# JURISPRUDENCE

## THE EFFECTIVENESS OF INFORMATION TECHNOLOGY IN THE PROTECTION OF HUMAN RIGHTS AND FREEDOMS IN AN OPEN SOCIETY

**Bondar V.**
*Ph.D., associate professor, head of the department of organization of scientific work of the Lugansk state university of internal affairs named after E.O. Didorenko, Severodonetsk, Ukraine*
**Bochkoviy O.**
*Ph.D., Senior Researcher, Leading specialist of the research and development laboratory for the prevention of the termination and investigation of crime of Lugansk state university of internal affairs named after E.O. Didorenko, Severodonetsk, Ukraine*
**Khankevich A.**
*Ph.D., Professor of the department of operative investigative activity and crimes investigation of the Kharkiv national university of internal affairs, Kharkiv, Ukraine*
**Shendrik V.**
*Doctor of Science, Professor, Honored Lawyer of Ukraine, head of the department of operative investigative activity and crimes investigation of the Kharkiv national university of internal affairs, Kharkiv, Ukraine*

**Abstract**

Rapid development of technologies provokes a revision of the existing attitude to the outside world including society. Areas of application of computer programs are diverse: space, defense, industry, education, etc.

New forms of organization of social relations (social networks, virtual reality, robotics, blockchain, etc.) are actively emerging, and the intensity with which they appear complicates the adaptation of existing social institutions to them, not to mention the forms of state control. The more personal data about an individual is aggregated and processed, the higher the possible impact on the life of such a person of automated processing results and, accordingly, the size of the risk associated with the violation of his rights.

This situation leads to a variety of contradictions both in the normative field and among the population.

The danger with the latest technology is that no rules of conduct have been formed, and therefore the institute of the responsibility for their violation has not been formed.

By ignoring the above mentioned social relations, the state poses a danger to the violation of the rights and freedoms of citizens, since it deprives them of the possibility of protecting them by the relevant law-enforcement bodies which operate exclusively within the legal framework which has not entered into new social relations.

The article provides an analysis of the above problem and possible ways of its solution in order to increase the effectiveness of the protection of the rights of citizens. The use of modern technologies in an open society greatly enhances the level of protection of the rights of citizens and the level of security in society.

**Keywords:** information technology, open society, citizen rights, protection, security, security, big data

In recent years, «Big Data» is a generally accepted trend of economic and technological development, which simultaneously forms many factors: 1) the penetration of the Internet in everyday life; 2) the development of e-commerce; 3) the emergence and development of search services, which are based on an advertising business model that involves the collection of large amounts of information about the behavior of individuals in the network on the Internet; 4) the emergence of social networks that aggregate data not only about individuals, but also about the relationship between them; 5) Distribution of smartphones and tablets, which allow you to constantly (online) track the route of their users, as well as exchange instant messages. As a result, the key processes of human life transmitted to the Internet and any action of the individual leaves a digital footprint, which in aggregate caused the appearance of huge amounts of digital information. At the same time, according to ICC, which specializes in analytics in the sphere of information technology, forecasts, most of the data will not be generated by humans, but by various devices during their interactions with each other and data networks (for example, smartphones, RFID devices, satellite navigation systems of the type (GPS).

Such rapid development of technologies provokes a revision of the existing attitude to the outside world including society. Areas of application of computer programs are diverse: space, defense, industry, education, etc. For example, special programs even carry out diagnostics of diseases in medicine and according to the doctors themselves, the accuracy of the diagnosis has increased to 90% [41]. During the comparative tests it was shown that due to intelligent software algorithms it is possible to increase the efficiency by reducing the di-

agnosis time to 70%. This makes it possible to significantly reduce the number of false diagnoses which plays a key role for the patient's health. In addition, there is a reduction in the time required for the recapture of diagnostic equipment, the need for repeated testing is reduced, the risk of legal consequences that may arise in the misdirection of the wrong treatment is reduced [34].

In the proceedings, the main digital technologies can be:

- large data (Big Date);
- neurotechnology and Artificial Intelligence (for example, "Bot Lawyer" is already able to file lawsuits against natural persons, artificial intelligence trained to foresee court decisions in cases of human rights abuses in the Strasbourg Court (ECHR) with a probability of 79%);
- distributed registry systems (for example, the use of blockade technology will be discussed further);
- quantum technologies (as one of the capabilities of computers based on (as one of the capabilities of computers based on quantum technologies, it is possible to provide cybersecurity and secure long-distance data exchange);
- components of robotics and sensorium;
- wireless technology (operational use of various data banks, accounting, conducting on-line procedural actions, etc.);
- technologies of virtual and supplemented reality (submission of evidence in court, modeling events in court process), etc.

New forms of organization of social relations (social networks, virtual reality, robotics, blockchain, etc.) are actively emerging, and the intensity with which they appear complicates the adaptation of existing social institutions to them, not to mention the forms of state control. The more personal data about an individual is aggregated and processed, the higher the possible impact on the life of such a person of automated processing results and, accordingly, the size of the risk associated with the violation of his rights.

This situation leads to a variety of contradictions both in the normative field and among the population. It is naturally that the unknown causes anxiety and fear. Catastrophic predictions and theories on the introduction of artificial intelligence became the ideas for many feature disaster films.

Insufficient understanding of the opportunities and the role of modern information technologies in the life of the society has led to the emergence of a three-dimensional problem:

1) the state has not developed effective mechanisms of influence and control in the field of new social relations which arose on the background of the rapid development of information technology;

2) the said omission on the part of the state was used by individuals who began to use modern information gains for criminal purposes while remaining unpunished;

3) the above-mentioned facts have created anxiety and threat to their rights and freedoms.

The reaction of society is fully justified and predictable. After all, anyone worries about the prospect of becoming a victim of a crime or subject to another violation of personal rights and freedoms. Despite the relative effectiveness of the provisions of the current legislation on personal data concerning the sustainable methods of processing data arrays isolated by individual organizations, the technology of "Big Data" is incompatible with a number of basic principles that form the basis of the legislation on personal data, which necessitates its reformation.

The danger with the latest technology is that no rules of conduct have been formed, and therefore the institute of the responsibility for their violation has not been formed. In particular, it is problematic to bring a person to the responsibility for illegal transactions with cryptic currency in a state that does not recognize the latter as a payment instrument.

Of course, any society can not exist without norms of behavior which are created only when the possibility of their violation is permissible. The law does not describe facts but benchmarks for our behavior. If this law has sense and meaning, then it can be broken and if it can not be broken then it is superficial and does not make sense. It is difficult not to agree with K. Popper, but what should be done when the legislator ignores the social relations that already exist?

By ignoring the above mentioned social relations, the state poses a danger to the violation of the rights and freedoms of citizens, since it deprives them of the possibility of protecting them by the relevant law-enforcement bodies which operate exclusively within the legal framework which has not entered into new social relations.

These topics are new to legal science in Ukraine, today some scholars (Rozovskiy B. [35, p. 280-292], Karchevskiy M. [18, p. 17], Konashevich O. [20] and others) draw attention to the need for appropriate responses by state authorities to the new threats, to prevent the ignorance of the social processes and information and technology progress that we are witnessing today.

For better understanding of the essence of the problem, and therefore to find ways to solve it, you need to understand two aspects.

Firstly, the level of the development and the possibilities of modern information technologies allow us to assert that we are heading towards the formation of an open society. Concurrently, in this case, we mean not Karl Popper’s concept [33] but an open society as an objective reality. Virtually every citizen today is in a virtual network. This happens regardless of whether we want it or not. It's almost impossible to stay out of the virtual network today, because being in the mother's womb, the information about the future person is being introduced to a variety of information records and computer systems. We can confidently say that in today's civilized world virtually every real person has a virtual twin.

Assuming that all systems and networks are united, the application of face recognition technologies combined with the active dissemination of CCTV will allow the observation of the life of any citizen in real time as in the film. Such a citizen becomes truly open to the structures that control such a system.

At the same time, it is necessary to clarify that, in the light of the above mentioned, calling the society open, we do not identify it with the information society which is often used as synonyms. The term "information society" is attributed to Professor Y. Khayashi of the Tokyo Institute of Technology [16, p. 62]. Further this term began to be widely used by other scholars in different fields of knowledge.

Some scholars define the information society as a whole as a society in which [6, p. 11-12]:

- every member of the society has the opportunity to receive timely and promptly through the global information networks full and reliable information of any kind and purpose, if found in practically any part of the geographical space;

- the possibility of operative, practically instant communication of not only every member of society but also certain groups of the population with state and public structures irrespective of place of residence is realized;

- the activity of mass media is transformed in the form of creation and dissemination of information, develops and integrates into information networks of television;

- geographic and geopolitical boundaries of states disappear within the framework of information networks, the unification of information legislation of the countries takes place.

The issues discussed were not ignored by the international community and were reflected in a number of international legal acts. For example, the Declaration of Principles "Building Information Society - A Global Challenge for the New Millennium" adopted by the United Nations in Geneva on 12.12.2003 states that the intention of States parties to build the people-centered, open to all and development-oriented information society [7] .

The Charter of the Global Information Society [25] states that in the information society, fundamental changes occur not only in the economy but also in other areas of activity. Scientific knowledge, modern information technologies, telecommunication and communication means are increasingly entering into everyday life of a person, substantially changing it. The information society allows people to more widely use their potential and realize their intentions, provide new opportunities for searching, storing, processing and disseminating information.

The information society should be also considered as [40]:

- a new type of the society which is formed as a result of the global social revolution and is generated by the development of information and communication technologies;

- a society of knowledge, that is, a society in which the main condition for the well-being of each person and each state is the knowledge gained through free access to information and the ability to work with it;

- a global society in which the exchange of information will have no time, spatial or political boundaries; which, on the one hand, promotes the interpenetration of cultures, and on the other hand, gives each community new opportunities for self-identification.

By combining existing concepts and positions individual scientists, by providing definitions, point to the interconnection between concepts of an informational and open society. Yes, Pastukhov P.S. notes that the information society is an open civil society based on free access to information, freedom of opinions, the right to direct voice, openness, tolerance and competition in opinions and evaluations [29].

In general, agreeing with the positions of scientists, we note that the concept of information and open society belongs to each other as a part and a whole. That is, an open society cannot exist without an appropriate information component in its modern sense with a set of systems, programs, and networks. At the same time, the information society becomes open only when an open civil position is formed when the security of every individual in the society is recognized as the highest value and is supported by all. An open society is a mental readiness of active behavior for public safety, including the use of modern information and technology achievements.

Of course, there are always threats of incorrect or illegal use of information obtained from relevant systems or networks. But we should not forget that criminals whose illegal activities will be visible to law enforcement agencies are similarly open.

Analysis of recent publications and practices has shown that most of the civilized world has long recognized the importance and inevitability of the introduction of modern analysis tools in the law enforcement sphere. So, in the English magazine "Police" the article on the use of modern information technology in the work of financial investigators has been published. At the beginning of the 21st century almost every person leaves behind an electronic track of information (for example, in the UK, the total number of databases where citizens can leave an electronic track is approximately three hundred). The investigators are faced with the task of collecting data from these databases in relation to a specific individual, then filtering from this information the ones that match the parameters of the investigation, that is, in other words, check the information received in relation to the wider context of the investigation in order to bring together all the information and conduct analysis according to which it is necessary to act in the future [32; 39, p. 22].

The ever-increasing cybernetization of information flows required a change in the existing staff structure of operational staff. In Scotland Yard (UK), the number of operational analysts exceeds the number of other ("classical") operational staff in 2.8 times while in the Federal Bureau of Investigation (US) - in 4.7 times. In the intelligence services (Central Intelligence Agency, USA) this figure reaches nine.

And this is understandable. The problem of today is that the information is too much: any modern sensor can transmit millions of terabytes of data and 5 thousand hours of high-definition video per day. This information is collected with gigapixel cameras and hundreds of sensors. Correctly organized analysis and visualization of these data will optimize the process of information and analytical support for criminal proceedings.

But to get the benefit of all these "mountains" of tera-bytes, scientists, who specialize in data analysis, for which the police have to compete with "civilian" industries, are needed.

Today there are already technologies that help automatically analyze huge arrays of texts, thus conducting not structural analysis and keyword search but semantic one. The system actually understands the content of the texts. In the long run, this same approach can be used to analyze video and static images as well as the sound.

These facts allow asserting that the development of analytical intelligence in Ukraine requires the withdrawal of the organization and tactics of law enforcement activities to a qualitatively new level.

In order to carry out computer intelligence specialized intelligence computer programs have recently been used. Due to its specific functions, intelligence programs, in comparison with other programs of search and analytical purpose, allow to expand the search zone, to reduce the search term, to discover latent links, to increase the value of the information received. Intelligence computer programs are the most universal and therefore the most widely used analytical intelligence tool. S.S. Ovchinskyi emphasizes the extremely important role of modern methods of processing various information for the formation of analytical intelligence as "an independent form of the activity" [28, p. 319].

As O.V. Demyanchuk writes, computer networks, first of all the Internet, are increasingly used by intruders for creating illegal markets for the sale of weapons, drugs, human organs, pornographic products, explosive devices, offers for providing of killer "services", and is a way of spreading information on the manufacture of homemade explosive devices, propaganda of national enmity and calls for entering into a war [8].

Law enforcement agencies of foreign countries widely use automated information search systems that allow to optimize the disclosure and investigation of crimes committed by members of organized groups significantly [19]. But the current pace of exchange of information and the overall rhythm of life, including criminal, makes it necessary to constantly improve methods and ways of working with constantly growing data arrays. In this process, irreplaceable assistants are information and analytical systems, the main advantage of which is analysis and forecasting.

Moreover, up to-day technologies make it possible to actively and productively counteract transnational crime at the expense of the absence of boundaries in the global network. The interaction and exchange of data between law enforcement agencies of different countries is greatly facilitated. For example, a wanted offender can be identified by using one of the identification software for a person on the photo or video image. Such experience is already practiced by individual foreign public and private agencies [23; 26; 5].

Space industry has more prospects in using the latest technologies. After all, in the distant 1962 M.S. Khrushchev, after successful trials of means of anti-rocket defense in the USSR, said: "We can aim at the fly in space" [37].

Today, in the US, a space control system is being developed that can observe ground-based processes even through clouds [12; 38]. Today, 12,000 artificial satellites have been taken into the Earth's orbit [1].

At the same time, not a single fact of using space satellites for the purposes of law enforcement sphere is known. First of all, this is due to technical capabilities and financial expediency. But work in this direction is being actively pursued and already there are first successes in the transmission of satellite image in real time regime [4; 30]. At the current pace of scientific and technological progress, technical capabilities of space monitoring for law enforcement purposes will quickly appear.

Secondly, the outdated system of public administration as well as its regulatory legal basis is not able to adapt to the rapid development of information technologies and society in general which creates significant contradictions that do not contribute to the protection of the rights and freedoms of citizens.

In the real world, in order to meet their needs, there are a huge number of restrictions and prohibitions that are not present in the virtual world. In particular, in the virtual network there are no borders, distances are leveled, the network is deprived of excessive legal regulation etc.

What the network is not deprived is the control that is carried out by the appropriate administrator and the level of controllability depends on the administrator himself since he sets the rules that will operate on the network. Thus, each network can, conditionally, be compared with the form of organization of the society (union, community, state etc.) as well as its guidance.

Thus, with the development of the network, its prevalence, the forms of its regulation have become more complicated that can eventually lead to the consequences with which some states are encountered. Already today we are witnessing the expansion of the staff of legal advisers as legal standards that need to be reconciled with the existing ones are constantly increasing. And than farther, this process becomes more complicated. Excessive overregulation leads to inconsistencies in legislation which, in its turn, leads to the violation of the rights of individuals and legal persons and to a certain chaos. In the future the attempts of each of the subjects of the society to protect only their rights and freedoms, a measure for which everyone has his own, provoke the introduction of repressive measures from the side of the state to resolve the situation. The results of such actions can be different, from the change of power or the introduction of authoritarian rule till the collapse of the state as such.

A successful historical illustration of the above process is the Roman Empire. Beginning in the 2nd and 1st centuries BC as a city-state, Rome had become a good example of the successful realization of the direct democracy as a form of state rule which had previously taken place in the Athenian republic since the 5th century BC and is considered to be the earliest known direct democracy [21].

All government positions were elective and the state apparatus itself was kept to a minimum. In Rome

there was no police, prosecutor's office or special services. Of all the instruments of the state influence they had only the army [3].

Such a management system was extremely effective for the well-being of citizens and was soon appreciated by residents of other areas around Rome. In the I-II centuries the Roman Empire grew rapidly due to the fact that in all conquered territories the local population was rapidly organized on the principle of Roman municipalities. In essence, the empire gave the state control over outsourcing, that is, it was managed through self-governed cities organized according to the Roman model.

In essence, at the initial stage, the Roman Empire was a network of self-regulated cities, which at basilar level were a classic example of a horizontal system. And it is in such a system that the Roman Empire had developed.

Not going deep into the historical discussions about the causes of the collapse of the Roman Empire, hardly anyone denies that one of the most important factors that accelerated the decline of the empire was the overload of the management of factors at which it was not able to react at that time. Moreover, the human factor in the form of growing appetites of the local nobility provoked a rejection of a one-level self-regulated urban network [22]. Consequences are well-known.

The further the society develops, the more complex and modern forms of organization it needs.

Modern information society, whose representatives we are, obviously requires such a form of its organization that could combine both its real and virtual sides. One of the outputs may be the introduction of blockchain technology - one-level network in which there is no single distinguished center and in which the validity of transactions is guaranteed by a crypto algorithm and, accordingly, by all participants of the network.

Blockchain is a distributed database in which data storage devices are not connected to the general server. This database stores a list of ordered records called blocks which constantly increases. Each block contains a timestamp and a reference to the previous block. Most frequently copies of the chain of blocks are stored independently from each other and are processed on different computers. The basic principle of the operation of the new technology is the transparency of the operations carried out with the impossibility of their change by persons who do not have authorized access to it.

Blockchain technology uses cryptography and digital signatures for identity verification: transactions are tracked up to cryptographic identification data that are theoretically anonymous but can be attached to real identifying data after some engineering analysis.

From the above mentioned it can be concluded that the function of the blockchain technology is to register each transaction with a crypto currency. Any transfer of crypto currency is confirmed on the network by bringing a transaction block. The block is added to the long chain which allows anyone to track the change of owners of each crypto currency from the moment of creation. Technically, this is achieved by sequential enciphering of data for each subsequent transaction. Any transaction entered in the block is assigned a cryptographic identifier (hash) which is added to the heading of the record about the next transaction, and it is repeated again and again so that the transaction hash on the top of the chain contains coded data about all previous transactions written in the block. It is impossible to intervene and change a transaction already written because it will compromise the whole chain.

The very fact that the blocks are correctly embedded in the circuit shows that the transaction was in the proper manner. So the block represents simultaneously both the confirmation of the transaction (with an electronic signature and a mark on the time of committing), and part of the total (across the entire network) transaction history. It is possible to use encipher with the open key, which is entered into the database, for identification in the registry of the holders of crypto currency. Only the owner of the closed key has the right to continue to deal with these crypto currencies. Yes, enciphering provides the necessary confidentiality, except that only the owner of the closed half of a pair of keys can accept a transaction. Thus, the user has only one key and with his ignorance it is impossible to access the primary information.

The considered technology of data transfer and storage has become the focus of attention of those who commit crimes. In the area of their special attention there was also crypto currency which, in essence, is not a means of payment in the literal sense but in fact has already become a substitute for issued payment means.

Crypto-currency actions do not have specific legislative regulation and criminal offenses cannot be identified. Marco Strang describes crypto currency as follows:

- non-inflationary;
- divisibility;
- duration;
- accessibility;
- globalization and, as a rule, anonymity;
- open source code;
- one rank;
- decentralization.

However, when committing crimes in the online space crypto currency act as a means of committing crime and are used as a means of payment for the purchase of weapons, narcotic drugs and other prohibited objects, or in order to legalize criminal profits.

One of the most popular ways to handle crypto currency for criminal purposes is through crypto currency exchange. The list of all crypto currency exchanges and bitcoin exchangers, Litecoin and their forks at the beginning of June 2016 contained the following data about their location: US - 25; Germany - 8; Russia - 6; China - 3; Poland, Great Britain, France, Taiwan - 2; Kazakhstan, British Virgin Islands, Ukraine, Canada, Switzerland, Bulgaria, India, New Zealand, Australia, Belgium - 1.

When it comes to legal regulation of bitcoin and other crypto currency in Ukraine (PPCoin or Peercoin), first of all they recall the explanations of the NBU in the Letter dated 08.12.2014 No. 29-208 / 72889 which defines Bitcoin as a "money surrogate" that does not have security of the real cost and can not be used by

individuals and legal persons on the territory of Ukraine as a means of payment, as this, in his opinion, is contrary to the norms of Ukrainian legislation.

If you consider the Law of Ukraine "On Payment Systems and Money Transfer in Ukraine" dated September 18, 2012, No. 2921-14, electronic money is a unit of value stored on an electronic device that is accepted as a means of the planet by persons other than those who release them and is a monetary obligation in cash or non-cash forms. The issuance of electronic money can be carried out exclusively by the bank which has obligations to repay them.

Due to its technology Bitcoin does not fall under the Ukrainian definition of "electronic money" because it does not contain an obligation of the issuer to repay it, has no single emission center, it is not tied to any cash or cashless funds. In turn, "non-cash funds", according to Ukrainian legislation, can exist only in the form of records on bank accounts. Banks do not participate in the process of issuance and circulation of crypto-currency, so Bitcoin can not be considered "funds". Bitcoin does not fall under the definition of "payment system" as the main and obligatory function of the payment system is the transfer of funds while Bitcoin is transferred exclusively through the electronic wallet, which is not money.

To clarify the legal nature of Bitcoin, it is important to draw attention to the fact that the Law of Ukraine "On the National Bank of Ukraine" dated May 20, 1999 No. 679-14 stipulates that money surrogate is any documents in the form of banknotes which are different from monetary unit of Ukraine, issued in circulation not by the NBU and made for the purpose of making payments in economic circulation. At the same time, signs of crypto-currency are not covered by the term "electronic document" since the latter refers to a document which information is recorded in the form of electronic data taking into account the necessary essential elements of the document.

Thus, one should agree with the opinion of scientists that the concept of crypto-currency is not recognized as money surrogate, and that the activity regarding the use of Bitcoin in the payment of services in Ukraine is innovative, the corresponding legal regulation and clear definition of the status of crypto-currency as such are completely absent.

However, technology, during its existence since 2009, has never been the victim of hacking or other unauthorized influence [31].

If, however, the information is stored in the blockchain then the information becomes invulnerable to external interference. In addition, there is no need for mediation which is the basis of state influence.

The indicated technology is actively implemented in the developed countries of the world. So, modern Switzerland is a rare example of a country with instruments of direct democracy. Citizens can directly propose amendments to any law or even to the Constitution [15].

We agree that in a civilized legal state the person, his interests, rights and freedoms must be the highest value. However, as if we did not magnify the personality, it was, is and will remain a part of the society. Consequently, the interests of the individual can not be opposed to the interests of the society which we observe today.

In today's realities unjustified competition between democracy and the security of individuals and society is impermissible. As the researchers note, "security is a complex social phenomenon that in a contradictory way reflects the relations of various social subjects. Often, some of them seek to provide their own security at the expense of others or in their activities they do not take into account the interests of other social groups and their need for security. In this case, the speech should be about a sort of "social selfishness" which, if it was relatively tolerant in the previous era, in the era of growing globalization it begins to become a serious threat itself ". Confronting the security of the person and the safety of social security in general, as a rule, arises in historically specific circumstances connected, oddly enough, with relatively stable and safe periods of the development of one or another society. The events of September 11, 2001, perfectly confirm this, since to this day the United States had long been unaware of the serious security problems, public opinion perceived the value of security as given and moved it aside on the second plan. It is logical that at some point of the idea that security interferes the freedom of the individual, changed the perceptions of security as a necessary condition for freedom "[24, p. 102-105]. In addition, narrowly-verified assessment of the citizen of his rights and freedoms with their indisputable priority but outside the interests of the society is unacceptable [36, p. 350-355].

To illustrate the principle of the work of the blockchain technology we can give an illustrative example. Let's imagine that there are many people in the big room (in the relevant network) who simultaneously watch two persons discussing the terms of the contract between each other and sign a contract. Everyone sees how the negotiators reach an agreement and place the signed contract into a glass block which is closed and sealed with the signatures of all people present. After closing the block can not be opened but you can read from it. Any actions in the room are immediately visible to all participants and non-fulfillment of conditions immediately becomes known to all members of the network. In this case, any actions with a packed contract are fixed in an automatic mode and are also placed into a block, on the top of the one which already exists and is also confirmed by all the participants who do not have any administrative rights.

Now, this primitive example is multiplied by the capabilities of computer systems and data processing programs and you will get an approximate idea of the principle of the blockchain technology which, however, is extremely important for the development of an open information society.

Today we are witnessing the monopolization and localization of certain information resources. Most databases belong to a state that has established a monopoly on their use arguing that they need to be protected and providing allegedly guarantees for such protection.

At the same time, any database can be cracked and obtained confidential information or distort it. Security systems are created by people and therefore people can break them. So, recently, information systems around the world have become the object of the attack of the virus Petya.A from which the information systems of Ukraine were affected most of all. The work of many state bodies and institutions as well as of most state banks was paralyzed. Against this backdrop, the bitcoin course only grew and the technology itself, during its existence since 2009, has never been the victim of breaking in or other unauthorized influence [31]. There are other examples of leakage of confidential information including India:

- Reliance Jio (2017) - 120 million customers;
- Aadhaar (2017) - 210 government sites made confidential information publicly available.

If, however, the information is stored in the blockchain then the information becomes invulnerable to external interference. In addition, there is no need for mediation which is the basis of state influence. After all, in case of purchase of a vehicle, the contract requires a notarial certificate and the fact of the proof of its ownership requires registration at the service center of the Ministry of Internal Affairs. In the same case, intermediaries are not needed to record information with the help of a blockchain in the form of a token (the digital expression of any material or not material object).

In small social groups such a system operates constantly and does not raise any questions. In the family children do not require parents to show them documents every time to prove their parenthood or students in the classroom are not forced to confirm weekly that they are from this class.

If the group increases, for example, to the size of a city or region, even such elementary questions as confirmation of the status give rise to difficulties. To enroll for work you need to provide documents on education, confirmation of family ties, criminal record or its absence, etc.

The blockchain technology, together with the comprehensive informatization and automation of the society, makes it as open as possible on the one hand, and on the other it is extremely protected.

When everything is open, it's extremely difficult to steal it. How to take something out of the table unnoticed when this table is in the middle of the room and all around are looking at it? It is impossible.

The introduction of the principle of the blockchain technology at the national level has definitely unquestionable advantages. But is society ready for such changes mentally? We do not think so.

The current level of corruption and oligarchization of the state apparatus will not allow the introduction of such technology. Indeed, even the filling of elementary electronic declarations by civil servants can not be provided within a year yet. In Ukraine there is no single information center that would allow monitoring the financial flows of citizens to control the level of illegal enrichment of officials. Even elementary databases of law enforcement agencies do not have a single coordinated center. What to talk about changing the technology of accumulation and processing of information.

But there is hope for more developed states. The successful implementation of the blockchain technology at the state level at least by some countries will motivate others.

In particular, the way Switzerland is developing is very inspiring. So, modern Switzerland is a rare example of the country with instruments of direct democracy. Citizens can directly propose amendments to any law or even to the Constitution. From 521 referendums, in 216 cases, the subject of the vote was the revision of the Constitution and, in 148, the subject was the laws, cases of adoption of a bill or approval of any contract. The people also do not fall behind two hundred of referendums were initiated by the ordinary Swiss person. For the people's initiative, according to the Swiss Constitution, 100,000 signatures of citizens are needed. The subject may include, in particular, review of the Basic Law. Additionally, Swiss may use the right to an optional referendum. It concerns international agreements, federal decisions, joining unions and international organizations. For this, support is required from 50,000 people or 8 cantons [15].

Moreover, Switzerland itself is a country that is trying to keep up with the times and transform its instruments of direct democracy into a digital format called e-Direct Democracy (EDD) or Direct Digital Democracy (DDD) [17]. Electronic direct democracy is sometimes referred to as terms of open source or common management [27].

So far, this is an experimental system and has not yet been fully implemented, in most cases it is used as innovative grant projects [10] but this process is gaining momentum and the blockchain technology extends the horizons for the application of such a system greatly.

In addition to Switzerland other countries have started the path of digital democracy: Australia, Sweden, Great Britain, India. In particular, the People's Administration Direct Democracy Party [9] is the first major party in direct democracy that was registered at the country's electoral commission. This party has developed and published a complete scheme of legislative implementation of the EDF reform. Founded by musicians and political activists, the People's Administration supports the use of the Internet and telephony to provide the majority of voters with opportunities to create, offer and vote on all political issues. The People's Administration project has been published in various forms since 1998. The People's Administration is the first in the world party of direct democracy registered in a format that allows voting.

There are first small steps in Ukraine. The first direction of using the blockchain technology is the eAuction 3.0 e-auction, which is currently being tested in Bila Tserkva, Odesa and Kherson [14]. In particular, Mayor of the White Church Gennadyi Dykyi registered a draft decision on the introduction of eAuction [13].

Moreover, discussions have begun on the use of technology on the platform block (e-Vox) for organizing and holding elections [11].

Therefore, an urgent need is an integrated solution which uses technology without human intervention to enforce the rules and provides:

- protection from internal malicious people who deliberately distort the data;

- protection against unauthorized external interference;

- mechanism for obtaining consent of people for every use of their personal data.

At the same time, the technology of the "Big Data" reveals the obvious fact: the legislation on personal data in the form in which it was formulated in the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data adopted by the Council of Europe on January 28, 1981, in the future supplemented by the protocol on the powers of supervisory bodies and transborder data transmission, is becoming less and less adequate to modern technological realities and needs substantial improvement.

The following basic categories such as the concept of personal data and the notion of the operator of personal data should be redefined. In a situation where the collection of information about users is massive even a harmless fragment of such information (information about visiting a site or making a purchase) combined with other similar information can provide more information about a person than a set of personal data. Are such units of special regulation information deserving of the status of personal data? Or does it make sense to allocate them to a special category with a separate regulation? Does the anonymity or use of the pseudonym affect the ability of qualification of the relevant information as personal data? These issues need to be solved. These data of users are one of the sources of multibillion profits from social networks, search services and other IT companies. However, this fact is ignored by the majority of users as well as Ukrainian legislation which does not recognize the provision of personal data for processing as a counterclaim for the qualification of a contract (Article 632 of the Civil Code of Ukraine).

In a technological sense, materials of any criminal proceedings can be presented as a set of procedural and other documents containing criminally relevant information and also reflect the course and results of the pretrial investigation of an event that contains signs of a crime. Each document digitally (of course, all documents that are in criminal proceedings must be translated into digital format including photo and video images of objects - the material evidence that appear in the proceedings) is such a block. This block has a label: the date and time of this document.

From the very beginning, the mandatory prohibition on any change of documents is considered obligatory since it is necessary that the information about time, sequence, participants in procedural actions etc., do not allow different interpretations and remain in the original form.

Security in blockchain technology is provided through a decentralized server that delivers the specified time labels and peer-to-peer network connections. As a result, a database is created which is managed autonomously without a single center. It makes the chain of blocks very convenient for registering events (for example, registration of received documents, protocols of investigative (search) actions, obtaining a decision of the investigating judge on granting permission to conduct investigators on secret investigative (search) actions related to restriction of rights and human freedoms, making medical records) and data operations, managing the identification and verifying the authenticity of the source. This allows us to derive compliance with the requirements of Part 1 of Art. 86 CPC of Ukraine about that the evidence is admissible if it is received in the established order to a qualitatively new level. Only investigator who has one closed key and a procedural supervisor who has another one has the access to the records. Then, only those to whom one of these users will provide has closed key will only be able to get the access to this information. For example, a forensic expert institution, in the case of setting an expert examination or investigating judge or lawyer within the limits of the realization of powers foreseen by the CPC of Ukraine. The above mentioned persons see all contents of the folder with the materials of the criminal proceedings (no hidden files); it can be quickly looked at: who, when and in which subfolders they downloaded the documents.

However, the level of access to file data must be delimited. Someone can only view the list of documents in each folder. And someone (the addressee of a particular document) can get acquainted or download data to himself.

Moreover, nobody else can get the access the file - only one to whom it was intended.

Consequently, there are a lot of benefits provided by the blockchain technology in case of its use in the criminal process.

The level of publicity will be increased without the loss of confidentiality of the investigation data, the investigation period will be reduced, issues related to the procedures for judicial control and procedural management will be promptly resolved, the quality of investigation will be improved etc.

However, as realists, we are forced to state that the introduction of new technologies in the domestic state structures is extremely low. Even long-used techniques and methods of using information technologies in other countries are not used for law enforcement purposes. The main problem of today which does not allow the application of the blockchain technology and the programs developed on its basis in public administration is the lack of a regulatory legal basis [2].

The hope is that the rapid development of other states will not allow Ukraine to ignore the latest technologies and we will develop although with a certain delay.

**REFERENCES:**

1. 12 thousand space satellites under control. Russia is not afraid of star wars. Available online: http://tvzvezda.ru/news/forces/content/201503051818-pdbu.htm (accessed on 15 december 2018).

2. Bitcoin against bureaucracy: how Ukraine moves to blockchain. Available online: https://ain.ua/2016/09/14/bitcoin-protiv-byurokratii-kak-ukraina-perexodit-na-blokchejn (accessed on 16 december 2018).

3. Cary M. A History Of Rome: Down To The Reign Of Constantine (2d.ed). / M. Cary; H.H. Scullard. London : Macmillan ; New York : St. Martin's Press, 1967. 820 p.

4. Cosmos is closer than it seems. What can spy satellites consider. Available online: http://zelenyi-kot.livejournal.com/47205.html (accessed on 15 december 2018).

5. Created a program to search for people on the Internet for photos. Available online: http://zhzh.info/blog/2011-11-13-3096 (accessed on 15 december 2018)

6. Crystalniy B. Informatsionnoye obshchestvo, informatsionnaya politika, pravovaya informatsionnaya zashchita. Informatsionnoye obshchestvo [Information Society, information policy, legal information protection. Information society]. 1997. № 1. P. 9-12. (in Russian)

7. Declaration of Principles "Building the Information Society - A Global Challenge in the New Millennium" of December 12, 2003. Available online: http://zakon4. rada.gov.ua/ laws/show/995_c57 (accessed on 16 december 2018).

8. Demyanchuk E.V. Monitoring seti Internet kak meropriyatiye, provo-dimoye s tsel'yu polucheniya operativno znachimoy informatsii [Internet monitoring as an event, conducted in order to obtain timely information]. Special technical support for law enforcement agencies: materials of the II International Scientific and Practical Conference. Kyiv nat. University of Internal Affairs, 2006. p. 171–178. (In Ukrainian)

9. Direct Democracy. Available online: http://www.paparty.co.uk. (accessed on 15 december 2018).

10. Electronic Voting in Switzerland. Available online: http://web.archive.org/web/20070212194901/www.swissworld.org/dvd_rom/eng/direct_democracy_2004/content/votes/e_voting.html (accessed on 15 december 2018).

11. E-Vox electronic petitions blockchain service selected for participation in the EGAP incubator. Available online: http://forklog.com/blokchejn-servis-elektronnyh-petitsij-e-vox-otobran-dlya-uchastiya-v-inkubatore-egap/ (accessed on 15 december 2018)

12. How the Pentagon is preparing for a new space war. Available online: http://www.dsnews.ua/future/kak-pentagon-gotovitsya-k-novoy-kosmicheskoy-voyne-11052016224400 (accessed on 15 december 2018).

13. In Belaya Tserkov, bidding for e-Auction 3.0 took place. Available online: https://bitcoin-conf.com.ua/ru/news/v-beloy-tserkvi-sostoyalis-torgi-na-eauction-3-0-52509 (accessed on 15 december 2018)

14. In Kiev, signed a historic Memorandum on the launch of the blockchain platform e-Auction 3.0. Available online: http://forklog.com/v-kieve-podpisan-istoricheskij-memorandum-o-zapuske-blokchejn-platformy-e-auction-3-0/ (accessed on 15 december 2018)

15. Ivanov V. In Switzerland 150 years more than 500 referendums were held: Vladimir Ivanov's blog. Available online: http://blogs.lb.ua/vladimir_ivanov/159889_shveytsarii_150_rokiv_shveytsarii.html (accessed on 15 december 2018).

16. Izmailova E.V. Informatsiya v kommercheskikh otnosheniyakh. Vestnik Moskovskogo universiteta[Information in a commercial relationship. Bulletin of Moscow University]. Ser. 11: Right. 2005. No. 1. P. 62–79. (in Russian)

17. Jan A.G.M. van Dijk. Digital Democracy: Vision and Reality. / Jan A.G.M. van Dijk, // I. Snellen & W. van de Donk 'Public Administration in the Information Age: Revisited', IOS- Press, 2013. p. 49-63.

18. Karchevskiy M. «Klasychni» ta novitni problemy kryminal′no-pravoho rehulyuvannya u sferi informatyzatsiyi. Aktual′ni pytannya kryminal′noho prava, protsesu i kryminalistyky, udoskonalennya diyal′nosti sudovoyi i pravookhoronnoyi system ["Classic" and the latest issues of criminal law regulation in the field of informatization. Actual questions of criminal law, process and criminalistics, improvement of activity of judicial and law enforcement systems]: mater. Allukr science-practice conf. (Severodonetsk, May 19, 2017). Severodonetsk: Lugan. state united-in deal with them EO Didorenka, 2017. pp. 11-19. (In Ukrainian)

19. Khirsin A.B. Udoskonalennya avtomatyzovanykh informatsiyno-poshukovykh system, yaki vykorystovuyut′sya u borot′bi z orhanizovanoyu zlochynnistyu. Pravo Ukrayiny [Improvement of automated information retrieval systems used in the fight against organized crime. The law of Ukraine]. No. 6 2004. p.55-60 (In Ukrainian)

20. Konashevich O.I. Legal grounds for the implementation of services and goods for bitcoins. Available online: http://jurliga.ligazakon.ua/blogs_article/725.htm (accessed on 15 december 2018)

21. Kurt R. Origins of Democracy in Ancient Greece. / Raaflaub, Kurt A.; Ober, Josiah; Wallace, Robert W. 2007. Berkeley: University of California Press. p. 5.

22. Latynina Y. Blockchain electronic analogue of freedom. Invented a way to get rid of excessive state care. Available online: https://www.novayagazeta.ru/articles/2016/06/06/68894-blokcheyn-elektronnyy-analog-svobody. (accessed on 15 december 2018)

23. Looking for a person through a photograph is a reality. Available online: http://softo-pirat.com/main/399-poisk-cheloveka-po-fotografii-yeto-realnost.html (accessed on 15 december 2018)

24. Mozdakov A.Yu. Sotsial'naya bezopasnost' i bezopasnost' lichnosti. Gosudarstvo i pravo [Social security and personal security. State and law]. 2008. No. 6. P. 102–105. (in Russian)

25. Okinawa Charter of the Global Information Society, July 22, 2000. Available online: http://www.conventions.ru/view_base.php?id=13180 (accessed on 15 december 2018)

26. On the photo in the social network you can learn all about the person! Available online: http://3rm.info/publications/13829-po-foto-v-socseti-

mozhno-uznat-o-cheloveke-vse.html (accessed on 15 december 2018)

27. Open Governance and the Definition of e-Democracy. Available online: http://www.gov2u.org/index.php/blog/128-open-governance-and-the-definition-of-edemocracy (accessed on 15 december 2018).

28. Ovchinsky S.S. Operativno-rozysknaya informatsiya. Teoreticheskiye osnovy informatsionno-prognosticheskogo obespecheniya operativno-rozysknoy i profilakticheskoy deyatel'nosti organov vnutrennikh del po bor'be s organizovannoy prestupnost'yu [Operational search information. The theoretical basis of information and prognostic support of operational-search and preventive activities of internal affairs bodies in the fight against organized crime]. M .: INFRA-M, 2000. 367 p. (in Russian)

29. Pastukhov P.S. Modernizatsiya ugolovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva [Modernization of criminal procedural evidence in the conditions of the information society]. Specialty: 12.00.09: Abstract. dis. on the competition Degree Doctor of Law Moscow, 2015. 65 p. (in Russian)

30. Planet Earth in real time. Available online: http://www.infokart.ru/planeta-zemlya-v-realnom-vremeni/ (accessed on 15 december 2018)

31. Podobriy O. In Bitcoin there is one negative point - a scientist from Italy. Available online: https://www.obozrevatel.com/finance/business-and-finance/19048-bitkoinyi.htm (accessed on 15 december 2018)

32. Police. 2001. September. P. 24–27.

33. Popper K. Otkrytoye obshchestvo i yego vragi. T. 1: Chary Platona [Open Society and its enemies. T. 1: Plato's spell]. Tr. from English, ed. V.N. Sadovsky. M .: Phoenix, International Foundation for Cultural Initiative, 1992. 448 p. (in Russian)

34. Review: IT in Healthcare 2014. Available online: http://www.cnews.ru/reviews/publichealth2014/articles/po_pomogaet_povysit_kachestvo_meditsinskoj_diagnostiki. (accessed on 15 december 2018)

35. Rozovskiy B.G. Pravo kak kletka v zverintse [Right like a cell in a zoo]. Bulletin of the Lugansk State University of Internal Affairs in the Name of E.O. Didorenka. 2017. No. 1. P. 280-292. (in Russian)

36. Rozovskiy B.G. Protivoprestupnoye pravo: popytka sinergii mer pravovogo regulirovaniya [Crime law: an attempt to synergize regulatory measures]. *Criminal Code of Ukraine: 10 years of expectations: Abstracts and reports of participants of the International Symposium September 23-24, 2011 Lviv: Lviv State University of Internal Affairs, 2011. p. 350-355.* (in Russian)

37. The New York Times, July 17, 1962.

38. The US Army is completely dependent on satellites. Available online: http://genocid.net/news_content.php?id=4470 (accessed on 15 december 2018)

39. Vyyavleniye prestupnikov s pomoshch'yu informatsionnykh tekhnologiy. Bor'ba s prestupnost'yu za rubezhom [Detection of criminals using information technology. The fight against crime abroad]. Newsletter. M: VINITI, 2003. No. 6. P. 19-23. (in Russian)

40. White Paper on growth, competitiveness and employment – the challenge and ways forward into 21st century // European Commission. Belgium, 1993. 54 p.

41. Zhmudyak L.M., Zhmudyak A.L. Disease Diagnostic Program. Available online: http://www.swsys.ru/index.php? page=article&id=2341. (accessed on 15 december 2018).

## COMPARATIVE ANALYSIS OF THE BEGINNING OF THE pre-trial proceedings: IN MODERN DIMENSION

**Maksimenko V.**
*graduate student of the department of the criminal procedure and criminalistics of the Institute of Law named after Vladimir Stashys Classic private university*

## КОМПАРАТИВНИЙ АНАЛІЗ ПОЧАТКУ ДОСУДОВОГО РОЗСЛІДУВАННЯ: У СУЧАСНОМУ ВИМІРІ

***Максименко В.В.***
*аспірант кафедри кримінального процесу та криміналістики Інституту права імені Володимира Сташиса Класичний приватний університет*

**Abstract**

The article analyzes some problems that arise at the beginning of the pre-trial proceedings, namely, the possibility and effectiveness of judicial control at this stage. On the basis of a comparison of the legal norms of the recent past and the existing criminal procedural legislation, the similarities and differences between them are established and ways to solve the problem are proposed.

**Анотація**

У статті проаналізовані деякі проблеми, що виникають на початку досудового розслідування, а саме можливість та ефективність судового контролю на цій стадії. На основі порівняння правових норм недалекого минулого та чинного кримінального процесуального законодавства з'ясовано подібності та відмінності між ними й запропоновано шляхи вирішення проблеми.