Palingenesis of Criminal Law in the Conditions of Digital Reality

Evgeny Russkevich

Associate Professor, Department of Criminal Law, University of the Internal Affairs Ministry, Candidate of Juridical Sciences. Address: 12 Akademika Volgina Str., Moscow 117997, Russia. E-mail: russkevich@mail.ru

Abstract

The article proves that the influence of exponential and combinatorial technological changes has led to a crisis of criminal law, which is expressed in the inability to perform its basic functions due to the permanent and dynamic external environmental impact. The author identifies the following fundamental provisions that should be relied on when making decisions on the modernization of criminal law: the emergence of a new (informational) method of committing a crime does not a priori indicate that it is more dangerous than the traditional one, but in many respects indicates the problem of lag social control from the development of society and changes in crime; the adaptation of the norms of the criminal law to the conditions of the information society should not be associated with the construction of "digital twins" of traditional criminal law prohibitions; the introduction of appropriate amendments to the content of the norms is justified only in cases where the adaptive capacity of criminal legislation to manifestations of digital crime exhausts itself; the recognition of the use of information technologies as a qualifying feature of a crime in general must comply with the criteria for differentiating criminal liability justified in science. The article separately substantiates that the emergence of a "digital personality" will complete the beginning of the transition from the traditional criminal law of the industrial society of the 20th century towards the criminal law of the digital world of the 21th century (criminal law 2.0). First of all, this is due to the fact that artificial intelligence and "digital personality" will fundamentally change the scope of criminal law protection.

Keywords

criminal law, criminal policy, informatization, information technology, information security, computer crimes.

For citation: Russkevich E.A. (2021) Palingenezis of criminal law in the conditions of digital reality. *Legal Issues in the Digital Age,* no 1, pp. 145–159.

DOI: 10.17323/2713-2749.2021.1.145.159

Introduction

Modern criminal law is the result of a longterm development of legal doctrine, legislation and law enforcement. In response to evolutionary changes in social relations, fundamental transformations in the economy, politics and culture, criminal law developed new categories and constructions, leaving behind what had lost its former significance over time. In essence, the development of criminal law has always followed the changing needs of its main object of protection — a human being.

People tend to treat the future as an extension of the present. This type of thinking is based on the idea that the order we have now will continue in the future, albeit in a slightly modified form. A similar logic, of course, is observed in the idea of the development of criminal law.

However, our present, that is experiencing the colossal influence of technological changes, lets us suggest that the future will no longer be its simple continuation. It will be something completely different. At the end of the second decade of the 21th century it is clear like never before that technologies of reverse engineering of the human brain will lead to the creation of Artificial Intelligence and to the emergence of "intelligent machines", as well as to the possible continuation of human life in digital form. These changes will become a point of no return, when our bodies cease to be the center of our identity [Leonhard G., 2018: 69].

The methodological basis of the research is a set of philosophical, general and particular scholar methods. The philosophical and worldview basis of the study is represented by such ideas as the rule of law, the division of law into private and public, etc. The philosophical basis of the study was also formed by the dialectical method of cognition, the use of which made it possible to identify and describe the objective dependence of the transformation of the criminal law mechanism on the impact of digitalization of the sphere of law as a whole.

Concerning the general exploration methods, such as analysis, synthesis, deduction, induction, classification, structural-functional one, etc. were used. Particular importance in the methodology of the study was given to the system method, as well as dialectical materialism.

I. "Crime 2.0" as a consequence of digitalization

"Crime 2.0" is an adaptation of the definition of "Web 2.0" to the problem of crime. Now this term is used by some Western experts to describe

crimes committed with the use of information and communication technologies that have become widespread as a result of the increasing use of the Internet, the rapid development of network and "cloud" technologies, etc. Recently, people have increasingly begun to interact for resolving social and financial issues directly in cyberspace, which has become a place for new crimes against them [Decker C., 2008: 987]. Recently, people have increasingly begun to interact to resolve social and financial issues directly in cyberspace, which has become a place for new crimes against them. Indeed, information technology has become an integral part of our daily life. It is hard t to overestimate the importance of high-tech means of communication in solving global challenges and threats to the modern world. So, stopping SARS has become possible in many ways because of the Internet. A few days after the outbreak of the deadly epidemic, the World Health Organization (WHO) launched a secured site where videoconferences were held on the problem, X-ray images of the lungs were exchanged, on the basis of which a diagnostic protocol was developed along with recommendations for quarantining infected patients. Despite the fact that atypical pneumonia, in terms of the duration of the incubation period, ease of spread and mortality, significantly exceeded the well-known epidemic of the Spanish flu, which carried away in 1918–1920, about 50 million lives [Taubenberger J., 2006], only 8422 persons were affected by it.[1]

At the same time, the rapidly developing architecture of the virtual space not only qualitatively improves our life, but also simultaneously generates new risks and threats. A negative consequence of global digitalization was the emergence of not only a new type of crime (computer crimes), but also a significant change in the nature of crime in general, which, due to the use of information and communication technologies, has acquired previously unusual features.

The performed research allows us to speak about the following six essential features of crimes committed using information and communication technologies:

extraterritoriality — the transnational nature of computer crime is its the most obvious and discussed feature. The global availability of information and communication services means that crime in the information space naturally has an extraterritorial dimension;

virtuality — the information and communication environment is the cornerstone of this crime. By ensuring anonymity and physical distance

[1] World Health Organization. SARS: How a global epidemic was stopped. 2006. Available at: https://apps.who.int/iris/handle/10665/207501 (accessed: 07.11.2020)

from the immediate victim, the virtual space is a significant advantage and, at the same time, a powerful determinant of the commission of a crime. In contrast to the real world, virtuality removes many psychological barriers on the way to the implementation of criminal activity, first of all, those related the maintenance of a feeling (and not always false) of the criminal's personal safety;

hyper-targeting — crimes committed with the use of modern information and communication technologies, perhaps like no others, are characterized by a focus on many victims at once and the ability to cause the chains of multi-level socially dangerous consequences. In case of large viral attacks on the financial sector or on the bank accounts of corporations and citizens, the number of victims can be measured in hundreds or even thousands. For example, a computer attack using the WannaCry ransomware virus began on May 12, 2017 and in a fairly short period of time hit over 500,000 computers in 150 countries. The leaders in the number of infected systems were Russia, Ukraine and India. In this regard, we should refer to the well-known theorem of Stanislav Lem, according to which the destructive power of small groups steadily increases with technological progress. Back in the early 1960s, Lem predicted that in the 21st century, a new industrial revolution will create conditions where not only criminal groups, but also individual criminals will be able to threaten the normal functioning and life of the population of megacities and even states [Lem S., 2012];

multiplicativity — this feature is largely based on such a property of computer crime as the ability to reproduce itself, i.e. multiplicativity. This symptom is most clearly manifested in the distribution of malicious computer programs. A virus attack on a specific organization due to the peculiarities of the architecture of the global information network Internet can result in colossal consequences not only for a single country, but even for a whole group of states. A computer virus, spreading through open communication channels without human participation, will infect all targets available to it, including social security facilities (hospitals, schools, etc.) and government. The other side of this multiplicative property is that the emergence of some form of virtual criminal activity, as a rule, causes new encroachments on information security relations. For example, the emergence of a new computer virus with an atypical way of spreading generates a surge of targeted attacks on protected information resources of both individual citizens and the state;

super-variability — the emergence of a new IT-technology on the mass market of goods or services almost immediately turns into another "re-

set" of crime. Attackers assess innovations as a field of next opportunities for attacking citizens or organizations. Taking into account that technologies are improving rapidly and continuously, it determines that kind of dynamic and permanent process of digital renewal of crime, when some relatively established forms of virtual criminal activity go into oblivion and are replaced by others;

6) systemic latency (hyper-latency) — computer crime is practically not amenable to accurate quantitative measurement. The explanation for this is complex: contradictions in the current regulatory framework, imperfection of law enforcement and statistical accounting mechanisms, massive non-reporting of harm by the victims themselves, as well as the countless and constantly changing nature of "digital crime". In Russia, according to experts, 85–97% of computer crimes are not detected [Agapov P. et al., 2014: 35]. We assume that the real level of latent computer crime in Russia, according to the most conservative estimates, exceeds these figures by several times.

It can be argued that crime that exists in the online space or uses the achievements and capabilities of information technology, manifests itself as a new, poorly studied negative cyber-social phenomenon, which requires a special approach and tools to counteract. Analysis of its characteristics, determination and the development of directions for combating crime 2.0 seems to be the most important task of modern society to ensure national and international security.

II. Digitalization and disruption of traditional criminal law of the industrial society of the 20th century

The traditional mechanism of criminal law protection quite often "does not work" in relation to the changed crime due to the digital transformation that it has undergone.

The most intractable, a kind of systemic challenge for the mechanism of criminal-legal protection of the information society is the previously designated globalism of crimes committed with the use of information technologies. A society in which billions of people are connected by mobile devices that open up unprecedented opportunities in the search, processing and dissemination of information requires a completely different approach both to the legal regulation of these processes and to the protection of the most significant benefits and interests. The extraterritorial nature of Internet communications forces us to admit that no regional and even more so intrastate measures will be sufficient.

We believe that a digital, hyper-connected and hyper-connected world will require a unified international criminal law built on common standards for countering cybercrime. At the same time, the recognition of the jurisdiction of such an "International Criminal Code on Cybercrimes", which establishes a minimum list of encroachments on the security of data and information infrastructure, should be a prerequisite for the participation of every state in all significant international organizations and institutions.

Significant difficulties arise in assessing the encroachments on relations that are emerging in connection with the implementation of human rights in the virtual space. So, for example, is legitimate the question of the possibility of applying the liability for libel to cases of dissemination of deliberately defamatory information about the so-called "digital personality", that is, about the hypertext components of the network image of an individual, formed by him in the online environment for the purpose of self-presentation. Clear, it is possible to speak about the honor and dignity of a "digital personality" only conditionally, implying them only to the real bearer of such qualities — the human person who owns the corresponding "nickname". By spreading deliberately false and defamatory information about the "digital personality", the attacker in one way or another directs these actions against a specific user of this or that Internet resource, that is, commits libel. However, the problem takes on a completely different dimension when the "digital personality" has an artificial origin and belongs to several users at once (for example, it was created and used in a social network for commercial purposes).

In accordance with the criminal law, illegal access to the personal page of another person on a social network can be classified as a crime, but it is very difficult to give a legal assessment of the creation and use of such a page on behalf of another person without his consent. At the same time, such actions can cause significant harm to the rights and legitimate interests of the individual, affect the decision-making on his employment, promotion, etc. Equally, the provisions of modern criminal legislation, as a rule, do not give a clear answer to the question of the qualifications of using technologies for reconstructing another person's face in real time (face swapping technologies). At the same time, such software allows, simply speaking, to "kidnap" the face of another person, to use it for creating certain materials (conditionally compromising or even pornographic).

Another problem is countering encroachments on fundamentally new objects — the so-called "virtual property". One of the most rapidly grow-

ing sectors of the modern economy is the market of multiplayer online games (World of Tanks, Worlds of Warcraft, etc.) and multimedia services (providing films, music, e-books, etc.). At the same time, the virtual space is rapidly commercializing and absorbing more and more cash flows. For real money, users of information services purchase game money, as well as other objects of informational nature that do not have physical (materialized) expression.

Already today there are a lot of special services on the Internet (trading platforms) for the sale of virtual objects used by players in multiplayer online games. It should be noted in Russia the legal nature of this kind of objects has not yet been clearly defined in legal doctrine. Lawyers argue about whether objects such as e-books, iTunes libraries, a social network account or a multiplayer game can be inherited, and whether it is possible to impose an encumbrance on such digital property or use it in enforcement proceedings.

In this regard, the question of the possibile recognizing virtual objects as the subject of theft under criminal law is becoming more and more relevant. "Virtual property" is basically just a computer code. At the same time, unlike other computer data expressing ideas, thoughts, etc., such a code is aimed primarily at imitating objects of the real (physical) world (buildings, vehicles, household items, etc.).

Although such objects exist only on a computer screen, they can be purchased and sold and have a pronounced consumer value. Maintaining the "neutrality" of criminal law regarding the assessment of encroachments on virtual objects is hardly an acceptable approach. The acquisition of real and virtual money, the accumulation of materialized and Internet property have one thing in common — a person's real time spent on this, his labor and, in many cases, real financial resources. In this regard, we can argue that such objects should not and cannot be excluded from legal protection by criminal law only because they have a slightly different nature, are expressed in a different form and look, simply speaking, unfamiliar. Of course, in solving this issue, the doctrine of criminal law largely depends on the development of civil legislation, which, as it seems, should single out such objects as a special category of objects of civil rights, as it's already done, for example, in relation to uncertified securities.

The development of information technologies will lead to significant transformation of transport crime. In these conditions, the doctrine of criminal law receives the need to develop a fundamentally new approach to the legal assessment of accidents involving such vehicles. At the moment, only one thing is clear: the traditional provision on the responsibility of the

driver in such a situation will not work, since he simply does not exist in such a situation.

The mechanism of legal regulation is driven by the state, namely by the activities of its competent authorities. At the same time it should be stated that this element of the mechanism of legal protection is experiencing significant difficulties in countering computer crime. Along with the lack of experts, technical lagging behind and outdated tactics of counteraction, one should also emphasize the unwillingness of police and judicial bodies to see a new digital dimension in the "old" norms of criminal law. In this aspect, one of the main tasks is to overcome the "traditional", i.e. "non-digital" understanding of criminal law by law enforcement officers. This is a rather complex and multifaceted problem that concerns both the initial training of future officers in educational institutions and the advanced training of police personnel in office. At the same time, we can note that the leading role in this regard belongs the doctrine of criminal law, which must first describe, classify and explain the crime of the information society, and thereby ensure the appropriate content of such educational programs.

Problems of procedural implementation of criminal law in the context of crime digitalization are also numerous and complex. At the same time, they are not in themselves the subject of this study. It should only be noted that the doctrine of criminal procedure faces a fundamental research task, without a successful solution of which all achievements of the doctrine of criminal law will be practically useless. As before, these related branches of legal knowledge should develop in concert, keeping up with and reinforcing each other in solving urgent problems of combating crime.

The above described systemic changes in social relations (and not only them) have a disruptive effect on the mechanism of criminal law protection, causing a state of disruption of criminal law — the inability to perform its basic functions due to permanent and dynamic external environmental impact. In the most simplified form, this is expressed in the idea of the complete failure of the criminal law mechanism in the face of the urgent threats of the 21st century and the justification of the need for a completely new model of combating crime.

We can highlight the following fundamental provisions that must be taken into account in the course of future changes in the criminal law:

the emergence of a new cyber method of committing a crime does not mean that it is more dangerous than the traditional one, but in many respects indicates the problem of social control lagging behind the development of society and changes in crime;

the adaptation of the criminal law to the conditions of the information society should not be associated with the construction of "digital twins" of traditional criminal law prohibitions. Such modernization of the criminal legislation will inevitably lead to excessive duplication of its provisions, leading to increasing number of rules competing with each other. In this part, a significant direction in adapting the criminal law mechanism to countering crimes committed with the use of information technology is overcoming the traditional — not digital — perception of criminal law;

amendments to the criminal law norms are only justified in cases where the adaptive capacity of criminal legislation in relation to the new digital crime is exhausted, and the interpretation of these norm goes beyond the meaning of the existing law, filling the systemic semantic gap, which already means the analogy of law;

the recognition of the use of information technologies as a qualifying sign of a crime must comply with the criteria for the differentiation of criminal liability justified in legal doctrine. At the same time, the obligatory grounds for making such a decision are: a) the need to recognize the use of e-technologies as a qualifying sign of a crime is established by the norms of international law and b) the use of information technologies has become widespread in the commission of a crime and has significantly influenced the state of the rights and interests of citizens protected by law.

III. Criminal law of the digital world in the 21th century

The transition to criminal law of a new generation will be associated with a change in our ideas about the key sign of a crime — a socially dangerous act. With the advent of the digital personality, this act will lose its human-centered physical interpretation. It will be possible to speak of an "act" in relation to any manipulation of computer information performed by a "digital personality". This "activity", as a result of which both members of the physical and cyber world may suffer, will become a new digital form of socially dangerous behavior of a criminal.

The development of the whole brain emulation technology will mean the possibility of a completely new form of life, when the very concept of a person is no longer associated with his biological envelope. It is clear that this life in the cloud will require the same criminal legal protection as in the real physical world, since here we will be dealing not just with computer code, but with a person.

As a result, we will have to revise the concept of a victim of a crime and extend the effect of traditional criminal prohibitions (on murder, kidnapping, human trafficking, libel, etc.) to all attacks against the "digital personality". The very moment of the onset of human death will lose its exclusively biological definition and will receive additional content in what we now call the ordinary destruction of computer information. A related problem is the protection of subjects who will possess a human-like consciousness of non-biological origin. Addressing this issue, one of the most famous professional futurists of our time, Google CTO Ray Kurzweil writes: "... today few people worry about the suffering we inflict on computer programs (but we often complain about the pain that computer programs bring us), but if in the future computer software gets the intellectual, emotional and moral qualities of a person, there will be a problem exactly in that regard ...The machine will become indistinguishable from a living person, whom we consider a conscious being, and, therefore, will share all those spiritual values that we associate with consciousness. This is not a humiliation of human dignity, but rather an elevation of our appreciation of (some) machines of the future. It may be necessary to choose a different terminology for these creatures, since they will be completely different machines "[Kurzweil R., 2019: 244, 256].

Already at this stage of technical development, we can talk about the inclusion of intelligent robots in legal relations. One such example is the humanoid robot Sophia, which was activated on April 19, 2015 by Hanson Robotics from Hong Kong. To create a humanoid robot, the technologies of pattern recognition and self-learning were used. During its short "life" the robot Sophia gave many interviews, was on the cover of a fashion magazine and visited many talk shows. In 2017, the robot was granted Saudi Arabian citizenship[2].

The gradual inclusion of the AI in all spheres of human life has led to the emergence of such a concept as "e-person". For the first time, a proposal for the use of this concept was recorded in subparagraph "f" of paragraph 59 of the Resolution of the European Parliament, together with the recommendations of the Commission on Civil Law Regulation in the Field of Robotics of the European Parliament of February 16, 2017 "Civil Law Regulations on Robotics"[3].

[2] Everything you need to know about Sophia, the world's first robot citizen. Available at: https://www.forbes.com/sites/zarastone/2017/11/07/everything-you-need-to-know-about-sophia-the-worlds-first-robot-citizen/?sh=2839a00e46fa (accessed: 14.01.2021)

[3] European Parliament Resolution of 16 February, 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (accessed: 14.01.2021)

Of course, the question of the model of criminal law protection of such "smart machines" entirely depends on the position of all mankind (as we believe, expressed by universal international organizations) regarding their nature and status. It is rather difficult to predict whether such entities will be recognized as equal to humans, that is, a new non-biological form of intelligent life, or whether their position in general will be comparable, for example, with animals, the criminal legal protection of which we implement in the context of protecting public morality.

A mixed scenario is very likely possible, when, depending on the level of reproduction of the intellectual and emotional qualities of a person, such cyber-physical systems will be differentiated in the legal field — as equal to a person, that is, full-fledged participants of social relations, new subjects of law, and as automated systems with limited functions (abilities) of artificial intelligence, that is, as high-tech devices, i.e. things.

A key indicator of the transition to "Criminal Law 2.0" will also be a change in the traditional understanding of the subject and the subjective side of *corpus delicti*. With external autonomy, such machines are and will remain nothing more than tools in the hands of a human. Consequently, either the owner or the developer should be held liable for harm caused by their use. Here the traditional model of the personal responsibility of an individ is triggered, the behavior of which (active or passive) in interaction with a complex technological system was the direct cause of the negative consequences. At the same time, the "digital personality" and artificial intelligence (in any form of their existence) will be independent subjects of law. This means that they should also be recognized as subjects of criminal responsibility. Thus, the theory of criminal law about the subject of a crime will move to a fundamentally new stage of development, when not only an individual and (or) legal entity, but also a digital clone of an individual, as well as AI will be recognized as the subject of crime.

Expanding the conception of the subject of crime will give rise to the problem of revising legal categories such as guilt, motive and purpose of committing a crime. The psychological theory of guilt will remain acceptable only to the physical representatives of Homo Sapiens. For AI and individuals who would continue their life in digital form, it can only be applied using a kind of legal fiction, when we agree that such subjects also have a psyche that allows them to "be aware, foresee and desire." However, as already shown above, this question will first of all need to be raised and resolved in relation to persons who have continued their lives in the digital world.

Conclusion

It is impossible to predict exactly what the future will be like. At the same time, one is clear — technologies will be much deeper and more firmly woven into our daily life. In a hyperconnected world, criminal risks will multiply. For numerous devices and applications that make life much easier, mankind will have to pay with the emergence of "digital crime", which will actively exploit the achievements of the fourth industrial revolution.

The progress in the development of the "Internet of Things" is fascinating. The advent of autonomous vehicles and the concept of a possible future — programmed accident-free and conflict-free road traffic — creates an optimistic view of global security. But at the same time, the potential catastrophic consequences that can occur if someone illegally gains access to such a system and changes its settings for at least a few minutes are quite clearly visible.

The Internet and digital technologies, the "digitalization" of crime are already having an impact on the Russian criminal law. However, we can say for sure — this is just the beginning. The next years will bring much more serious difficulties in the implementation of criminal law protection.

As a global and interconnected world takes shape, individual approaches to countering crime will need to be analyzed and revised. At the same time, it is extremely important that the "digitization" of the Russian criminal law does not lead to the destruction of the essential features of this branch of law. A significant part of adapting the criminal law mechanism to countering cyber crimes, in our opinion, is overcoming the "traditional", "non-digital" perception of criminal law. This is a rather multifaceted problem, which concerns not only the training of personnel in educational institutions and the advanced training of existing law enforcement officers.

The essential features of crimes committed with the use of information technologies are: a) extraterritoriality; b) virtuality; c) hyper targeting; d) multiplicativity; e) supervariability; f) systemic latency (hyperlatency).

Taking into account the rapid digitalization of public relations, we can conclude about the disruptive impact of information and communication technologies on the mechanism of criminal law protection (disruption of criminal law).

The following fundamental provisions can be distinguished, which should be relied upon to overcome this crisis and make a decision on the modernization of the criminal law:

the emergence of a new (informational) method of committing a crime does not a priori indicate that it is more dangerous than the traditional one, but largely indicates the problem of social control lagging behind the development of society and changing crime;

the adaptation of the criminal legal norms to the conditions of the information society should not be associated with the construction of "digital twins" of traditional legal prohibitions. Such modernization of criminal legislation will inevitably lead to excessive duplication of its provisions, expressed in presence of a significant number of norms competing with each other exclusively at the junction of the problem of distinguishing between the virtual and the real in law. In this part, a significant part in adapting the criminal law mechanism to countering cyber crimes is overcoming the traditional — not digital — perception of criminal law;

the adoption of amendments to the criminal law is justified only when the adaptive capacity of criminal legislation to digital crime exhausts itself, and the interpretation of the norm goes beyond the meaning of the law, filling the systemic semantic gap, which in fact is already an analogy of law;

the recognition of the use of information technologies as a qualifying sign of a crime must comply with the criteria for the differentiation of criminal liability justified in legal doctrine. At the same time, the obligatory grounds for making such a decision are: a) the need to recognize the use of e-technologies as a qualifying sign of a crime is established by the norms of international law and b) the use of information technologies has become widespread in the commission of a crime and has significantly influenced the state of the rights and interests of citizens protected by law.

The emergence of the "digital personality" will complete the beginning of the transition from the traditional criminal law of of the 20th century industrial society to the criminal law of the digital world of the 21th century. ("Criminal Law 2.0"). This is primarily due to the fact that AI and "digital personality" will fundamentally change the scope of criminal law protection.

The complexity of digitalization of the criminal law sphere implies an increased responsibility of the academic community, which must provide an appropriate level of understanding of the emerging trends. The attempt made in this article to predict the development of criminal law, of course, does not pretend to be absolute, it is subjective, and therefore probabilistic in its nature. At the same time, there is no doubt that the joint efforts of philosophers, sociologists, high-tech specialists and lawyers will make it

possible to obtain a fairly accurate forecast of the evolution of criminal law in a digital reality.

References

Agapov P., Borisov S. et al. (2014) *Counteraction to cybercrime in the aspect of national security.* Moscow: Academy of the General Prosecutor's Office, 136 p. (in Russian)

Bostrom N. (2007) Technological revolutions and problem of prediction. In: Allhoff F., Lin P., Moor J., Weckert J. (eds.) Nanoethics: the ethical and social implications of nanotechnology. Hoboken (N.J.): Wiley-Interscience, pp. 101–118.

Brenner S. (2012) *Cybercrime and the law: challenges, issues and outcomes.* Boston: Northeastern University press, 263 p.

Decker C. (2008) Cyber-crime 2.0: An argument to update the United States criminal code to reflect the changing nature of cyber-crime. *Southern California Law Review*, no 5, pp. 972–995.

Grabosky P. (2016) *Cybercrime: keynotes in criminology and criminal justice series.* New York: Oxford university press, 168 p.

Kurzweil R. (2019) *Evolution of the mind or the endless possibilities of the human brain based on pattern recognition.* Moscow: Eksmo, 352 p. (in Russian)

Leonhard G. (2018) *Technologies against man*. Moscow: AST, 320 p. (in Russian)

Lem S. (1968) *The sum of technologies.* Moscow: Mir, 1968. 608 p. (in Russian)

Lv A., Luo T. (2018) Authoritarian practices in the digital age. asymmetrical power between internet giants and users in China. *International journal of communication,* no 12, pp. 3877–3895.

Meissner M., Wübekke J. (2016) IT-backed authoritarianism: Information technology enhances central authority and control capacity under Xi Jinping. China's Core Executive, Leadership Styles, Structures and processes under Xi Jinping. *Mercator Institute for China studies,* no 1, pp. 52–57.

Ohlberg M., Ahmed S., Lang B. (2017) Central planning, local experiments: the complex implementation of China's Social Credit System. *Merics China Monitor,* no 43, pp. 1–15.

Qianyun Wang (2016) *A study of cybercrime comparative criminal law: China, US, England, Singapore and the Council of Europe.* Rotterdam: Erasmus University Press, 381 p.

Rhaman M. et al. (2009) Cyberspace claiming new dynamism in the jurisprudential philosophy: a substantive analysis of conceptual and institutional innovation. *International Journal of Law and Management,* no 5, pp. 274–290.

Schwab K. (2018) *The fourth industrial revolution.* Moscow: Eksmo, 288 p. (in Russian)

Sithigh D., Siems M. (2019) The Chinese social credit system: a model for other countries? *EUI Working papers,* no 1, pp. 1–30.

Taubenberger J., Morens D. (2006) 1918 Influenza: The mother of all pandemics. *Rev Biomed*, no 1, pp. 69–79.

Williamson D. (2017) China's online consumerism: managing business, moral panic and regulation. Available at: https://lancaster.academia.edu/DermotWilliamson (accessed: 17.02.2021)

Zhang T. et al. (2015) Using big data theory to establish a new standard for Social Credit System. *Information China*, no 10, pp. 94–95.