of society to automate production processes has led to the emergence of robotic systems (robots). A fairly long process of technology development in the area of robotics and artificial intelligence, which is considered for more than a decade, has provided the "technological evolution" of robots from laboratory prototypes to the mass use of robots in the industrial sector and the first significant steps in the use of robotics in consumer services, medicine, military and space spheres. Every year, robots are given an increasing number of functions, they begin to be used in various fields, and robots become more autonomous when used (DANCHUK et al., 2021). All this is the path that humanity is quite successful in the field of robotics, the pinnacle of which is the creation of a universal intelligent anthropomorphic robot. The emergence of robots was predominantly conditioned upon the aim to simplify human life in the field of production, displace human labour in areas that are complex and dangerous, as well as to accelerate the pace of production at the expense of robots, making it more technologically advanced, accurate, and high-quality. Robotisation of production processes has led to changes in the labour market around the world, the emergence of new professions, which are usually associated with the management, control of technological processes, etc. (GINTERS et al., 2010). Even though humanity has managed to replace humans with robots in many areas of production

and life support, robots will never be on a par with humans in their status, regardless of what level technological advance has reached in the field of creating robots, in particular an intelligent anthropomorphic robot. For humanity, robots should remain only a means of abetter way of life – helpers. As noted by N. Richards and W. Smart (2013), the idea of possible equality between a robot and a human in terms of its status should be unequivocally rejected. As the world is filled with robotic and artificial technologies, lives and relationships of social, political, and economic power are also changing, creating new and unexpected problems for law (LARSON, 2010; BALKIN, 2015). Solving problems of legal regulation of relations arising in the field of robotics use, their legal nature is a natural process, as with the emergence of any new objects of civil legal relations (KHARYTONOV et al., 2021).

To date, there is no civil law regulation, as well as in general legislative regulation of relations regarding robots as such in Ukraine. This cannot be stated about the European Union, which Ukraine seeks to join and has committed itself, in particular in the legislative sphere, to harmonise legislation with the latter. The European Parliament adopted a resolution "Report with recommendations to the Commission on Civil law Rules on Robotics" (2017), which defined the key issues and ways to form civil law regulation of relations in the European Union regarding the use of robots. Notably, legislation in the field of robotics in the form of a special law was adopted in 2008 (with subsequent changes) in South Korea "Intelligent Robots Development and Distribution Promotion Act" (2008). However, this law does not contain conceptual provisions of civil law regulation of relations regarding the use of robots but is only aimed at developing a national policy for the development of robotics in the state. The key issues to be resolved include determining what should be understood by robots in general, from the standpoint of legal regulation, the civil law turnover of such robots, as well as liability for damage caused to a person or property during the robot's work (activity). The solution of these issues will ensure the development of the fundamental principles of the civil law concept of legal regulation of relations in the field of human use of robotics in Ukraine.

HISTORICAL ASPECTS OF ROBOTISATION

The idea of ordinary people about robots, as a rule, is based on films and literature of the science fiction genre, and the robot is associated with the "Iron Man". Such a view, today, is not devoid of real content, but it is rather distortedand narrow. Thus, indeed, humanity is striving to create an anthropomorphic intelligent robot and there are real first steps in this direction. However, excessive "humanisation" of robots is to a certain extent a trend of modern realities (KHAN et al., 2012). Although a robot may once be considered a human, this situation is unlikely to happen in the near future (ASARO, 2007).Most of the robots that currently exist do not have a uniform similarity but are designed for practical application in a particular field, and in the first place is not its appearance, habits, abilities similar to human ones, but its autonomy and functionality according to the needs of the field of application. The word "robot" was first proposed in a science fiction play by Czech writer Karel Capek (2021) R.U.R. (Rossumovi univerzální

roboti (Czech.), "Rossumi Universal Robots"),which the world saw in 1920. In the play, robots are considered as humanoid mechanisms used as slave labour in a factory. Later, in the collection of science fiction stories by Isaac Asimov "I, Robot" (2018), the "Three Laws of robotics" were formed for the first time, which are still relevant today and form the basis for developing the rules of ethics for robots around the world. These two literary works of the science fiction genre marked the beginning of robotics, the idea of which was picked up by the fields of engineering and programming to bring fantastic ideas to life.

Today, much attention is paid to defining the understanding of the robot for the purposes of legal regulation both in the legal scientific literature, and there are also the first steps to consolidate the legal understanding of the robot as an object of civil legal relations in regulations. R. Calo (2016) refers to a robot as an artificially created object or system that can receive and process information, as well as act according to their surrounding world. N. Richards and W. Smart (2013) define a robot as a developed system that demonstrates both physical and intelligent activity but is not alive in the biological sense.Evidently, in the definition of a robot, scientists emphasise that it is not a biological object, but an artificially created one. Even though the current legislation of Ukraine does not govern the issue of robots, the Appendix to the Procedure for state control of international transfers of military goods provides a legal definition of a robot. The specified Appendix determines that robot is a manipulative mechanism that can move continuously or from point to point, can use sensitive elements (sensors) and has all the following characteristics:

(1) Multi-functionality;

(2) Ability to set or orient material, parts, tools, or special devices using variable movements in three-dimensional space;

(3) Equipped with three or more closed-loop or open-loop servomechanisms, which can include stepper motors;

(4) Ability "to be programmed by the user" using the teach/repeat method or using an electronic computer, which can be programmed by a logic controller, i.e., without mechanical intervention (RESOLUTION,2002).

The legislator based this understanding of the robot on the fact that the robot is a manipulative mechanism that can perform tasks independently in space according to the programmed functionality of the robot.

MAIN CHARACTERISTICS OF ROBOTS

The Law of South Korea "Intelligent Robots Development and Distribution Promotion Act" (2008) indicates one of the main characteristics of a robot as its mechanical nature upon defining the concept of a robot, namely as a mechanical device that perceives the external environment for itself, distinguishes between circumstances and moves voluntarily (Article 2.1 of the Law). At the same time, clause 1 of the European Parliament resolution "Report with recommendations to the Commission on Civil law Rules

on Robotics"(2017) emphasises that the following characteristics are necessary to qualify acertain device as a smart robot:

(1) Ability to become autonomous using sensors and/or exchange data with the environment, the ability to exchange this data and analyse it;

(2) Ability to self-learn based on experience gained and interaction (optional criterion);

(3) Presence of at least minimal physical support;

(4) Ability to adapt actions and behaviour according to environmental conditions;

(5) Absence of life from a biological standpoint.

Considering the above-mentioned scientific opinions and legislative provisions in terms of understanding the robot as an object of civil legal relations, the robot has 4 main components (features): materiality, intelligence, functionality, and autonomy.

Materiality. A robot is an object of the material world, a device created by human intelligent/manual labour, and not by nature. The materiality of the robot on the one hand allows considering it as a thing, on the other hand, the absence of life in the robot from a biological standpoint excludes the possibility of qualifying it as a person – an individual (subject of civil legal relations), and as an animal – an object of civil legal relations.

Intelligence. The intelligent component of the robot ensures that the latter performs all actions according to its functionality. The intelligent attribute of the robot is software, artificial intelligence, which in their unity form the "digital (electronic) brain" of the robot. It is the intelligent component of a robot that transforms it from a simple thing – an object of the material world – into a robot as an independent object in the system of objects of civil legal relations. The basic abilities of a robot are laid down (programmed) by a person according to its functionality. Thanks to artificial intelligence, which can be a component of the robot's "digital (electronic) brain", it can be programmed for self-study, considering the principles of ethics for robotics, which can ensure its functional self-improvement (BAPIYEV et al., 2021). In terms of artificial intelligence as a component of the "digital (electronic) brain" of the robot, artificial intelligence is an independent object of civil legal relations, and as a result of intellectual (creative) human activity, it is an object of intellectual property rights. From the standpoint of material features, "the difference between a robot and artificial intelligence is that artificial intelligence does not require physical form, and robots can be represented in forms of distinctive designs" (LARSON, 2010; BUIL et al., 2015).

Functionality. The functionality of a robot should be understood as a set of features that the robot can perform. The developer determines the functionality of the robot according to the needs of the scope of application of the corresponding robot. The robot can be equipped with one function or several (a combination of them). In a robot, functionality can be "physical" and/or "intelligent". Physical functionality lies in performing physically active actions in space – moving (walking, running, jumping, flying, etc.), transporting, or performing other actions with objects according to the established task. At

the same time, intelligent functionality can include speaking, counting, learning,analysing, decision-making, etc.

Autonomy. The autonomy of a robot should be considered as the ability of a robot to perform its functional component independently, without external interference. The robot's autonomy depends on two factors. First, the level of autonomy of the robot depends on the level of its intelligence component, since it activates the functionality component of the robot and thereby ensures its endent performance of certain actions. The second factor of robot autonomy depends on the level of human intervention in the robot's activity when the robot performs certain actions that make up its functional component. The level of human intervention that makes up the second factor of robot autonomy is majestic relative and is directly dependent and proportional to the first factor. Since engineers, programmers, and other specialists involved in the development of robotics face a considerable number of extremely complex problems that need to be solved for maximum autonomous operation of a robot that worked efficiently and would ensure the achievement of the goal in a particular field of robotics use. Thus, the robot is an object of the material world (device), which, depending on the level of autonomy and intelligence components, can perform the functions laid down by the developer according to the scope of application.

CIVIL LAW REGIME OF ROBOTS IN MODERN LEGAL REGULATION

Considering the civil law regime of robots in modern legal regulation, it can be compared with the legal status of slaves in the Roman state. Modern robots that are used in production, in human life support and other spheres of public life have a similar purpose as a slave in Rome. The main principle underlying the legal status of a slave was servi res sunt (slave – thing) (NOVITSKII, 2008). The slave was a thing that could speak. The only difference between a slave and an ox or mule was that they were an “instrument that speaks” (instrumentum vocale) (CHERNILOVSKIY, 1991). Robots are objects of the material world, i.e., de facto – things, but the combination of the above features that describe a robot as an object of civil legal relations gives grounds, de jure, to consider the robot along with things and other objects-goods as an independent object in the system of objects of civil legal relations. At the same time, the current level of development of robotics does not indicate the need to create an entirely new, special civil law regulatory regime for them as objects. The set of legal tools already formed in the legislation, which form the civil law regime of things, can be extended to robots, which is more than sufficient to ensure their effective civil law turnover for the next several decades (ELENEY et al., 2022; NASS et al., 2021). However, this does not exclude the addition of certain special provisions to the current civil legislation in the legal regulation of robotics (e.g., in the field of liability for damage caused by a robot to a person or their property).

A separate aspect of the civil law regime of robots that requires attention is the issue of liability for damage caused by the robot to a person or their property. Being an object of civil legal relations, a robot cannot be held liable for damage caused to a person or property, since the responsibility is borne by the

subject of civil legal relations, and not by the object. Accordingly, it can be assumed that the subject of liability for damage caused by the robot may be the owner of the robot or its manufacturer (developer), etc. In this case, the resolution of the European Parliament "Report with recommendations to the Commission on Civil law Rules on Robotics" (2017) identifies two approaches to liability for damage caused by a robot:

(1) Objective liability, wherein it is necessary to prove the damage caused and the causal relationship between the functioning of the robot and thedamage caused;

(2) Risk management, when responsibility is assigned to the person who should have minimised risks and consider negative consequences.

Considering that the robot is essentially a mobile thing and guided by the provisions of the Civil Code of Ukraine (2003), on compensation for damage caused by defects in goods, works and the Law of Ukraine No. 3390-VI "On liability for damage caused by product defects" (2011), it can be stated that in Ukraine, as a general rule, the first approach is laid down – the objective responsibility of the manufacturer (developer). And today, if harm is caused by a robot in Ukraine, the manufacturer (developer) will be held responsible. However, since the robot is not just an object of the material world, the choice of the approach of liability for damage caused by the robot is not sufficiently unambiguous towards the responsibility of the manufacturer (developer).

Quite striking in this regard will be the example of the use of robotics in the field of medicine. At the end of January 2022, Johns Hopkins University published information that for the first time in the world, the STAR (Smart Tissue Autonomous Robot) performed laparoscopic surgery without human assistance (GRAHAM, 2022). The STAR robot performed the procedure on animals, which requires the surgeon to apply stitches with high accuracy and consistency. A unique feature of the STAR is that it is the first robotic system that plans, adapts, and performs a surgical plan in human soft tissues. In this case, an autonomous robot in surgical intervention acted as a high-precision tool that substituted the hands of a human surgeon in terms of applying highprecision and consistent sutures to soft tissues (DE PAGTER, 2021).

Without detracting from advances in technology and artificial intelligence, carrying out such an operation would not be without human participation, namely making a diagnosis, preparing for surgery, administering anaesthesia, monitoring vital signs during the operation, and most importantlyquality control of the work performed by the robot on suturing soft tissues andstating the success of the surgical intervention by the human doctor. Ultimately, the surgeon who performed the operation using an autonomous robot is responsible for the quality of the operation as a whole and is obliged to assess all risks when performing such a surgical intervention using an autonomous robot as an instrument. If a patient dies during such an intervention using an autonomous robot, then when determining who should bear responsibility (manufacturer (developer) of the robot or a surgeon) the degree of autonomy of the robot, the quality of the work performed by it (considering its technological capabilities in this situation)

and the actions of the doctor, who was generally responsible for such a surgical intervention, regarding its taking all sufficient, in this situation, measures according to medical instructions. Only after evaluating these two circumstances can one determine the degree of guilt of the manufacturer (developer) of the robot and the surgeon, and accordingly the amount of responsibility or lack thereof.

Another illustrative example that indicates that a risk management liability approach to robot harm should be considered when using robotics occurred in the United States. With the widespread advent of autopiloted cars, accidents involving such vehicles have become more frequent in the United States. The very first high-profile case was in December 2019 with 27-year-old driver Kevin George Aziz Riad in the Los Angeles suburb of Gardena. He was driving at high speed in a Tesla Model S car using autopilot, left the freeway, ran a red light, and crashed into a Honda Civic at the intersection. Two people who were in the Civic died at the scene. Riad was charged with manslaughter, although he denied his guilt, since the car was not driven by him, but by autopilot. Tesla, in this case, stated that autopilot and the more complex "full self-driving" system cannot control the car independently, and that drivers must be careful and ready to respond at any time, as indicated in the instructions (KRISHER and DAZIO, 2022). In this case, as with the robot surgeon, autopilot is a tool (assistant) for more comfortable and safe driving, and not a full-fledged driver. The absence of the driver's fault, in this case, could only be said if there were defects in the autopilot, which clearly could have caused the accident, and the driver, with all caution, could not prevent it (O'SULLIVAN et al., 2019).

Therefore, when it comes to liability for damage caused by a robot, it is considered that the approach of risk management is more correct than objective liability. When considering the issue of liability for damage caused by a robot, one cannot fail to pay attention to the conditionally third alternative approach of liability, according to which the robot is given the status of a subject – a legal or electronic entity. Giving the robot the status of a subject suggests its tort status,and accordingly the ability of the robot to independently bear responsibility for the damage caused (LI et al., 2022). This, in turn, will eliminate such a problem as the difficulty of determining the presence of guilt and its degree in relation to the manufacturer (developer) and the owner of the robot. This approach is most beneficial for the manufacturer (developer) of robots, since it factually exempts them from liability for damage caused by the robot. One of the key issues of civil liability of the robot as a subject is the availability of property, at the expense of which compensation for the damage caused will be carried out.

Evidently, the robot itself does not possess property as such.

Appropriate legal structures are required to ensure that the robot has such a property component. There are several solutions in this aspect: robot's civil liability insurance; creation of a financial fund, into which a certain percentage of the amount will be deducted when purchasing a robot (e.g., according to the principle of how value-added tax is paid when buying goods), which can later serve as a source of compensation for damages. However, despite some positive aspects of this approach for certain participants in civil legal relations, thisapproach is currently at least premature and impractical. Since the

the introduction of robots into the status of a subject will complicate their civil law turnover, the question arises whether a subject can be an object of turnover.

CONCLUSIONS

This scientific study suggests that an autonomous robot is an independent object of civil legal relations in the system of objects and is described by four key features: materiality, intelligence, functionality, and autonomy. Considering the legal nature of the robot as an object of civil legal relations, first of all its materiality, it allows introducing a regime of things regarding the legal regulation of robotics relations. This does not exclude the existence of special legislation exclusively for autonomous robots, which will determine the specific features of certain aspects of legal regulation. Furthermore, the available legal structures of civil liability in civil law are quite competitive in the approach of liability of the robot as a subject, formed doctrinally and worked out in law enforcement.

Liability for damage caused by the robot to a person or their property should be assigned to the manufacturer (developer) or owner of the robot. An analysis of the two approaches of objective responsibility and risk management suggests that the approach of responsibility of risk management is fairer. At the same time, giving the robot the status of a subject of law and assigning responsibility to the robot is not relevant, since the available well-established structures are quite effective and worked out in practice. Despite everything, regardless of what difficulties legal science currently faces in legal regulation of robotics relations, the introduction of effective legal regulatory mechanisms is an inevitable process, since this is required by the present, and all the shortcomings and gaps of legal structures that will sometimes be identified in practice can be eliminated in the future.

REFERENCES

Asaro, P. M. (2007). Robots and responsibility from a legal perspective.Available at: https://peterasaro.org/writing/ASARO%20Legal%20Perspective.pdf.

Asimov, I. (2018). I, Robot. London: Harper Voyager.

Balkin, J.B. (2015). The Path of Robotics Law. California Law Review, 6, 45-60.

Bapiyev, I., Kamalova, G., Yermukhambetova, F., Khairullina, A. &Kassymova, A. (2021). Neural network model of countering network cyber attacks using expert knowledge. Journal of Theoretical and Applied Information Technology, 99(13), 3179-3190.

Buil, R., Piera, M. A., Gusev, M., Ginters, E. & Aizstrauts, A. (2015). Mas simulation for decision making in urban policy design: Bicycle infrastructure. Proceedings of the International Conference on Harbour, Maritime and Multimodal Logistics Modelling and Simulation, 95-102). Bergeggi: I3M Conference.

Calo, R. (2016). Robots in American law. University of Washington School of Law Research Paper, 4, 1-45.

Capek, K. (2021). R.U.R. Kyiv: Komora.

Chernilovskiy, Z. M. (1991). Lectures on Roman Private Law. Moscow: Yuridicheskaya Literatura.

Danchuk, V., Bakulich, O., Taraban, S. & Bieliatynskyi, A. (2021). Simulation of traffic flows optimization in road networks using electrical analogue model. Advances in Intelligent Systems and Computing, 1258 AISC, 238-254.

De Pagter, J. (2021). Speculating about robot moral standing: On the constitution of social robots as objects of governance. Frontiers in Robotics and AI, 8.

Eleney, C.M., Bradley, M., Alves, S. & Crudden, D. M. (2022). Development of a low-cost semi-automated robotic orthophosphate system for batch analysis. Analytical Methods, 14(35), 3444-3450.

European Parliament. (2017). Report with recommendations to the commission on civil law rules on robotics. Available at:

Ginters, E., Barkane, Z. & Vincent, H. (2010). System dynamics use for technologies assessment. 22th European Modeling and Simulation Symposium, EMSS 2010, 357-361.

Graham, C. (2022). Robot performs first laparoscopic surgery without human help. Available at: https://hub.jhu.edu/2022/01/26/star-robot-performsintestinal-surgery/.

Khan, P.H.; Kanda, T.; Ishiguro, H.; Gill, B.T. & Ruckert, J.H. (2012). Do people hold a humanoid robot morally accountable for the harm is causes? Proceedings of the Seventh Annual ACM.IEEE International Conference on Human-Robot Interaction, 1-8. Boston: Attitudes and Responses to Social Robots.

Kharytonov, E., Kharytonova, O., Kostruba, A., Tkalych, M. & Tolmachevska, Y. (2021). To the peculiarities of legal and non-legal regulation of social relations in the field of sport. Retos, 41, 131-137.

Krisher, T. & Dazio, S. (2022). Felony charges are 1st in a fatal crash involving Autopilot. Available at: https://cutt.ly/qLmMI1h.

Larson, D. (2010). Artificial intelligence: robots, avatars, and the demise of the human mediator. The Ohio State Journal on Dispute Resolution, 25(1), 105-164.

Li, Y., Guo, S. & Gan, Z. (2022). Empirical prior based probabilistic inference neural network for policy learning. Information Sciences, 615, 678-699.

Nass, O., Kamalova, G., Shotkin, R. & Rabcan, J. (2021). Analysis of Methods for Planning Data Processing Tasks in Distributed Systems for the Remote Access to Information Resources : Topic: Communication and control systems and networks. International Conference on Information and Digital Technologies 2021, IDT 2021, 273-276.

Novitskii, I. B. (2008). Roman Private Law. Moscow: Jurisprudence.

O'sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U. & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. International Journal of Medical Robotics and Computer Assisted Surgery, 15(1).

Republic Of Korea. (2008). Intelligent Robots Development and Distribution Promotion Act. Available

Richards, N. & Smart, W. (2013). How should the law think about robots? SSRN Electronic Journal, 5, 1-25.

Ukraine. (2003). Resolution of the Cabinet of Ministers of Ukraine No. 1807"On approval of the Procedure for state control of international transfers of military goods". Available at: https://cutt.ly/bLmByvP.

Ukraine. (2011). Law of Ukraine No. 3390-VI "On liability for damage caused by product defects". Available at: https://zakon.rada.gov.ua/laws/show/3390-17#Text.

Ukraine. Civil Code of Ukraine. (2003). Available at: https://zakon.rada.gov.ua/laws/show/435-15#Text.

The Concept of Artificial Intelligence in Justice

Oleksandra Karmaza*Sergii KoroiedVitalii Makhinchuk***Valentyna Strilko****Solomiia Iosypenko*****

A B S T R A C T

[Purpose] *The aim of the article is to cover the main definitions of the concept of artificial intelligence, its origins, characteristics, grounds for application, as well as direct interaction and influence on the implementation of the main tasks of justice through the use and development of artificial intelligence in the judicial procedure.*

[Methodology/Approach/Design] *To solve the tasks set, the study employed the appropriate methods and materials of scientific research, namely dialectical, historical, statistical, sociological, and other methods of cognition of processes and phenomena, including specialised methods of grammatical consideration and interpretation of legal norms. Furthermore, an entire block of logical methods was used, including classification (upon creating a complete classification and structuring of scientific hypotheses and assumptions), extrapolation, induction and deduction, analogy, abstraction, comparison.*

[Findings] *This paper investigates the emergence and transformation of artificial intelligence in modern technological and information relations, its gradual introduction in various spheres of life, namely the ways of implementation and the possibility of application in justice. Furthermore, the study analyses possible ways and legal consequences of introducing artificial intelligence into the e-justice system in Ukraine and proposes the stages of reformation.*

[Practical Implications] *The materials of this study are of practical value in the implementation of the goals set for the active use of artificial intelligence tools and their gradual improvement, including the development of methodological guidelines, legislative acts covering the judicial procedure and reference books and recommendations for the interpretation of regulations that have already been adopted in the process of introducing electronic justice in the country.*

Keywords: Legal Proceedings. Artificial Intelligence. Electronic Justice. Corporate Disputes.

INTRODUCTION

The development of information systems that help a person make decisions began with the emergence of expert systems in the 1950s, which describe the algorithm of actions for choosing a solution depending on particular conditions. Expert systems have been replaced by machine learning, thanks to which information systems independently form rules and find solutions based on dependency analysis, using initial data sets (without first drawing up a list of possible solutions by a person), resulting in the emergence of artificial intelligence. Technological solutions developed using machine learning methods are an example of artificial intelligence that can only solve highly specialised problems (weak artificial intelligence) (PONKIN and REDKINA, 2018). The creation of a universal (strong) artificial intelligence, capable, like that person, to solve various problems, think, interact, and adapt to changing conditions, is a complex scientific and technological issue, the solution of which is at the intersection of

various areas of scientific knowledge – natural science, technical, and socio-humanitarian (ARTIFICIAL INTELLIGENCE…, 2017; APPLICATION OF ARTIFICIAL INTELLIGENCE…, 2021). Solving this problem can lead not only to positive changes in key areas of life, but also to negative consequences caused by social and technological changes that accompany the development of artificial intelligence technologies (LARINA and OVCHINSKY, 2020; YAROSHENKO et al., 2020).

In recent years, the expert community has increasingly discussed whether it is possible to automate the entire procedure of delivering justice using artificial intelligence, as well as replacing a judge with a system of universal (strong) artificial intelligence capable of analysing the factual circumstances of a case, giving them a legal assessment and making an appropriate decision (ALETRASet al., 2018; CHERNIAVSKYI et al., 2019). In China, the United States, Great Britain, France, and some other countries, such computer programmes are already finding their application, but currently serve merely as an auxiliary tool for analysing documents and do not replace a judge. In December 2018, the first International Act specifically dedicated to the use of artificial intelligence in justice appeared – the European Ethical Charter on the use of artificial intelligence in judicial systems, approved by the European Commission for the Efficiency of Justice of the Council of Europe (EUROPEAN COMMISSION, 2020). The Charter sets out five principles for the use of artificial intelligence: the principle of respect for human rights, by virtue of which the use of a computer programme should not detract from the adversarial nature of the procedure and the right to a fair trial; principle of prohibition of discrimination; the principle of quality and safety, which makes provision for the use of certified software, which is evaluated by both technical specialists and lawyers; the principle of transparency, by virtue of which all technologies used must be brought to the public attention in an understandable form (COUNCIL OF EUROPE, 2018).

Thus, more than three decades of improvements in information and communication technologies (ICT) are breaking into the activities of courts and prosecutors, promising transparency, efficiency, and radical changes in working practices, such as paperless courts. Even if such promises have not yet been fulfilled in most jurisdictions, programmes and algorithms are already performing increasingly more judicial procedures. The impact of such technologies on the functioning of justice and the values established by international principles of judicial conduct are mostly positive. The latest technological wave in the foreign experience of well-known countries is based on artificial intelligence (AI) and promises to change the way court decisions are made (LOMAKIN and SAMORODOVA, 2017). This purpose is mainly pursued through a specific technology called “machine learning”, which makes predictions by evaluating case materials, both procedural documents and related court decisions. This data set, known as “training data,” is analysed to build statistical correlations between cases and related court decisions.

The more data the algorithm processes, the more accurately it predicts decisions in new cases (LOMAKIN and SAMORODOVA, 2017). For this reason, such systems “learn” (even if only in terms

of improved statistical accuracy) to reproduce the results that judges have already achieved in such cases. Unlike the already available technological tools that digitise the exchange of data and documents, this technology of "predictable justice" (as it is usually labelled) is intended to influence judicial decision-making (APPLICATION OF ARTIFICIAL..., 2021). However, it is not yet clear whether this trend leads to better solutions or undermines the proper performance of the system. That is precisely why, to solve this and other related issues, the scientific literature contains many studies on this matter, conducted by Ukrainian and foreign researchers such as R. F. Zakirov (2017), S. O. Furashev (2018), I. V. Pokin and A. I. Redkina (2018), V. A. Shemshuchenko (2018), M. G. Matveev, A. S. Sviridov, N. A. Aleinikova (2008), K. Pittman (2016), J. Nesbitt (2017).

The present paper aims to cover the main definitions of the concept of artificial intelligence, its origins, characteristics, grounds for application, as well as direct interaction and influence on the implementation of the main tasks of justice through the use and development of artificial intelligence in the judicial procedure.

MATERIAL AND METHODS

Using dialectical and historical methods, the authors of this study considered the ways of establishment and development of artificial intelligence in the scientific field, its main functions and tasks, signs and conditions of application. The Aristotelian and sociological method allowed determining the main stages of the development of artificial intelligence, as well as the analysis of scientific research of Ukrainian and legislative researchers, and their significance in its further development. Comparison is one of the key methods in this paper, since the subject of the analysis covers not only the legal scope of its application, but also the experience of the existence of artificial intelligence in various spheres of human and state life. Methods of grammatical analysis and interpretation of legal provisions helped identify the available regulations governing the existence of artificial intelligence in the process of regulating public relations in the state. Monitoring and making suggestions for its improvement. The methods of scientific cognition used in this study are most often general scientific methods. Within the framework of general scientific methods, the authors analyse the available opinions of foreign authors on this controversial issue.

The authors of this study describe and compare legal opinions on the regulation of the activities of artificial intelligence abroad. The paper proposes the classification of approaches to the legal understanding of artificial intelligence proposed in the scientific literature. Apart from the aforementioned methods, the study employed the comparative legal method. Firstly, to investigate the success of legal regulation of the issues under study in other countries and the possibility of implementing the corresponding legal constructions in Ukrainian legislation. Secondly, the method of legal modelling allowed formulating the alleged positive aspects and disadvantages of certain legal

structures for regulating the legal status of artificial intelligence. Based on Ukrainian and foreign legislation, as well as judicial practice, the study identifies the most viable options for resolving controversial legal issues that correspond to the legal nature of artificial intelligence Notably, the hermeneutical method was used in this paper to interpret the essence and content of the main definitions that describe artificial intelligence in the legal plane. The provisions and conclusions of this study are also based on articles on philosophy, economic theory, general theory of state and law, financial law, theory of administrative law, other branch legal sciences, studies of individual foreign researchers. Current legislation, scientific publications, statements, assumptions, and other regulations that establish and regulate the procedure for resolving socio-legal conflicts constitute the main legal basis for scientific research. Using the sociological method, the authors clarified the positions and opinions of lawyers, prosecutors, and judges on the practical application of artificial intelligence in the justice system proceeding from judicial practice. The statistical method is used to generalise and analyse the conclusions of Ukrainian and foreign researchers and investigate the problems under study. The empirical and informational structure of this study also comprises generalisations of practical activities of subjects of jurisprudence, statistical materials, reference publications, political and legal journalism, and other legal achievements.

RESULTS

Trends in the development of modern public relations indicate a desire to use artificial intelligence in the field of electronic justice. The developed ideas about the technological aspects of artificial intelligence do not fully fit into the legal consciousness of both Ukrainian and foreign researchers of law. The legislator's unwillingness to determine the legal mode of operation of artificial intelligence is conditioned upon the lack of any experience in its use. The introduction of artificial intelligence in the life of society will show its advantages and disadvantages only after a long time. Under these circumstances and modern forecasting of mechanisms of legal regulation of machine intelligence is rather conditional and imperfect. That is why this study investigates the possible ways and legal consequences of introducing artificial intelligence into the e-justice system in Ukraine (SHEMSHUCHENKO, 2018).

Upon considering court cases, artificial intelligence will allow the court to quickly and reliably establish the essential circumstances of the case, verify the arguments of the participants in the process and, as a result, considerably reduce the time for making an objective decision. In such disputes, it is often necessary to evaluate the integrity of the behaviour of participants in public relations, regardless of the emotional and psychological factors that affect, in particular, the work of a human judge. Understanding artificial intelligence as a digital programme based on the mathematical algorithms laid down by its developers, which produces “new” solutions (machine thinking), requires studying the algorithms of its

work in court, including from the standpoint of optimising the judicial procedure and the purpose of establishing the truth in the case. This article reveals the problems of two areas of application of artificial intelligence in court when considering legal disputes: office management and general issues of litigation; assessment of evidence and establishment of legally significant circumstances in a public or private legal dispute (PONKIN and REDKINA, 2018).

Thus, in the specialised literature, artificial intelligence is understood either as a device capable of "acting, determining its actions and evaluating their consequences without full human control based on the results of processing information coming from the external environment", or as a computer programme that simulates the human brain, which has a learning mechanism built in (GOLDFARB and TREFLER, 2018). In Europe, artificial intelligence (AI) is a cyberphysical (non-biological) autonomous, but physically (energy) dependent support system that can exchange data with its environment and analyse it, selflearn based on acquired experience and interaction, and adapt its actions and behaviour in accordance with environmental conditions. According to the philosophical encyclopaedia, artificial intelligence is a digital system that simulates human intellectual and sensory abilities using computing devices (a neural network). The fact that artificial intelligence will be neutral in relation to humans is a myth. It was dispelled in modern times, when it became clear that technology has its autonomy and independence from humans. The humankind has become a hostage to the technology it created, it cannot free itself from its reverse influence on themselves It is obvious that artificial intelligence created by humans contains not only unlimited possibilities, but also unlimited dangers.

At the present time, the artificial intelligence system is spontaneously improving, influencing a person and subjugating them; it can grow into a dangerous world for humans, which is partly what is happening today and becomes an inevitable threat. Artificial intelligence has its own laws and language, the lack of a deep understanding of which in humans makes decisions unpredictable (SHEMSHUCHENKO, 2018). For example, procedural legislation requires a judge to be guided by his internal belief when evaluating evidence, which is a much more complex category than software algorithms. Depending on the particular circumstances, the same evidence may be rejected in one case and, on the contrary, accepted as a basis in another case. Admittedly, the artificial intelligence system will never be capable of penetrating the depth of the human psyche. Artificial intelligence can assess the circumstances of a case only from the standpoint of formal logic, and that is why it will never be capable of fully understanding the plot of the case, since in many cases, for example, family, and especially criminal, there is a lot of irrationals, as opposed to formal-logical.

Furthermore, upon making a decision, the court is guided by numerous evaluation and value criteria stipulated by the law. For example, the principles of justice and humanism in the imposition of punishment, the requirements of reasonableness and good faith in civil law. Understanding of such

general categories is formed in a person in the process of socialisation, upbringing, and personality development – all this cannot be reproduced in a software algorithm.

In the context of dynamic updating of legislation caused, among other things, by the technological advance, it is not uncommon for courts to apply the analogy of statute and the analogy of law, which is understood as dispute resolution based on the general principles and content of legislation. The meaning of legislation, that is, its spirit, can only be revealed by a person with a high level of legal culture, and not by a computer. With particular clarity, the impossibility of replacing a judge with artificial intelligence is established in cassation proceedings. After all, the basis for cancelling a court decision in cassation is not any formal violation, but only a substantial violation of legal norms that affected the results of consideration of the case and without the elimination of which it is impossible to restore and protect violated rights, freedoms, and legitimate interests. These criteria derive from the principle of legal certainty, by virtue of which the quashing of a judicial decision on formal grounds is inadmissible. Only a professional judge can evaluate whether the violation committed meets the materiality criterion and whether it can affect the outcome of the case (COUNCIL OF EUROPE, 2018)

In turn, the computer algorithm will record any violation and come to the conclusion that the judicial act is subject to cancellation, even if the formal cancellation leads to the same outcome of the case. Therefore, it is at least premature, but most likely impossible, to contemplate replacing the judge with artificial intelligence. Therewith, the use of artificial intelligence in the consideration of the already mentioned indisputable requirements is not excluded, primarily in writ proceedings, since such work is not related to the analysis of legal relations between the parties and is more technical in nature. In some developed countries, such systems are already being implemented (PONKIN and REDKINA, 2018).Admittedly, the constant expansion and change of the regulatory framework, judicial practice, increasing the burden on the judicial system, which leads to a large number of investigative and judicial errors, actualises the use of artificial intelligence in the Ukrainian judicial system as it is disinterested, incorruptible, objective, and capable of finding almost infallible legal solutions, ways, and methods of effective justice. The authors of the present study cannot but agree that such systems will not only be of great service in the work of courts, prosecutors, officials of investigative bodies, and advocates, but will also enable an objective external control over their activities. Unfortunately, to date, no official document of the legislative framework of Ukraine contains a regulatory definition of the term “artificial intelligence”, although the term itself is actively used in many countries. This situation is conditioned upon the lack of a single legal approach to establishing its common characteristics in different countries. In particular, the creators of the European civil legislation on robotics point out that it is impossible to give an accurate definition of artificial intelligence, which is associated with the real presence of various robots. In this regard, in their opinion, the study of the latter should be approached casuistically, considering each work individually, as a separate unique case.

DISCUSSION

Thus, the term "artificial intelligence" is used to refer to a large scope of scientific and applied research. This name, which is attached to this subject area, most people are more likely to associate with smart robots or thinking computers, numerous images of which were created in science fiction works. That is why many concerns about artificial intelligence are circulating in modern society, and such alarm signals continue to arrive with increasing force. Artificial intelligence is not only associated with the display of human qualities in machines, it also helps drive vehicles, can become an ideal tool for stealing confidential data, increase company productivity, or create ideal opportunities for corporate spies. Artificial intelligence is not yesterday's invention. The history of its creation is full of memorable moments and names of reputable scientists, ups and downs, extravagant promises and loud disappointments. Artificial intelligence is finally starting to bring real benefits to the state, business, citizens, and the humankind in general.

The power of computers has dramatically increased, there are more algorithms for solving tasks, and, most importantly, the world produces a huge amount of fuel that feeds artificial intelligence – billions of gigabytes every day. Notably, despite the active development of AI technologies, the level of their implementation remains low, which complicates the assessment of the true potential of such technologies. McKinsey Institute experts conducted detailed case studies on five sectors of government activity. The obtained results allow assuming a hypothetical transformation of some types of activities, which, in turn, will disrupt the work of other sectors by a chain reaction (ARTIFICIAL INTELLIGENCE…, 2018). Artificial intelligence has broad prospects for many stakeholders, including multinational corporations, start-ups, governments, and social institutions (WORLD BANK GROUP, 2016). There is no doubt that artificial intelligence has a huge potential for fundamental change in society. However, at this stage, it is difficult to predict the direction that the development of this technology will take. Corporations, governments, and employees themselves are guided by the principle of time intervals. However, there is already a need for urgent and clear measures to respond to risks, which are also evident in every existing state (PONKIN and REDKINA, 2018).

The development of digital technologies in the era of the information society and the processes of globalisation, the speed of data transmission, confirmed the prospect of introducing artificial intelligence in the courts. It became evident that artificial intelligence is our present, and not the future, which the humankind has long begun to study and only recently approved and began to apply it in most countries of the world. Therewith, the current state of the research on artificial intelligence in the world indicates a long workflow of software engineers together with neuroscientists to build an artificial cognitive system close to human physiology and the reproductive abilities of the human brain, which are still not studied by science (PONKIN and REDKINA, 2018; BABAK et al., 2021). In legal proceedings, human activity is limited by certain formal rules, which is why it is permissible to use only specialised

intelligent systems that can work, although independently, but under full human control(EUROPEAN COMMISSION, 2020). Artificial intelligence should be recognised as a source of increased danger; therefore, in this case, it is necessary to assign responsibility for the damage caused by its activities to its creators in accordance with the law. Responsibility for damage caused as a result of the use of artificial intelligence in legal proceedings should be borne by the state. After all, only the state should act as the sole creator of intelligent systems, if they are used in state bodies, to perform the obligations assigned to them. Therefore, the creation and use of "smart" robots for criminal purposes, as well as illegal interference in the activities of artificial intelligence systems, which will lead to causing socially dangerous harm, should impose criminal liability (SHEMSHUCHENKO, 2018; TACIJ et al., 2014).

For example, in the United States, scientists have long begun to think about the use of artificial intelligence in court proceedings. The country annually considers a huge number of cases of deprivation of parental rights. Considering the fact that there is a case law in the USA, that is, the possibility of copying a decision from another case that is suitable in terms of parameters, the idea is not so strange. It is enough to find a similar case in the database and see what decision was made then. And if there is a large amount of information, evidence base in the case, then the task is completely reduced to analysing statistics and actions according to the template. Thus, such algorithms are created by people, which means that they somehow reflect the picture of the world of their creators. Neural networks used in artificial intelligence technologies are based on decisions made by humans. Therewith, as data accumulates, it is possible to identify patterns that have nothing to do with decision-making (BUOCZ, 2018). But the neural network is designed in such a way that it will certainly take the detected pattern for the necessary material. For example, if men were convicted more often than women in any type of criminal case, then for artificial intelligence, the defendant's gender may eventually turn into a significant factor and would influence decision making.

In December 2018, the European Commission for the Efficiency of Justice of the Council of Europe approved the European Ethical Charter, which containsthe principles of the use of artificial intelligence in judicial and law enforcement systems (ARTIFICIAL INTELLIGENCE…, 2020). This is the first international act regulating such a sensitive and unknown area. The Charter deals with the need for user control: a judge has the right to disagree with a decision proposed by artificial intelligence, and any participant in a dispute has the right to appeal against such a decision and demand that the court consider their case without using artificial intelligence in court. There is, however, another aspect that cannot be ignored. In the present-day world, "advanced" technologies are used not only by lawyers, but also by representatives of criminal structures, organised crime, etc. If their actions are not countered by the same modern technology, the criminals will find themselves in a deliberately advantageous position. The same reasoning allows contemplating the importance of maintaining equality before the law or the court: if modern technologies are used, then ideally, they should be accessible to everyone. Thus, the question

of whether or not artificial intelligence will penetrate the field of law should not be considered critically. It is only important to understand where it belongs, and which areas of activity of the state and citizens in it will forever or at least for a long time remain with a person (SHEMSHUCHENKO, 2018).

Undoubtedly, for more than three decades, advances in information and communication technologies (ICT) have been penetrating the work of courts and prosecutors, promising transparency, efficiency, and radical changes in the procedure and methods of activity, such as the transition to paperless proceedings(GETMAN et al., 2019). Although these promises have not yet been fulfilled in most countries, computer programmes and algorithms are carrying out a growing number of judicial procedures. These technologies have a predominantly positive impact on the operation of judicial systems and the values stipulated by international principles of judicial conduct. The latest wave of technologies is based on artificial intelligence and promises to transform the way court decisions are made. This goal is achieved mainly through a special technology called "machine learning", which makes forecasts by analysing case materials – both procedural documents and corresponding court decisions (SHEMSHUCHENKO, 2018). Based on the analysis of this set of data (“training data”), statistical comparisons are established between cases and corresponding court decisions. The more data the algorithm processes, the more accurate its predictions for new cases will be. Consequently, these systems “learn” to reproduce decisions that judges would make on similar ones. Unlike the already used technologies for digital data and document exchange, this technology of “predictable justice” (as it is often incorrectly called) is designed to influence court decisions. At present, it remains unknown whether it will improve the quality of solutions or interfere with the proper operation of the system (LARINA and OVCHINSKY, 2020).

The potential impact of such technology on the administration of justice can be assessed by examining the problems posed by already used technologies, such as record-keeping and electronic filing systems. In and Wales, a simple arithmetic error in the official form of the document used in divorce cases led to an incorrect calculation of alimony in 3,600 cases in 19 months. The problem is not the error itself, but the reasons why the Ministry of Justice and those who used this form did not notice it for so long. Users usually pay attention to the interface and the tools that enable them to use technological systems, rather than their internal operation (MATVEEV et al., 2008). Judicial technologies provide access to an array of court case data to increase transparency, but the way systems assess this data internally is difficult to evaluate and control. Therefore, the main question is whether it is possible to create effective mechanisms to control the internal operation of ICT and data processing algorithms. Another question is how to guarantee due oversight of technologies and their accountability, namely using the example of artificial intelligence (or rather machine learning).

Some countries, including the United States, use technology that makes recommendations for making decisions about pre-trial detention. Such programmes use algorithms calculating the probability of

relapse and “estimate” the probability that the accused will commit a crime if they are not taken into custody. Technologies, whether office management systems, simple online forms, or more complex programmes that use artificial intelligence in their activities, should only be used in litigation if there are appropriate human-side control mechanisms (BUOCZ, 2018; SHULZHENKO and ROMASHKIN, 2021). After all, today, the problem of control is even more acute when it comes to artificial intelligence systems based on machine learning. In this case, the forecasts are based on algorithms that change over time. In machine learning, algorithms “learn" (change) based on their experience. When algorithms change, one no longer knows how they work or why they behave in a certain way. How can the humans ensure their accountability if they do not possess effective monitoring mechanisms? This question remains open. And until technical and institutional solutions are found, the principle of caution should be guided. The reservations and precautionary principle mentioned are part of the Ethical Charter on the use of artificial intelligence in the judicial systems of the Council of Europe. This specifically refers to the principles of compliance with fundamental rights and user control of artificial intelligence (SHEMSHUCHENKO, 2018). However, the way these principles are to be implemented remains unclear. This task is certainly not for lawyers, parties to the case, or judges. It can only be carried out with the involvement of specialists from various fields, monitoring the operation of systems and evaluating artificial intelligence for compliance with key values stipulated by international principles of judicial conduct and regulations available in national legislation in each state practicing artificial intelligence.

CONCLUSIONS

Considering the arguments brought up in the present study, broad discussions at international conferences and scientific discussions, the issue of developing common approaches to understanding the place of artificial intelligence in the modern system of knowledge and international relations is topical. However, the scientific literature contains enough reasons to doubt the use and implementation of artificial intelligence. In this regard, it would be correct to suggest the following questions that are to be resolved, namely:

(1) development of approaches to the future strategy or concept of legal regulation of artificial intelligence;

(2) determination of the scope of its legal personality and probability of liability;

(3) suggestions of areas for development in both national and international law;

(4) investigation of legally significant problems relating to links with new developments in artificial intelligence, as well as relating to the application of the available types of autonomous intelligent systems, in various transport, communication, security, legal systems, etc.;

(5) determination of the prospects for creating doctrines and legal provisions concerning the developers, control and improvement of autonomous intellectual systems, legal regimes, variables for the use of

such systems, as well as the development of links between new mechanisms of legal support for artificial intelligence;

(6) permissibility and limits of application of modern legal norms concerning liability (administrative, civil, criminal) against developers of artificial intelligence systems, their operators, and other persons.

An analysis of those arguments suggests that litigation and the work of artificial intelligence are impossible in isolation from a human judge. The available artificial intelligence technologies do not allow making "machine decisions" (judicial acts) independently and completely. Questions of law and legal qualification cannot be transmitted to artificial intelligence without their evaluation by a human judge. It is necessary to use artificial intelligence in matters that require processing a large amount of information and documents in electronic form. Thus, artificial intelligence will ensure procedural savings and terms of consideration of a legal dispute on the merits by means of speed and error-free calculation and processing of a large number of incoming and outgoingcorrespondence, procedural documents in the case, evidentiary material, including decisions made in the given proceedings. The use of artificial intelligence ensures the development of technological legal science in Ukraine in terms of objective establishment of legal facts. Public disclosure of digital algorithms for the operation of judicial artificial intelligence will bring greater digital publicity to Ukrainian litigation and ensure transparency of the entire judicial system in the state.

REFERENCES

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D. & Lampos, V. (2018). Predicting judicial decisions of the European Court of Human Rights: A Natural Language Processing Perspective. PeerJ Computer Science, 2,e93.

Application of Artificial Intelligence on the Basis of the Court of First Instance: VRP Initiates the Launch of a Pilot Project. (2021). Available at: https://jurliga.ligazakon.net/news/201578_zastosuvannya-shtuchnogo ntelektu-na-baz-sudu-persho-nstants-vrp-ntsyu-zapusk-plotnogoproektu.

Artificial Intelligence: The Next Digital Frontier? (2017). Available at:https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificialintelligence-discussion-paper.ashx

Babak, V. P., Babak, S.V., Eremenko, V.S., Kuts, Y.V., Myslovych M.V., Scherbak, L.M. & Zaporozhets, A.O. (2021). Models of Measuring Signals and Fields. Studies in Systems, Decision and Control, 360, 33-59.

Buocz, T. J. (2018). Artificial intelligence in court: Legitimacy problems of AI assistance in the judiciary. Retskraft — Copenhagen Journal of Legal Studies, 2(1), 41-59.

erniavskyi, S. S., Holovkin, B. M., Chornous, Y. M., Bodnar, V. Y. & Zhuk, I.V. (2019). International cooperation in the field of fighting crime: Directions, levels and forms of realization. Journal of Legal, Ethical and Regulatory Issues, 22(3), 1-11.

Council of Europe. (2018). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment. Available at: https://rm.coe.int/ethical-charter-en-for-publication-4-december2018/16808f699c.

European Commission. (2020). On Artificial Intelligence – A European approach to excellence and trust. Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper artificial-intelligence-feb2020_en.pdf.

Furashev, S. O. (2018). Internet of things: Problems of legal regulation and implementation. Kyiv: Polytechnic Publishing House.

Getman, A., Karasiuk, V., Hetman, Y. & Shynkarov, O. (2019). Ontological representation of legal information and an idea of crowdsourcing for its filling. Advances in Intelligent Systems and Computing, 836, 179-188.

Goldfarb, A. & Trefler, D. (2018). AI and International Trade. Cambridge: National Bureai of Economic Research.Larina, O. S. & Ovchinsky, V. S. (2020). Artificial intelligence. Ethics and law.Moscow: Knizhnyĩmir.

Lomakin, N. I. & Samorodova, I. A. (2017). Digital economy with artificial intelligence, 254-257. Advances in Science and Technology: Collection of articles based on the results of the IX International Scientific and Practical Conference. Moscow: Research and Publishing Center "Aktualnost.RF".

Matveev, M. G., Sviridov, A. S. & Aleinikova, N. A. (2008). Artificial intelligence models and Methods. Application in economics. Moscow: Publishing House "Finansy I Statistika".

Nesbitt, J. (2017). Ways artificial intelligence is transforming trade. Available at: https://www.tradeready.ca/2017/topics/import-export-trade management/4-ways-artificial-intelligence-transforming-trade/Pittman, K. (2016). Infographic: A brief history of collaborative robots. Available

at: https://www.engineering.com/story/infographic-a-brief-history-ofcollaborative-robots.

Ponkin, I. V. & Redkina, A. I. (2018). Artificial intelligence from the point of view of law. Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences, 22(1), 91-109.

Shemshuchenko, V. (2021). Artificial intelligence in justice. Available at: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/.

Shulzhenko, N. & Romashkin, S. (2021). Types of individual criminal responsibility according to article 25 (3) of Rome Statute. Juridical Tribune, 11(1), 72-80.

Tacij, V. J., Tjutjugin, V. I. & Grodeckij, J. V. (2014). Conceptual model establish responsibility for offense in the legislation of Ukraine. Criminology Journal of Baikal National University of Economics

and Law, 2014(3), 166-183.

World Bank Group. (2016). Harnessing the Power of Big Data for Trade and Competitiveness Policy. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/26266/113275-WP-PUBLIC-P152206-8-3-2017-17-28-0-BigDataTCEdited.pdf?sequence=5&isAllowed=y.

Yaroshenko, O. M., Vapnyarchuk, N. M., Burnyagina, Y. M., Kozachok-Trush, N. V. & Mohilevskyi, L. V. (2020). Professional development of employees as the way to innovative country integration. Journal of Advanced Research in Law and Economics, 11(2), 683-695.

ZAKIROV, R.F. (2018). The use of modern IT-technologies as a means to achieve the main objectives of the judiciary. Bulletin of the Civil Process, 2(1), 211-219.

Identity of the Suspect in Cyber Sabotage

Oleh Peleshchak*Roman BlahutaLarysa Brych***Nataliya Lashchuk****
Dmytro Miskiv*****

A B S T R A C T

[Purpose] *The purpose of the study is to identify means and measures to counteract and prevent cyber sabotage.*

[Methodology] *The research is based on a systematic approach and logical tools (description, analysis, synthesis, induction, deduction, etc.). Special scientific, general scientific, and philosophical methods are applied.*

[Findings] *The study analyses the possible motives of the suspect in cyber sabotage and unifies classification approaches. Attention is focused on information support for the interrogation of a suspect in cyber sabotage by an investigator to learn the identity of the suspect. Certain features of the sources of obtaining information about a person suspected of committing cyber sabotage are noted. The general characteristics and features of the identity of a cyber sabotage suspect cannot be considered outside the context of other socially dangerous attacks in cyberspace. The development of mechanisms for countering cybercrime in Ukraine continues.*

[Value] *The practical significance of the study is determined in the list of measures means proposed by the authors to reduce the risk of cyber sabotages and eliminate their harmful consequences.*

Keywords: Criminal Identity. Forensic Characteristics. Cybercrime. Prevention.Cybercrime.

INTRODUCTION

Nowadays, cybercrime is the most dynamically developing type of socially dangerous attacks in the world and in Ukraine. Over the past ten years, there has been an increase in this type of crime exponentially. During 2020, more than 5000 cybercrimes were registered in Ukraine, 106 persons involved in criminal proceedings were detained (In 2020, the National Police…, 2021). The prerequisites for this increase are the availability of computer knowledge, a growing level of integration of technologies into the economy and public life, technological progress (improving the technical characteristics of equipment combined with reducing the price of it), insufficient level of security of information processes, cross-border (no state borders in cyberspace), an increase in the Internet, telecommunications, and other types of networks (the ability to connect to them via ordinary telephone lines), improvement of network technologies, an increase in the number of users (their low legal awareness, disregard for the rules of cyber hygiene, non-compliance with the policy of code (password) and information security), corruption component, hyperlatedness (fear of victims losing their reputation, revealing their security schemes, exposing their own illegal actions) etc (DE FRÉMINVILLE, 2020; GETMAN et al., 2019). Cyber threats against unauthorised interference, distributed denial-of-service (DDoS) attacks, the spread of malicious software (including one that can

automatically type all alphanumeric combinations based on the principle of a random number generator for setting a password), internet fraud, the establishment of hidden access for the purpose of future control to the use of fake twin sites, simulation programmes, chatbots, cloud technologies, and many others are also being modified. In this context, cyber-attacks on the public sector are also increasing, which, considering modern threats and challenges, slow down positive development trends and threaten both society and the state. Illegal access or distortion of computer information can disrupt the operation of state security systems and lead to material damage and human casualties (RYCHKA, 2019).

Modern information technologies and the latest software not only affect economic processes, and therefore politics and overall society, but also provide new and more advanced opportunities for committing previously unknown offences, or committing traditional crimes by non-trivial methods and means. However, there is a limit of the law that is mandatory for both the real and virtual world (BILENCHUK, 2001). The identity of the criminal is the source of the crime, and therefore, the analysis of thinking, characteristics, and specific features of the person suspected of committing cyber sabotage play an important role in forming the trace picture of this crime. The study is significantly complicated by the lack of an unambiguous assessment of "cyber incidents" in national legislation (usually they are conditionally interpreted as a way of committing), the dispersion of factual and objective information about these individuals in the reports of various law enforcement departments of Ukraine, the hyper-diversity and atypicality of ways and means of committing cyber sabotages (TACIJ et al., 2014). Therefore, the work of law enforcement agencies to detect, investigate, and prevent crimes in this area in a timely manner requires further adequate organisational, managerial, and forensic means and measures to counteract and intensively introduce innovations.

The above causes an urgent need for further study in this area to clarify certain scientific provisions in order to improve the methodology for investigating crimes of this category, establish productive interaction between law enforcement agencies, strengthen criminal legal protection, and criminal liability, require analysis and addition of the arsenal of countering the commission of cyber sabotages (DENYSOVA, 2003; LUTSENKO, 2017; BORYSOVA et al., 2019).Liability for criminal offences in the use of electronic computers (computers), systems and computer networks and telecommunication networks are provided for in Chapter 16 of the Criminal Code of Ukraine. If the violation of automated systems is associated with the commission of more serious crimes (for example, sabotage, espionage, theft of property, etc.), the actions of the perpetrators are qualified according to the totality of crimes (BORYSOVA, 2006). The purpose of the study is to identify means and measures to counteract and prevent cyber sabotage.

MATERIALS AND METHODS

The study applied special scientific, general scientific, and philosophical methods. This allowed

comprehensively considering the subject matter. Using the dialectical method, the process of developing criminological knowledge about the identity of a cybercriminal in general and a person suspected of committing cyber sabotage, in particular, was considered. The use of a criminological approach to the investigation of a person suspected of committing cyber sabotage is complex, since it covers sociological, criminal-legal, psychological, and pedagogical aspects of scientific analysis. The use of methods of analysis, synthesis, induction, and deduction identified socio-demographic, criminal-legal, and moral and psychological features of a person suspected of cyber sabotage, forming a list of measures and means of countering and preventing cyber sabotages.

Criminological and criminalistic sources were analysed using various methods of legal interpretation and in the context of the hermeneutical method of scientific knowledge. This facilitated an in-depth analysis of the subject matter. The logical and semantic approach was used to analyse classification systems and types of cyber criminals. The scientific conclusions were confirmed using the statistical method.

The problems of characterising the face of a cybercriminal have been considered by many researchers since the beginning of the 21st century. Some aspects of this problem were investigated by: P.D. Bilenchuk (2001), O.O. Denysova (2003), L. Borysova (2006), K. Titunina (2006), V.B. Shkolnyi (2012), N.S. Kozak (2013), S.V. Yakimova and B.C. Borovikova (2016), O.Yu. Ivanchenko (2019), M.O. Gvozdetska and K.Yu. Izmaylov (2016), V.Yu. Shepitko and V.A. Zhuravel (2017), B.Yu. Chernikov (2018), O.Yu. Dovzhenko (2019), M.I. Maliy and P.D. Bilenchuk (2019), D.O. Rychka (2019), N.L. Pushina (2020), M.W. Kranenbarg, S. Ruiter, J.L. Van Gelder (2021), A.F. Karachka (2017), O.R. Peleshchak (2021).

RESULTS AND DISCUSSION

When qualifying crimes related to computer equipment, it is necessary to consider not only the general rules for qualifying crimes, but also some specifics of crimes inherent only in such acts. The object will be especially important for the qualification, that is, the identity of the criminal and their forensic characteristics. Computer criminals are colloquially referred to as "hackers", "software crackers", and "phreakers". A hacker is a highly qualified IT (information technology) professional who understands the intricacies of computer software. A cracker is an IT professional who hacks security systems (including software protection), software, creates or modifies hacking, and much more. The result of hackers is deliberate cracks, which are programmes that allow hacking software. Software crack is usually suitable for mass production. In fact, a crack is the epitome of a type of hacking, most often it is a general patch (information intended for automatically making certain changes to computer files). In most cases, software crack does not have the source code of the programme, so the disassembler and debugger investigate the programme using special utilities (MAYER LUX & VERA VEGA, 2020). A

phreaker is a person who is engaged in phreaking. This term is also used for people who use the phone for their illegal actions in order to psychologically influence the end user.

Recently, phreaking is understood as various ways of hacking electronic systems, such as bank security systems and access control systems. As a consequence of the above, these individuals have special knowledge and practical skills in the field of computer technology and are at least computer users. In a computer information crime against a legal entity, the perpetrator or accomplice (accomplice) is usually an employee of this institution or organisation. These are computer operators, peripherals and communications equipment; programmers; system administrators; electronics engineers; database administrators; network security specialists, civil servants and other persons who have access to computer information and equipment, their networks. Competitors or industrial spies, professional criminals and cyberterrorists, can pose a serious threat to network security. Representatives of these groups are engaged in illegal activities from corporate espionage to extremely dangerous sabotage of computer systems of vital objects. In recent years, the investigation of the identity of a criminal in global computer networks has faced a significant increase in criminal activity on the part of hackers. Not only in identifying the fact of committing a cyber sabotage after the fact (according to experts, 90% of cases of crime detection are generally due to chance), but also in investigating this type of crime, there are certain difficulties. It is quite difficult to identify, record, and seize criminally significant information when performing investigative actions for use as material evidence (CHERNIKOV, 2018). Most of this information can be obtained by using profiling methods both when identifying a cybercriminal and to prevent illegal actions. Since a wide range of people are involved in cybercrime, the establishment of a database of typical profiles of cyber criminals and the study of their general features allows optimising the process of narrowing the circle of suspects. Speaking about the personality of criminals, it is important to emphasise that this type of person is characterised by a high level of intellectual development, unusual thinking, professionalism, fanatical attitude to new computer technologies, ingenuity, rich imagination, and secrecy. As a rule, the criminal among the employees of the organisation is an exemplary employee with appropriate training. Such persons have not previously committed any criminal offences. Often these are managers of various ranks who have leadership roles, but are not directly responsible for specific areas of work with computer information. Most often, crimes in the field of computer information are committed by stable criminal groups that are characterised by mobility, high technical equipment, a clear distribution of roles, expressed self-serving motivation and a well-thought-out system for hiding traces of criminal activity(CHERNIAVSKYI et al., 2019). The greatest danger and difficulties for detection and disclosure are criminal groups, which include highly qualified specialists with special knowledge in the field of secret obtaining and protection of computer information. Most of the crimes committed by these subjects remain latent.

The vast majority of offenders are adults, with an almost uniform distribution by age. It should also be

be noted that the vast majority of those who have committed these types of offences have higher or secondary special education. As for the gender characteristics of the attacker, it can be stated that criminal offences in the field of computer information are committed mainly by men. In the current period, a large number of people, both non-professional and highly qualified specialists, will be involved in the commission of crimes. At the same time, all of them have different social status and level of education, which already allows them to be divided into two large groups – these be noted that the vast majority of those who have committed these types of offences have higher or secondary special education. As for the gender characteristics of the attacker, it can be stated that criminal offences in the field of computer information are committed mainly by men. In the current period, a large number of people, both non-professional and highly qualified specialists, will be involved in the commission of computer crimes. At the same time, all of them have different social status and level of education, which already allows them to be divided into two large groups – these are both people who are in an employment or other employment relationship with the victim, and people who do not have a corresponding connection with the victim. The first group should include employees who abuse their position. These are different types of clerks, security guards, supervisors, people who deal withorganisational issues, engineering and technical personnel.

Computer security experts believe that amateur hackers are the most numerous, but the least dangerous. They account for up to 80% of all computer attacks. But these people are not interested in a specific target, but in the attack process itself, and they enjoy overcoming defence systems. For the most part, their actions can be easily stopped, since amateur hackers prefer not to take risks and avoid problems with the law. Most people of this type were connected to computers at school. Knowledge of computer technology is limited to one or two programming languages. The installation of criminal behaviour among amateurs happens spontaneously, mainly under the influence of a random chain of successful and unsuccessful "hacks" of security programmes on other computers. The consolidation of this attitude occurs under the influence of the "authoritative opinion of senior comrades", which they express after communicating with the "newcomer" in the network "lobbies". As the level of professionalization increases, amateurs acquire a deeper, more systematic knowledge of computer technology, programming languages, solid skills and abilities in working with networks, software, etc. This is related to the actual acquisition of higher technical education. They are already specialists. People in this group are psychologically more balanced, have a well-developed system of thoughts and values, but are not yet very ambitious. In most cases, the criminal "career" of such a group of people is transformed from an amateur "career" or developed by entering the criminal environment, for example, with the help and support of "professional" friends. The main areas of criminal activity of "specialists" are network hacking, actions in operations to obtain confidential information using powerful data protection systems, economic and mental espionage.

One of the most important elements for identifying a cybercriminal is motivation, the definition of which can provide information about the needs, interests, and characteristics of the suspect. Motives can be the following: political, ideological (for example, as a form of protest, so-called "hacktivists"); hooligan motives; self-serving (commercial calculation, thirst, material interests); sexual motive; obtaining specific items that have a special value in the cyber world or a higher unofficial social status, competition, technical challenge, struggle between human and artificial intelligence; the desire to have fun, assert themselves, prove intellectual abilities, curiosity, game; research, experiments on the study of software and technical electronic devices, networks, search for weaknesses, opportunities for them use and elimination; manifestations of sadism, painful imagination, pathological predisposition to destructive influence on society and public relations, obtaining moral satisfaction from the scale of destructive consequences; revenge (for example, for troubles at work), personal hostility; negligence, etc. (SHULZHENKO & ROMASHKIN, 2021). Sometimes the motives are complex or complementary to the main ones. The prerequisites for cyber sabotage are the following objective and subjective circumstances:

(1) Wide development of the high-tech industry and significant spread of computer technologies among the population;

(2) Availability of specialities in higher educational institutions that train students with the instillation of subject knowledge, programming skills, and knowledge;

(3) Influence of the family and non-family environment on the process of becoming the culprit of computer information;

(4) Actual impunity of persons who have committed computer crimes due to the high latency of these illegal actions, the lack of proper training of law enforcement officers involved in criminal proceedings on this category of crimes.

No less informative is the professional operation of investigative types of classifications of cyber criminals. For example, depending on their motives, they are divided into: hackers, criminals, vandals (In 2020, the National Police…, 2021). Depending on the purpose of committing a criminal offence, and the scope of application of professional skills, cyber criminals are conditionally divided into four groups: those who "crack" codes and passwords more through curiosity and self-affirmation, trying to find out what will happen for this (usually teenagers, students), by their actions they create serious obstacles to the normal operation of networks and computers; persons who are engaged in targeted theft of new software that is distributed for a fee. Characteristic of this category is the establishment of stable groups with a clear distribution of responsibilities among their members: some crack security codes and passwords, others are engaged in their implementation; computer hooligans who spread computer viruses that destroy software; criminals who hunt for confidential information, sometimes on order, receiving material remuneration for this.

In the specialised literature, there are a large number of other classifications of cyber criminals according to: age characteristics; professional and qualification characteristics (the most difficult to investigate are cases of combining professions); type of labour relations with the affected party; signs of employment; state of health, mental changes; gender characteristics; repeatability of criminal actions (recidivism); individual psychological traits; the ability to access information, the nature of encroachment on it; the method and purpose of committing; social status in society; the scope of crime; the state of awareness of crime actions (often the criminal is not able to fully foresee the consequences of their actions, which depend on many subjective and objective factors. This applies to professional violators of the operating modes of equipment, whose unintentional actions can lead to less serious consequences than a planned cyber attack); the number of performers, etc. At the stage of preparing for the interrogation of a cyber sabotage suspect, the investigator needs to conduct information support, investigate the suspect's identity and carry out planning. The main tasks of the interrogation are: identification of elements of the composition of cybercrime; establishment of its circumstances, method, motives, accompanying circumstances; identification of signs of cybercrime; establishment of the method of its concealment.

Next, the study considers the investigation of the identity of a suspect in cyber sabotage. Information is to be established by traditional investigative means: biographical data, previous activities (educational, labour); individual psychological characteristics (assigned forensic psychological and/or forensic psychiatric examination, visual observation is conducted, sources of open information are analysed for the study of professional interests, interests, hobbies, attitude to social phenomena, approval of criminal behaviour, etc. (sources of Information: groups in social networks, free ads); special and professional skills (pattern in crime of cyber criminals, which is expressed in certain ways, methods and techniques committing cybercrime, they can be detected by an involved specialist based on the analysis of the technology and method of obtaining illegal remote access (more often cyber criminals prefer to intercept information when transmitting it via telecommunications channels and computer networks, rather than directly entering the premises), establishing important technical data (IP(internet protocol), email address, mobile phone number); features of the subject of encroachment (for example, banking or commercial information); interaction with the victim or the affected organisation; time and place of the crime.

The investigator conducts research and compares data about a person from different sources. Thus, scientific studies on individuals who had information about those who committed cybercrime note that in 31% of cases other people had information about the plans of the criminal; in 64% of cases – colleagues, in 21% – friends, in 14% – family members, in 14% – accomplices (GVOZDETSKA e IZMAYLOV, 2016). Usually, cyber criminals think through their actions in advance and take measures to hide them. If the preparation for the commission of a crime takes place without the involvement of unauthorised persons, the search history in the browser or information from witnesses regarding the

search for special literature or special software tools by the suspect may become informative.During the interrogation, as in a normal interview, the investigator should identify contradictions, lies in the testimony, identify the person's attitude to the crime and be prepared for intellectual opposition from the criminal. The investigator and specialist should pay particular attention to the unsystematic unjustified destruction of obstacles (including in cyberspace), the absence of traces in places where logically they should be (staging), the nature of hacking (may indicate penetration from the inside of the room/internal server of the organisation). According to a study by IDG (International Data Group) Corporation, 88% of cases of information theft occur through employees of firms and only 12 % –through external penetration using special means (YAKIMOVA e BOROVIKOVA, 2016).

Therefore, the main danger is caused by internal users (or with their help). They commit 94% of crimes, while external crimes – only 6% (AIKOV e FONSTORCH, 1999). Notably, deliberate destruction of information is most often carried out by former employees or employees of the organisation in order to conceal other crimes or negligence. In cyber extortion, the criminal has access to information that is used when threatening the victim. The peculiarities of the interrogation of a perpetrator of cyber sabotage are the high intellectual level, the special psychological make-up of the interrogators, and the complex technical nature of the questions to be clarified. Recently, there has been a tendency to complicity in group cyber-attacks. Judicial practice shows that 38% acted independently, 62% – as part of organised groups and terrorist communities (SHEPITKO e ZHURAVEL, 2017). The most dangerous due to the ability to organise and commit cyber sabotage are organised groups of corrupt representatives of various state structures, special services that have almost unlimited financial capabilities, independently regulate and control Internet traffic, highly professional, educated, can enjoy the support of legislation and local authorities.

In order to prevent cybercrime, including cyber sabotage, the following technical and organisational measures can be implemented: periodic inspection of equipment for unauthorised access, statistical analysis of traffic to detect anomalies (with the help of a specialist or special software); maintaining a register, database of cyber criminals; introducing mandatory identification and verification of the Internet users; limiting the circle of intermediaries; constant testing and improvement of programmes for the state of protection of users' rights, especially in the field of public services; improving the protection of electronic digital signatures of users; informing internet users about the rules of cyber hygiene, risks and possible cyber threats (including in the cloud environment); establishing rules on the tactics of internet users' actions for typical, atypical and suspicious actions of unauthorised persons in cyberspace (recommendations); establishing technical and other types of restrictions (for example, setting network filters, using a virtual private network), etc. High requirements are also imposed on the investigator of the fact of cyber sabotage, they must have training at the level of a professional programmer or system administrator, be able to use the aappropriate software, understand the internal mechanisms of systems

and networks, be able to use certified software tools during a search and when collecting physical evidence.

CONCLUSIONS

Cybercrime is becoming more and more global, the latest technologies are turning real criminals into anonymous ones, and the ease of getting rich quickly attracts more and more people to join this criminal activity. Lack of demand for creative potential combined with ignorance of all the consequences of illegal actions – on the one hand, cold professionalism – on the other. These are just common features of cyber criminals. Their technical armament, knowledge, and skills far exceed the capabilities of law enforcement agencies, so improving law enforcement systems is becoming more difficult and expensive. Since the conditions of cyberspace differ significantly from real ones, in order to establish the process of occurrence of criminal intent, its nature, and the degree of public danger of the criminal, there is also a need to classify criminals depending on various subjective and objective factors. Prevention of cybercrime is based on measures aimed at reducing the risk of committing such crimes and neutralising harmful consequences for society and the public and private sectors. Effective counteraction combines a complex of legal (legislative), technical, organisational, and informational measures.

At the legislative level in Ukraine, many issues in the field of countering cybercrime remain unresolved. These are, first of all, gaps in the current legislation in the field of: information technologies, electronic proof, prevention and counteraction to the legalisation of proceeds from cybercrime, and the lack of sufficient investigative and judicial practice in criminal cases on the fact of cyber sabotage and single information and legal space that ensures legal awareness of all structures of society and each citizen separately. Advanced legal regulation can also be provided by: highlighting cyber sabotage and other crimes committed using computer technologies (cyber sabotage, unauthorised collection of information, cyber stalking, cyber investigation) in a separate group of illegal acts in the criminal law, strengthening criminal liability for cybercrime; improving the mechanism for recognising electronic documents and other data as an evidence base in the investigation of cybercrime; clear regulation of interaction between law enforcement agencies. Difficulties in obtaining the necessary amount information about the identity of the criminal are associated with their high latency, as noted above. These issues are rarely brought to the attention of law enforcement agencies, which allows tracking the characteristics of the criminal introduced in the form of technical developments. However, it is possible to use the above to create a portrait that meets modern realities. Paradoxically, attracting hackers to socially useful work can also help law enforcement agencies, as one of the measures to prevent computer crimes and solve those already committed.

REFERENCES

Aikov, D., Seiger, K. & Fonstorch, W. (1999). Computer crimes: A guide to combating computer crimes. Moscow: Mir.

Bilenchuk, P. D. (2001). Questions of social and criminological characteristics of a computer criminal. State and Regions, 4, 16-22.

Borysova, L. (2006). Subject (person) of transnational computer crime: forensic and psychophysical aspects. Current Issues of State and Law, 1, 76-81.

Borysova, V. I., Ivanova, K. Y., Iurevych, I. V. & Ovcharenko, O. M. (2019). Judicial protection of civil rights in Ukraine: National experience through the prism of European standards. Journal of Advanced Research in Law and Economics, 10(1), 66-84.

Cherniavskyi, S.nS., Holovkin, B.nM., Chornous, Y.nM., Bodnar, V.nY. & Zhuk, I.V. (2019). International cooperation in the field of fighting crime: Directions, levels and forms of realization. Journal of Legal, Ethical and Regulatory Issues, 22(3), 1-11.

Chernikov, B. Y. (2018). Criminological characteristics of cybercrime. Young Scientist, 11(63), 941-944.

De Fréminville, M. (2020). Cybersecurity and decision makers: Data security and digital trust. Wiley: ISTE

Denysova, O. O. (2003). Information systems and technologies in legal activity.Available at: http://ukrkniga.org.ua/ukrkniga-text/817/.

Dovzhenko, O. Y. (2019). On the question of tactics of interrogation in cybercrime cases. Scientific Bulletin of the International Humanities University, 37, 143-145.

Getman, A., Karasiuk, V., Hetman, Y. & Shynkarov, O. (2019). Ontological representation of legal information and an idea of crowdsourcing for its filling. Advances in Intelligent Systems and Computing, 836, 179-188.

Government Portal. In 2020, the National Police exposed more than 5000 cybercrimes. Available at: https://www.kmu.gov.ua/news/u-2020-munacpoliciya-vikrila-ponad-5-000-kiberzlochiniv.

Gvozdetska, M.O. & Izmaylov, K.Yu. (2016). Criminological characteristics of cybercrime: Current state, structure and specifics of committing. Current Challenges and Achievements in the Field of Cybersecurity, 2, 52-53.

Ivanchenko, O. Y. (2019). Criminological characteristics of cybercrime, prevention of cybercrime at the national level. Actual Problems of Domestic Jurisprudence, 3, 172-177.

Karachka, A. F. (2017). Technologies of information protection. Ternopil: National University of Economics.

Kozak, N. S. (2013). Forensic characteristics of persons who commit computer crimes. Scientific Bulletin of the National University of the State Tax Service of Ukraine (Economics, Law), 2(61), 186-191.

Kranenbarg, M. W., Ruiter, S. & Van Gelder, J. L. (2021). Do cyber-birds flock together? Comparing

deviance among social network members of cyber dependent offenders and traditional offenders. European Journal of Criminology, 18(3), 386-406.

Lutsenko, O. (2017). Bringing civil servants to liability for disciplinary misconduct in judicial practice of Ukraine, Poland, Bulgaria and Czech Republic. Journal of Advanced Research in Law and Economics, 8(1),103-112.

Maliy, M. I. & Bilenchuk, P. D. (2019). Cyberspace in the new millennium. Who are they: cybercriminals? Available at: https://cutt.ly/UZmm0d9.

Mayer Lux, L. & Vera Vega, J. (2020). The crime of cyber espionage: Definition and delimitation. Revista Chilena De Derecho y Tecnologia, 9(2), 221-256.

Peleshchak, O. R. (2021). Survey of the premises in the investigation of cyber diversions. Madrid: Barca Academy Publishing.

Pushina, N. L. (2020). Forensic characteristics of a person who commits criminal offenses in the field of economic activity with the use of computer technology. Scientific Notes of TNU named after V.I. Vernadsky, 31(70), 121-126.

Rychka, D. O. (2019). Peculiarities of the criminal-law qualification of crimes in the sphere of the use of electronic computers, systems and computer networks and telecommunication networks. Dnipro: University of the State Fiscal Service of Ukraine.

Shepitko, V. Y. & Zhuravel, V. A. (2017). Innovative principles of technical and criminalistic support of the activity of criminal justice bodies. Kharkiv: Apostil.

Shkolnyi, V. B. (2012). Some reasons for the emergence and development of crime in the use of computers. Law and Society, 2, 222-227.

Shulzhenko, N. & Romashkin, S. (2021). Types of individual criminal responsibility according to article 25 (3) of rome statute. Juridical Tribune, 11(1), 72-80.

Tacij, V. J., Tjutjugin, V. I. & Grodeckij, J. V. (2014). Conceptual model establish responsibility for offense in the legislation of Ukraine (draft). Criminology Journal of Baikal National University of Economics and Law, 2014(3), 166-183.

Titunina, K. (2006). Characteristics of computer crimes committed using the Internet (analysis of questionnaires). Fight against Organized Crime and Corruption, 21, 307-313.

Yakimova, S.V. & Borovikova, B.C. (2016). Personality of an economic criminal. Bulletin of the National University Lviv Polytechnic, 837, 521-527

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Note