PRZEGLĄD WSCHODNIOEUROPEJSKI IX/2 2018: 55–67

Pavel Zhesterov
Russian State Social University

FROM VISIBLE PASTS TO AN INVISIBLE PRESENCE: NEW CRIMINOLOGICAL REALITY AFTER PLANETARY CYBER ATTACK 12/05/17 WANNACRY

Keywords: criminal repression, crime prevention, augmented reality, organised crime, cyber crime

Abstract: The fourth industrial revolution is transforming crime and fight against it, causing fundamental consequences for research in the field of criminal law. Under the conditions of the second decade of the 21st century, the terms 'Internet', 'information and telecommunications network', 'electronic network', 'communications facility', 'mobile communications' are no longer an IT specialist dictionary, in the meantime they affect the doctrine of criminal repression and integrate into a scientific turnover of specialists in the field of criminal law and criminology. Transformation of crime has caused serious gaps, both in the theory of criminal law and in criminal procedural and criminal executive law inextricably bound with it. The emergence and exponential development of the Internet, electronic communications, control and tracking systems and many other technical achievements create for researchers three types of problems that need to be discussed and resolved. First, the problem of national sovereignty in criminal matters (the operation of criminal law in space) and jurisdiction, which are in contradiction in the boundless cyberspace. Secondly, the prognostic problem, which urges not only to forecast the influence of modern technologies on substantive criminal law, criminal procedure, execution of criminal punishment, but also to anticipate the general impact of technology on Russian society and the way of life of its members. Thirdly, the problem of expenses resulting from the introduction of high-tech crime prevention measures, the cost of which is constantly growing. The interdependence of these problems should form the basis of criminal law research in the era of augmented reality under the conditions of exponential growth of cyber threats directed at citizens, businesses and governments.

The true mystery of the world is the visible, not the invisible.
Oscar Wilde

1. Introduction

Among the institutional problems of modern criminology, a special position is taken by the prevention of cyber crime (Lesnikov 2014). Cyber crime in its various manifestations and the enormous scale that it has acquired in recent years in Russia and the world is a phenomenon from which citizens, society and the state itself

are not provided with reliable protection. Massive cyber attacks, which occurred on May 12 last year, as a result of which a virus-extortionist spread to computers in 150 countries, only confirm the growing scale and diversity of cyber threats (Meduza 2017). Cyber crime is a real national security threat (Kobets 2016).

To confirm the foresaid, the main argument is the perception of such danger by the population. Public – opinion polls of the All-Russian Public Opinion Research Center (VCIOM) concerning the greatest fears in cyberspace record first of all the fears of theft of money from bank cards and electronic bills, as well as personal information (surname, name, passport data, etc.) – according to 65% of respondents, respectively. About a third of Russians (31%) has already faced with illegal activities related to cellular communications and Internet services. At the same time, nowadays only 36% of Russian respondents (44% among men, 45% – among 18–24-year-olds, 39% among permanent Internet users) have the feeling of safety from illegal actions connected with cellular communication and Internet services, while 58 % of them rather feel their vulnerability (64% among women, 65% among 45–59-year-olds) (Press Release 2017). According to Europol, 85% of Internet users feel the risk of becoming a victim of cyber crime (Europol 2017).

This vision of the danger of cyber crime by the population reflects the low effectiveness of the work of law enforcement agencies (primarily due to the lack of funding for this "fighting line" and, in general, the low "digital" qualification of the majority of police officers) and the legislator's unwillingness to establish distinct limits of criminal repression in the sphere under consideration.

The actual task of the legislator and enforcer is the deeper insight into the essence of modern cyber crime, its nature in order to develop algorithms for effective counteraction. Cyber crime causes huge direct material damage to individuals, legal entities and the state, as well as indirectly affects the stability of the banking sector, damaging social and political relations, the scale of which cannot even be assessed. Let us illustrate the last statement. The highest-level leaders of our country justify the need to limit the cash turnover to control payments and expensive purchases made for cash, in order to create conditions of hardship for corrupt officials (Girko/Lesnikov 2014). At the same time, the implementation of this initiative of high priority is hampered by cyber crime and, moreover, in the most unexpected way. As experts note, 80% of Russians are against restrictions on cash settlements. Consumers are slow to refuse to use cash (Shilovskaya et al. 2016). In addition to the above, the reluctance of the Russian population to give up cash is explained not only by the power of habit, but more by fear of new technologies and the allied risks, including cyber crime (Vedomosti 2017).

Threats in the field of cyber security can no longer be ignored (Kobets 2017). In his speech at the IV International Arctic Forum "The Arctic: Territory of Dialogue" on March 30, 2017, the President of the Russian Federation emphasized:

"Network access systems, digitalization of public and private life require reliable protection of interests of both citizens and the state as a whole" (Kremlin 2017).

Thus, cyber crime undermines the security of the country and its population. With the globalization of economic ties, cyber crime has assumed global, international proportions, has become a threat to international law and order in general. In other words, if it is complicated by an international element (criminal, crime scene, and victim) it will acquire a transnational character. Further steps are needed to develop recommendations for creating a more reliable legislative basis for anti-cybercrime measures. In this regard, it is very important to improve legislation at the national and international levels.

2. Methodology

The author employs qualitative methods, including systemic and structural analysis with the goal of identifying the influence of modern technologies on substantive criminal law, criminal procedure, execution of criminal punishment, paying special attention to the problem of expenses resulting from cyber crime prevention. The author also employed a historical analysis of laws and norms relating to cyber crime. The researcher also uses the comparative law method to define the main trends concerning national sovereignty in criminal matters in the boundless cyberspace. Logical methodology, such as deduction and generalization, was used for the theoretical interpretation of empirical facts in an effort to work out new provisions for legislative development in the challenging area of criminal repression in cyberspace.

3. National sovereignty and crimes in cyberspace

A classical study in the field of criminal law often solves problems in a one-dimensional way: the criminal law is initially seen as a given, which is limited by the space-time framework and assumes the presence of a real or seeming threat to the economic and social interests of society. In order to establish a boundary between cans and cannots in a society, the criminal law imposes a certain absolute requirement on a person to observe a certain moral minimum of behavior in each individual society (Fedorova 2016). In other words, the criminal law acts as a means of social control. The legislator has the right to decide only to a certain extent what behavior will be considered criminal (Burlakov/Pryakhina 2014, 10). As N. P. Meleshko notes with concern, "there is always a threat that the justice and

sanctions system may become an instrument for transforming the rule of law into a mechanism of suppression for political, social and other purposes" (Meleshko 2014, 130).

The problem is particularly acute for the limits of social control over members of society when it comes to controlling the circulation of information in cyberspace (Volkova et.al. 2015). The Internet space is based both on the products of information technology and on social services, which are the field of a specific human behavior (Voiskunsky 2016). Services are built on network technologies and promote communication, entertainment (including games and listening to music), learning, work, shopping (Voiskunsky 2016). However, not all the people use Internet to communicate, work, get education and purchase goods and services. As a result of the cooperation of law enforcement agencies and network providers, many "digital" criminals are increasingly being identified: hackers, personal account attackers, organizers and participants of cyber attacks, etc. (Thomas 2002). At the same time, not all offenders are identified, since for many of them there was no criminal law norm due to the imperfection of the criminal legislation.

The latter circumstance has become particularly topical in connection with the growing danger of terrorism. As early as in the mid-1930s A. Traynin wrote that the concept of terrorism "spread out into a whole system of crimes, essentially a small international criminal code, which provides for very heterogeneous offences: against life, bodily integrity, health and property holdings, etc." (Traynin 1935). By the turn of the XX and XXI centuries, terrorism has ceased to be the only problem requiring international unification. According to G. K. Mishin, a similar evolution occurred with the notion of corruption, which spread out in the "small criminal code" (Mishin 2004). For our part, emphasizing the accuracy of the comments of the above-mentioned authors with regard to terrorism and corruption, we can state that in modern international law the genesis of the concept of "cyber crime" and its interpretation in the national criminal laws of various countries, including Russia, takes its rise. And here we should draw a parallel with the treatment of the phenomena of "terrorism" and "corruption" in connection with the protection of society from offences in the field of computer systems.

One has to agree with the foreign (English) experts that criminology must develop a digital specialism which investigates the multifaceted role performed by digital technologies as intersectional and transformative mediums in the crime and justice field (Smith/Moses/ Chan 2017).

This tendency urges governments of different countries to continue to raise issues on the conceptualization and categorization of cyber crime. Cyber crime is increasingly seen by experts as part of transnational organized crime. For example, the BRICS states at a summit in Ufa on July 8–9, 2015 discussed the use of information and communication technologies "for the purposes of transnational organized crime, the development of weapons and the implementation of terrorist

acts" (Ufa Declaration, 2015). It is noteworthy that in the final document of the Russia – ASEAN summit held in Sochi on May 19–20, 2016, cyber crime was named among the manifestations of transnational organized crime, along with human trafficking, illegal migration, maritime piracy, arms smuggling, money laundering, and international economic crime (Sochi Declaration, 2016).

The concept of foreign policy of the Russian Federation refers cyber crime to the challenges and threats of "transboundary nature" (p. 17). Further, in p. 64 of the Concept, attention is drawn to the need to intensify the joint work of Russia and the EU on combating organized crime, including its manifestation, such as cyber crime (Concept 2016).

At the EU level, the legal framework for combating cyber crime has evolved with the enactment of legislation on attacks on information systems (Directive 2013) and the use of passenger name record (PNR) data for prevention, detection, investigation and prosecution of terrorist offences and serious crime (Directive, 2016). In addition, nowadays the state – members of the EU have access to the mechanisms of combating cyber crime, developed at the international level. The Convention on Cybercrime (ETS No. 185) (Convention on cybercrime, 2001) was signed not only by the member states of the EU, but also by the other "member states of the Council of Europe, Canada, Japan, South Africa and the United States of America and entered into force on July 1, 2004. The Convention addresses a variety of cyber crime: against the confidentiality, integrity and availability of computer data and systems, forgery and fraud with the use of computers, crimes associated with data content, in particular offenses related to child pornography and infringement of copyright and allied rights (Chapter II, Section 1, Part 1–4)" (ECHR Resolution 2012).

These documents and agreements make compelling arguments about productivity and the need to further develop international cooperation in the sphere of counteraction to cyber crime.

The international scale of cyber crime is manifested in particular in the fact that emails with illegal content often pass through many countries during the transfer from the sender to the recipient, or illegal content can be stored outside the country, or illegally accessed from an IP address, physically located in another country. There are other examples of cybercrime offences of international dimension. At the same time, as the experts note, criminal prosecutions at the global level are usually limited to those crimes that are criminalized in all countries involved in the investigation (Understanding cybercrime 2012). In this regard, the investigation of crimes related to the spread of child pornography via the Internet, which is criminalized in most countries of the world, is successful.

However, the complexity of the investigation may arise due to the uneven criminalization in the world of liability of legal persons for crimes committed in cyberspace. The practice is that more and more cybercrime offences are

committed not only by individuals, but also by legal persons (Lavorgna/Sergi 2016). It is appropriate to recall that the Budapest Convention ETS No. 185 placed on the agenda the issue of the collective responsibility of legal persons (Convention on Cybercrime 2001).

4. Criminalization of cybercrime offences: the consequences of criminalization

We are witnessing a large-scale informatization in the world (Arkhipova 2011). In this regard, the need to protect human rights and freedoms in cyberspace is obvious and indisputable. However, the existing national standards of mechanisms for their enforcement and exercise differ significantly and are conditioned by various subjective factors reflecting the degree of development of the economy and law in the state, crime figure, ethnic composition of the population, geographical location, culture, traditions, customs, etc.

One of the main requirements for the national system of crime prevention and criminal repression should be a comprehensive study of criminalization and decriminalization as its criminal-legal component. Meanwhile, G. V. Nazarenko regretfully states that "criminal policy of Russia at the present stage has the reflective nature, because forms, means and methods of combating crime are determined spontaneously" (Nazarenko 2016, 94).

We would add for ourselves that modern crime-fighting tools are not sufficiently completed with a "digital" component. However, with allowance for the ongoing fourth industrial revolution, criminologists should pay more attention to the specifics of the era of augmented reality we are experiencing now, when even crime is complicated by a digital element. Foreign criminologists note the potential impact of Big Data on the production of security in society (Chan/Moses 2017, 299). In this regard, the topical subjects are: use of prediction of future ways of committing crimes; assessment and forecast of the development of the crime scene, complicated by a virtual or augmented reality; study of the identity of a criminal who is fluent in high-tech instruments for the commission of a crime. The enumerated range of ideas is only a small part of the criminological information that should be the basis of the criminological forecast aimed at finding effective measures to counter new unlawful acts committed (or those that are more likely to be committed in the future) with the use innovative technologies.

Having referred the penal prohibition to the social problem, it becomes necessary to assess the consequences of its establishment or, on the contrary, abolition. Any changes in the criminal legislation should be preceded by discussions why and how the national criminal law should change. And at present these discussions should

come to a new level under the global impact of technologies, whose role in law and society is constantly growing. It is impossible to deny so far the ongoing process of mutual regulation of technology and society. Prudent solution to the problems arising in this connection requires an interdisciplinary study that explains this interaction and mutual influence. The theory of criminal law should keep pace with the problems of the second decade of the XXI century, in which cyberspace makes inroads in all the spheres of society, such sacred ones as personal life and delicate as the financial sphere. Consequently, the dogmatic understanding of the very system of criminal law is no longer sufficient. In order to cope with the global problems of combating crime, complicated by a "digital" element, a researcher must be well - versed in the theory of criminal law regulation, skillfully adapting the newest tools for combating crime and its prevention to the traditional paradigms of the sciences of criminal law and criminology.

5. "The cost" of high-tech crime prevention measures in Russia

We diagnosed an issue that urges to forecast the influence of modern technologies on criminal law, criminal procedure and enforcement of criminal law. We would like to cover this influence step by step.

First, the analysis of the literature shows that many specialists place greater focus on the significant difficulties associated with assessing the prospects for the criminalization of certain acts. According Gavrilov, "when implementing a criminal policy, there is often no specific information about the social consequences of the forthcoming changes in criminal repression" (Gavrilov 2008, 6).

Zhalinsky noted with reason that

> in criminal legal science, and not only in Russia, there's no solution for its main question concerning a real role of the criminal law, and in particular, the actual impact of criminal law on people's behavior. In the scientific literature, it is assumed by default that prohibitions and punishments establish framework for people's behavior defined by the criminal law. But no one has ever proved a connection, and certainly there was not shown the tightness of the connection between the dynamics of crime and the changes in criminal legislation. At the same time, the social costs of repression are well known, but there is no information about the possibility of their more reasonable use (Zhalinsky 2005).

The point at issue is about, first of all, the direct costs of ensuring criminal proceedings, the execution of the punishment imposed by the court.

Indeed, explanatory notes to the draft laws on amendments to the Criminal Code of the Russian Federation are not aimed at providing forecasts, other data on

criminological, social, economic consequences and the "cost" of criminal repression. As a rule, the financial and economic justification for the draft law contains a dry, formalized phrase that its adoption "will not require additional expenditures from the federal budget". While experts note a number of "costs that increase with a more extensive application of criminal prosecution" (Grigoriev/Kurdin 2012). For example, the costs of implementing the "Yarovaya's Act" – a law that obliges cellular operators and Internet providers to store information about the negotiations and turnover of messages of subscribers and users of the Internet for three years, and their content for up to six months, – even according to the most approximate estimates amount to hundreds of billions of rubles. According to the information agency RBC, the Ministry of Communications and Mass Media began to develop proposals to reduce costs (RBC 2016). There arises a rhetorical question of whether it was possible to assess the "cost" of such repression at the stage of consideration of the bill. Ultimately, Russian cellular operators will indirectly impose these costs on their subscribers, raising tariffs for their services, in the conditions of insufficient strict state control over tariff formation in our country.

We believe that one should seriously consider not only the criminological expert study that precedes any change in the criminal law, but also financial, economic, and even possibly technical one. The conclusions of independent experts would give an answer to the question of whether the introduced or amended criminal-legal norm will be "free" for the budget, and its implementation will not require the development of global electronic, communication or technical systems.

Secondly, Kolokolov (2012, 120) notes that the technological inferiority of the Russian criminal procedure is more than obvious, "for it still tries to drag in the technologies of the industrial age in the postindustrial society". This is largely due to the historical reasons for the formation of Russian criminal procedure law and professional environment. The Romano-Germanic legal family, to which Russian law belongs, is not so mobile to innovations as the law of the Anglo-Saxon family. So, if in 2016 the Supreme Court of England allowed judges to use predictive coding (the technology of "computer analytics", that is, a computer retrieval of documents that showed its effectiveness in a number of major civil cases in the US and England, according to which the number of relevant documents reached the amount of about one million copies) (Technology 2017). In the US, you can get legal advice in many areas of law with the help of IBM Watson, the question-answer system of artificial intelligence, within a few seconds. The accuracy of the consultation is 90% compared to 70% accuracy of the consultation held by a legal practitioner (PSJ 2017).

As for Russia, one can say that, unfortunately, its modern judicial system is a picture preserving the features of the last century. In Russia, until now, the records in primary legal documents are mostly hand-made. The main technological achievements of the national criminal procedure system are the possibilities to store

physical evidence on electronic media and conduct interrogation of a witness by using videoconferencing systems.

In the era of spreading augmented reality to all spheres of society, the process of technological inferiority of Russian criminal justice will only gain strength, first of all, due to the high cost of universally introduced technologies and insufficient budgetary financing of such a work. To illustrate this, Kobets & Krasnov write that "unexpected deterioration in macroeconomic indicators may be accompanied by a decrease in the financing of law enforcement and the fight against crime" (Kobets/Krasnova 2009, 41). For example, within the framework of the national project "Safe City" in Russia, there was created a comprehensive information system that ensures the forecasting, monitoring and prevention of possible threats. With the help of this system, it is possible to monitor the processes of taking action to recover from the consequences of emergencies and delinquencies. However, the insufficient funding envisaged within the framework of regional state programs (sub-programs) for the prevention of offenses is called "one of the main obstacles to the further development" of the hardware and software complex "Safe City" (Eliseev/Agafonov 2016, 139–142).

Thirdly, the Russian penal enforcement system also uses technical achievements in an insufficient way, although the legal framework for putting the penal repression on a high-tech level has been established in our country long ago. We have in mind such a form of criminal penalty as restriction of liberty (Article 53 of the Criminal Code of the Russian Federation). Restriction of liberty is a form of penalty that can be imposed as the primary for crimes of small and medium gravity, and as an additional to forced labor or imprisonment. Its general terms are from two months to four years when applied as the primary, or from six months to two years with its assignment as additional. In the case of minors, restriction of liberty is imposed only as the primary punishment for a period from two months to two years (Sitdikova/Shilovskaya 2015). The essence of this type of punishment is to impose a number of restrictions to a convicted person. Two of them are mandatory: the obligation to appear in the probation department from one to four times a month for registration and prohibition on changing the place of residence or stay, as well as on leaving the territory of the relevant municipal entity without the consent of the aforesaid department. Other restrictions are set in the verdict at the discretion of the court that can revoke or supplement them in the process of serving the sentence at the instance of the chief of the probation department. These include: not to leave the place of permanent residence at a certain time of day, not to visit certain places, not to visit places of public and other events and not to participate in these events, etc.

Supervision of the convict who is serving a restriction of liberty is carried out by the probation departments. At the same time, since 2013, it is possible to use special technical means to monitor the location of convicts (including electronic

bracelets). In the criminological literature it is emphasized that "when applying this type of punishment, the use of modern technologies is considered to be progressive" (Dikaeva/Gilinsky 2014). First of all, this refers to the means and systems of electronic control over the convicted person during the execution of the sentence. However, the positive potential of using the innovative technologies in the practice of executing this type of punishment was lost as a result of a headline-making corruption scandal involving a kickback received by Alexander Reimer, the former head of the Federal Penitentiary Service of the Russian Federation.

It will be recalled that a kickback is an illegal covert payment to an official, made in return for the service rendered by him. Most often, this is the percent from the total amount of the state contract, paid in cash (Krasnova 2014, 269). The materials published in the "Kommersant" newspaper contained information that Alexander Reimer received 140 million rubles (€1,9 mln) in cash, in his office, as payment for his services. As the results of the investigation show, this huge kickback amounted to approximately 10% of the total amount of budget funds received by the companies of the organized group members who managed to conclude contracts for manufacturing and supplying electronic means of monitoring the persons under supervision (so-called "bracelets") with the direct support of Alexander Reimer. The first contract was concluded in 2010. The cost of one bracelet varied in it from 108.5 thousand to 128 thousand rubles. In 2011, the contract price rose to 2.6 billion rubles. At the same time, as it turned out during the investigation, some of the bracelets produced did not work. The cost of all the output was overestimated several times. At the same time, part of the money being received by the companies – contractors (who had to perform state contracts) was transferred to the criminal groups of the company that were affiliated with another participant (Nikolay Martynov) under sham contracts. There it was cashed and transported to Moscow. The investigators believe that only out of overpricing of electronic bracelets the accused "made" more than 1.2 billion rubles. The total damage from their actions exceeded 2.7 billion rubles. In the end, this story slowed down the development and implementation of high-tech control means and monitoring of persons convicted to the restriction of liberty. This case not only had an indelible, degenerative impact on the entire penal system and its officers. The most sad is the fact that as a result of criminal supplies of faulty equipment, the principle of economizing criminal repression in the sphere of execution of criminal penalties was put on an "idle" course for almost three years (in the period from 2010 to 2012, while the criminal scheme worked out by the head of the Federal Penitentiary Service of Russia existed) (Kommersant 2016).

The criminal justice system still needs time to realize the preventive nature of the type of criminal penalty in question. It should be noted that at the moment, it is the lack of appropriate equipment and systems of control over those sentenced to this measure of punishment that impedes to economize repressions in the penal system.

6. Conclusion

Summarizing the above, we note that the global nature of the problem of cyber crime gave an impetus to the creation of an international system for countering cyber crime, which includes multilateral regional legal instruments and the activities of international organizations and regional associations in this field. At the same time, it should be noted that there are no mandatory obligations compelling the EU member states, as well as Russia and its BRICS and ASEAN partners to bring their criminal legislation in line with the above-mentioned directives and conventions.

These circumstances allow us to conclude that the impact of technology on Russian society and the way of life of its members will only increase. And this process has just started to gain strength. When solving the global problem of cyber crime, international organizations, regional associations and the national legislator rely on the criminal law as a means of regulating legal behavior in cyberspace. Noting the impetuosity with which digital realities change socio-economic relations, we regretfully state that criminal repression does not have time to react to these changes. In attempting to correct criminal repression, it is important to pay attention to the social conditioning of criminal law prohibitions and to observe the necessary conditions for criminalizing dangerous behavior in cyberspace. Future researches might seek to explore the impact of modern technology on substantive criminal law, criminal procedure, and execution of criminal penalties at the national level.

References

Arkhipov, I. K. (2011), About the "transfer of information" in the literal and metonymic sense. In: Przegląd Wschodnioeuropejski. II, 453–464.

Baeva, L. (2017), Values of mediasphere and E-Culture. In: Przegląd Wschodnioeuropejski. VIII/1, 173–184.

Burlakov, V. N./Pryakhina, N. I. (2004), Restructuring of criminal law: results and prospects. In: Criminology Journal of Baikal National University of Economics and Law. 2, 5–15.

Chan, J./Moses, L. B. (2017), Making Sense of Big Data for Security. In: The British journal of criminology. 57 (2), 299–319: https://doi.org/10.1093/bjc/azw059.

Convention on Cybercrime (ETS No. 185) (signed in Budapest, 23.11.2001) (as amended on 28.01.2003). In: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7convbudapest/7convbudapesten.pdf [Access 14.09.2017].

Dikaeva, M. S./Gilinsky, Y. I. (2014), Application of criminal penalties not related to deprivation of liberty: present and future. In: Science Week of SPbSPU. Materials of the research and practice conference with international participation. St. Petersburg, 200–202.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Official Journal of the European Union (2016). L 119, 132. Official website of European Union legislation: http://eur- lex.europa.eu [Access 14.09.2017].

Directive 2013/40 / EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222 / JHA. Official

Journal of the European Union (2013). L 218, 8. Official website of European Union legislation: http://eur- lex.europa.eu [Access 14.09.2017].

Eliseev, A. V./Agafonov, S. I. (2016), On the law-enforcement segment of the HSC "Safe City". In: Bulletin of the Moscow University of the Ministry of Interior of Russia. 7, 139–142.

European Union serious and organized crime threat assessment: crime in the age of technology. In: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [Access 14.09.2017].

Fedorova, L. L. (2016), Discourse of mass demonstrations. In: Przegląd Wschodnioeuropejski. VII/1, 101–119.

Gavrilov, B. Ya. (2008), Contemporary criminal policy of Russia: figures and facts. Moscow.

Girko, S. I./Lesnikov, G. Y. (2014), Public security and fight against corruption in the Russian Federation. In: Social and Political Sciences. 3, 22–25.

Grigoriev, L. M./Kurdin, A. A. (2012), Economic consequences of criminal reprisal against entrepreneurs. In: Zaostrovtseva, A. P. (Ed.), Economic freedom and the state: friends or enemies. St. Petersburg.

Judgment of the European Court of Human Rights of 18.12.2012 "Case Ahmet Yildirim v. Turkey" (lawsuit No. 3111/10). In: Precedents of the European Court of Human Rights (2016). 6 (30).

Kobets, P. N. (2016), On modern information technologies used by extremist and terrorist groups and the need to counter cyber crime. In: Development of Science and Education Bulletin. 6, 4–9.

Kobets, P. N. (2017), Police forces of the Netherlands in combating child pornography distributed on the Internet: international standards and foreign experience. In: Police and investigative activities. 1, 70–80.

Kobets, P. N./Krasnova, K. A. (2009), About need for social and criminological modeling of the criminal situation in Russia. In: Dolgova, A. I. (Ed.), A New criminal situation: assessment and response. Moscow, 41–46.

Kolokolov, N. A. (2012), Directive, communicative and technological aspects of criminal proceedings. In: Bulletin of the Moscow University of the Ministry of Interior of Russia. 4, 118–120.

Kommersant: Alexander Reimer has been forked up for bracelets [Коммерсант: Александру Реймеру отстегнули за браслеты]. (In Russ.). In: http://www.kommersant.ru/doc/2923518 [Access 14.09.2017].

Krasnova, K. A. (2014), General characteristics of forms of manifestation of corruption in the European Union. In: Dolgova, A. I. (Ed.), Criminological situation and response to it. Moscow, 265–273.

Kremlin: International forum "The Arctic: Territory of Dialogue". In: http://www.kremlin.ru/events/president/news/54149 [Access 14.09.2017].

Lavorgna, A./Sergi, A. (2016), Serious, therefore Organised? A Critique of the Emerging "Cyber-Organized Crime" Rhetoric in the United Kingdom. In: International Journal of Cyber Criminology. 10 (2), 170–187.

Lesnikov, G. Y. (2014), The criminal policy of Russia: Institutional Problems. In: Scientific portal of the Ministry of Interior of Russia. 4 (28), 5–8.

Meduza: Monday of the virus-extortionist WannaCrypt hit China; Microsoft compares the incident with the theft of "Tomahawks". In: https://meduza.io/feature/2017/05/15/ponedelnik-virusa-vymogatelya [Access 14.09.2017].

Meleshko, N. P. (2004), Problems of improving the criminal legislation of Russia in the light of international experience. In: Komissarov, V. S. (Ed.), International and national criminal legislation: the problems of legal technique. Moscow, 130–142.

Mishin, G. K. (2004), On the methodology of global criminal law. In: Komissarov, V. S. (Ed.), International and national criminal legislation: the problems of legal technique. Moscow, 58–60.

Nazarenko, G. V. (2016), Contemporary criminal law policy: a new phase of liberalization. In: Central Russian Journal of Social Sciences. 11 (2), 94–98.

Press Release No. 3282. Security in the information society: Challenges of the New Century. In: https://wciom.ru/index.php?id=236&uid=116024 [Access 14.09.2017].

PSJ: On the singularity and what will happen during the 4th industrial revolution. In: http://www.psj.ru/saver_national/detail.php?ID=90070 [Access 14.09.2017].

RBC: The Ministry of Communications and Mass Media of the Russian Federation will try to reduce the costs of the "Yarovaya's Act". In: http://www.rbc.ru/technology_and_media/13/12/2016/584ec8c99a79473a81b0d963 [Access 14.09.2017].

Shilovskaya, A. L./Sitdikova, L. B./Starodumova, S. J. et al. (2016), The consumers 'rights' protection in the sphere of consultancy services: the problems of theory and judicial practice in Russian Federation. In: Journal of Internet Banking and Commerce. 21 (S 4).

Sitdikova, L. B./Shilovskaya, A. L. (2015), On the improvement of compulsory educational measures for minors. In: Criminology Journal of Baikal National University of Economics and Law. 9 (4), 682–690.

Smith, G. J. D./Moses, L. B./Chan, J. (2017), The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. In: The British journal of criminology. 57(2), 259–274: https://doi.org/10.1093/bjc/azw096.

Sochi Declaration of the ASEAN – Russian Federation Commemorative Summit to Mark the 20th Anniversary of ASEAN-Russian Federation Dialogue Partnership "Moving Towards a Strategic Partnership for Mutual Benefit" (Adopted in Sochi on May 20, 2016). Site of The Association of Southeast Asian Nations: http://russia-asean20.ru [Access 14.09.2017].

Technology: The Supreme Court of England authorized the use of computer analysis of documents. In: http://pravo.ru/story/view/126752 [Access 14.09.2017].

The Criminal Code of the Russian Federation of June 13, 1996 [Уголовный кодекс Российской Федерации]. (In Russ.). In: http://www.consultant.ru/document/cons_doc_LAW_10699 [Access 14.09.2017].

The Presidential Decree of the Russian Federation No. 640 of November 30, 2016 "About approval of the concept of foreign policy of the Russian Federation". Official Internet Portal of Legal Information: www.pravo.gov.ru [01.12.2016, No. 0001201612010045] [Access 14.09.2017].

Thomas, D. (2002), Hacker Culture. Minneapolis/London.

Traynin, A. N. (1935), Penal intervention. In: Vyshinsky, A. Y. (Ed.), the Movement for the unification of the criminal legislation of capitalist countries. Moscow.

Ufa Declaration of the VII BRICS Summit (Adopted in Ufa on 09.07.2015). Official site of the Russian Federation presidency in BRICS: http://brics2015.ru [Access 14.09.2017].

Understanding cybercrime: phenomena, challenges and legal response. In: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf [Access 14.09.2017].

Vedomosti: VCIOM: 80% of Russians are against restrictions on cash payments. In: https://wciom.ru/index.php?id=238&uid=116117 [Access 14.09.2017].

Voiskunsky, A. E. (2016). Behavior in cyberspace: psychological principles. In: Human. 1, 36–49.

Volkova, M. A./Sitdikova, L. B./Starodumova, S. J. et al. (2015), Legal problems in implementing information services in Russian civil law. In: Review of European Studies. 7 (6), 243–271.

Zhalinsky, A. E. (2005), On the current state of criminal legal science. In: Criminal law. 1, 21–24.