Journal of Siberian Federal University. Humanities & Social Sciences
2020 13(1): 116–122

DOI: 10.17516/1997-1370-0542
УДК 343.3/.7:004.8

Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects

Alexander P. Sukhodolov[a], **Artur V. Bychkov**[b]
and Anna M. Bychkova[c]*
[a]Baikal State University
Irkutsk, Russian Federation
[b]Irkutsk Institute (branch) of The All-Russian State University of Justice
(RPA of the Ministry of Justice of Russia) Irkutsk, Russian Federation
[c]Baikal State University
Irkutsk, Russian Federation

Received 31.10.2019, received in revised form 30.12.2019, accepted 10.01.2020

Abstract. The aim of the work is to study the criminal policy in relation to crimes committed using technologies based on artificial intelligence algorithms. The varieties of these crimes are described: phishing, the use of drones, the synthesis of fake information, attacks through automated autonomous systems and bots. Given the fact that artificial intelligence technologies are capable of self-learning and independent actions without direct human intervention and control, the key issue in the criminal policy regarding crimes committed using artificial intelligence algorithms is the question of the subject of criminal liability. The concepts existing in official documents and scientific literature are analyzed on this issue, in the development of scientific discussion, it is proposed to update the legal construction of "innocent harm". The prospects of criminal policy in this direction are indicated in the creation of a fundamentally new variety of blanket norms: from "law as a text" to "law as a code" and its implementation by technological platforms.

Keywords: artificial intelligence, artificial intelligence technologies, the subjectivity of artificial systems, the subject of criminal liability in high-tech crimes, the improvement of the criminal law, innocent harm, "the law as a code".

Research area: law.

Citation: Sukhodolov, A.P., Bychkov, A.V., Bychkova, A.M. (2020). Criminal policy for crimes committed using artificial intelligence technologies: state, problems, prospects. J. Sib. Fed. Univ. Humanit. Soc. Sci., 13(1), 116-122. DOI: 10.17516/1997-1370-0542

* Corresponding author E-mail address: amb-38@mail.ru, science@bgu.ru, rpa38@mail.ru
ORCID: 0000-0002-8233-9520 (Bychkova)

Introduction to the research problem

"The National Strategy for the Development of Artificial Intelligence for the period until 2030", approved by Decree 490 of the President of the Russian Federation of October 10, 2019, defines artificial intelligence as a set of technological solutions that allows simulating human cognitive functions (including self-learning and finding solutions without a predetermined algorithm) and obtaining results when performing specific tasks that are comparable to at least the results of human intellectual activity. The complex of technological solutions includes information and communication infrastructure, software (particularly those using machine learning methods), processes and services for data processing and search for solutions.

Technologies based on the use of artificial intelligence include, in particular, computer vision, natural language processing, speech recognition and synthesis, intellectual decision support and promising methods of artificial intelligence.

Artificial intelligence is considered as a triple-use technology that can be used for civil, military and criminal purposes (Larina, Ovchinsky, 2018: 374). Partly due to the fact that this technology is capable of self-learning and independent actions without direct human intervention and control, a number of serious questions arise for the legal regulation of relations involving artificial intelligence, including legal liability issues.

Statement of the problem

Socially dangerous acts, in which the method of committing a crime is the use of technologies based on artificial intelligence algorithms, include such acts as fishing, the use of drones, the synthesis of fake information, encroachments through automated autonomous systems and bots (Sukhodolov, Bychkova, 2018: 756).

Fishing refers to a form of Internet fraud, the purpose of which is to gain access to confidential user data such as logins and passwords. Mass mailing of emails on behalf of popular brands and personal messages within various services (most often banks and social networks) with links to a site that is apparently indistinguishable from the real one, leads some users to enter their usernames and passwords when they go to a fake page used to access a particular site, as a result of which fraudsters gain access to accounts and bank accounts.

In the case of drones, we deal with the creation of combined systems in which artificial intelligence is combined with a robotic device. Drones associated with artificial intelligence, which are the centre of their control, are used by criminal organizations in attacks on life, in terrorist attacks, surveillance, unauthorized shooting, studying real estate with the aim of the subsequent penetration of drug smuggling and other prohibited substances, the delivery of various items to detention facilities. Thus, drug cartels from Mexico send their goods to the United States using drones with pre-entered GPS data and this completely eliminates the need to use not only a courier, but also an operator (Larina, Ovchinsky, 2018: 37).

The progress of artificial intelligence poses new threats associated with minimizing the human factor: thus, properly trained artificial intelligence will be able to control hacker attacks, create and disseminate misinformation (Sukhodolov, Bychkova, 2017: 160; Alizar, 2017; Efremova, 2017).

There is a process of automation of social engineering, an example of which is bots (abbr. From "robot"), which are programs that can perform certain actions according to a specific algorithm through interfaces designed for people. For example, they can conduct a dialogue with visitors to the forum or on the social network (Ilchenko, 2017; Sukhodolov, Bychkova, 2019: 9; Sukhodolov, Bychkova, 2019: 655).

It is worth noting that the state of the criminal policy in combating crimes committed using artificial intelligence algorithms is by no means covered by the presence of the chapter "Crimes in the field of computer information" in the Criminal Code of the Russian Federation containing four articles: unlawful access to computer information (Article 272 of the Criminal Code); creation, use and distribution of malicious computer programs (Article 273 of the Criminal Code of the Russian Federation); violation of the rules for the operation of means of storage, processing or transmission of computer information and information and telecommunication networks (Article 274 of the Criminal Code of the Russian Federation) and unlawful impact on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation).

Obviously, technologies based on artificial intelligence algorithms can be a tool for a wide range of crimes, including attacks on individuals, property, environmental safety, public and state interests. As an example, we can cite the "deep fakes" technology, the use of which allows creating reliable-looking video images. Thus, the technology of subject-independent face swapping and face reconstruction called Face Swapping GAN (FSGAN) does not depend on the falsified subject and can be applied to any pair of faces without even requiring machine learning on these faces. As a result, we can observe how famous people allegedly participate in obscene filming or open their mouths to utter someone else's text with their own voice. From the point of view of the laws in force in most countries of the world, the production and distribution of such fakes can be qualified as slander, however, Texas lawmakers, in anticipation of the 2020 elections, also criminalized the fact of creating political deepfakes, punishing these acts with up to a year in prison (Noskov, 2019).

Conceptual basis of the study

I.V. Anokhov rightly draws attention to the emergence of a new public subject called "a cyber physical system that should solve two fundamental problems of modern man, namely, the inability to process an exponentially increasing amount of information, as well as the insufficient stability of the results (compared with robotics) of his mechanical and other activities" (Anokhov, 2019: 380). It is no coincidence in this regard that the issue of the subject of criminal liability is a key problem in criminal policy regarding crimes committed using artificial intelligence algorithms. This issue is raised both at the level of official documents and is discussed in specialized literature (Begishev, Khasimova, 2018; Shestak, Volevodz, 2019, etc.). The current concepts are presented as follows.

1. Based on the fact that the subject of law is not a natural reality, but a design created to describe legally significant factual compositions, it becomes possible to formulate the concept of "electronic entity" and further consider it as a subject of law, since the latter is essentially a set of legal obligations and rights, the content of which can be recognized as the actions of artificial intelligence. Such an approach makes it possible to define an "electronic entity" (a machine, a robot or a program) as a carrier of artificial intelligence that has a human-like intelligence, the ability to make decisions that are conscious and not based on the algorithm laid down by the creator, and therefore certain rights and obligations (Shestak, Volevodz, 2019: 200, Morkhat, 2018).

2. The legal status of artificial intelligence is believed to be similar to the legal status of animals (Larina, Ovchinsky, 2019: 174). Thus, according to the head of the board of directors of Mail.ru and the founder of Grishin Robotics Dmitry Grishin, robots cannot be subjects of law due to the lack of emotions, but they are able to carry out autonomous actions like animals, and therefore must be legal entities and can be endowed with legal personality (Grishin, 2016).

3. N.L. Denisov writes that one more important issue that is worth considering is the possibility of a special harmful effect on the learning artificial intelligence by another person who is not its developer and believes that in this case its responsibility can be established in criminal law on the basis of the provisions provided for in Art. 150 "Involvement of a minor in the commission of a crime" of the Criminal Code of the Russian Federation, "A common feature of artificial intelligence and minors is that they are not able to critically treat harmful effects and, accordingly, are likely to follow such an influence. However, at the same time, it is impossible to absolve the developer from liability on the basis that he did not provide for such an opportunity and (or) again did not determine the appropriate measures of protec-

tion against such a negative impact" (Denisov, 2019: 19).

4. A number of American jurists propose to consider artificial intelligence as an employee and register it as a legal entity. At the same time, the responsibility will continue to rest with the owner of artificial intelligence, but artificial intelligence itself as a legal entity may be requested to compensate for damage, including requisition in favour of the person who suffered the damage (Larina, Ovchinsky, 2019: 175).

5. The legislation on artificial intelligence is proposed to be developed by analogy with Roman law regarding slaves: the owner bears responsibility for the damage caused by their slave (Larina, Ovchinsky, 2019: 174). PACE recommendations "Merging with Technologies, Artificial Intelligence and Human Rights" #2102 dated April 28, 2017 contain a statement that responsibility for the acts of artificial intelligence lies with a person, regardless of the circumstances of the incident, and even references to the independence of decisions made by artificial intelligence units cannot relieve their creators, owners and operators of liability (Technological Convergence… 2017). The head of Paul Allen Institute of Artificial Intelligence O. Etzioni believes that an autonomous system using artificial intelligence is required to submit to the full range of laws that apply to its human operator. Such a rule should cover private, corporate, and state systems, and the rules of international law need to be changed so that a person cannot claim that an autonomous system has done something that he could not understand or foresee (Etzioni, 2016). The position of O. Etzioni is also supported by some Russian authors, who point out that "at the present stage of the development of law, the illegal behaviour of artificial intelligence should always result in human responsibility" (Shestak, Volevodz, 2019: 202-203).

Discussion

As rightly pointed out by V.A. Shestak and A.G. Volevodz, new technologies do not necessarily require the formation of special or new rules, "Existing legal concepts are flexible and abstract enough to adapt to new scenarios for the development of technology" (Shestak, Volevodz, 2019: 203).

Fully sharing this opinion, we believe it is right to actualize one of such legal constructions in the development of this scientific discussion that is innocent harm, according to which "the act is recognized as committed innocently, if the person who committed it did not realize and because of the circumstances of the case could not be aware of the social danger of their actions (inaction) or did not foresee the possibility of socially dangerous consequences and, according to the circumstances of the case, should not or could not have foreseen them" (part 1 of Article 28 of the Criminal Code of the Russian Federation). In this regard, the concept of the distribution of responsibility between entities involved in both the development and use of technologies based on artificial intelligence algorithms seems to be the most viable.

As for the prospects of criminal policy in this direction, we believe that they can be seen in creating a fundamentally new variety of blanket norms from "law as a text" to "law as a code". Thus, the USA and the countries of the British Commonwealth of Nations, primarily Canada, Australia and New Zealand, are preparing for a gradual transition from the "law as a text" approach with its interpretation by people, to "law as a code" decisions and its implementation by technology platforms. Based on this fact, V.S. Ovchinsky and E.S. Larina write that the legislation will not only regulate people's behaviour, but also determine the requirements for algorithms, i.e. to certain procedures and sequences, which then, being recorded in a programming language, will have to be automatically executed on the platform. In this regard, the law becomes the basis for the code, that is, it turns into a kind of textual description of the algorithm or sequence of operations, which are then encoded in one programming language or another and converted into a program automatically executed by the platform (Larina, Ovchinsky, 2019: 158, 164- 165).

Conclusion

The use of artificial intelligence technologies in criminal activity is a distinctive feature of modern crime and requires careful attention to improving criminal policy in this direction. The concept of the distribution of responsibility between entities involved in the development and use of technologies based on artificial intelligence algorithms in combination with the legal construction of "innocent harm" seems to be the most rational. Prospects for criminal policy are concentrated in the formation of a fundamentally new type of blanket norms in the form of "law as a code".

References

Alizar, A. (2017). *Neiroset' sdelala fal'shivogo Obamu* [*Neural network made a fake Obama*]. Available at: www.habr.com/post/405269/

Anokhov, I.V. (2019). Dvizhushchie sily Industrii 4.0 i ee posledstviia dlia cheloveka i ekonomiki. Novye osnovaniia dlia sborki obshchestva [Drivers of Industry 4.0 and its implications for humans and economies. New grounds for the assembly of society]. In *Izvestiia Baikal'skogo gosudarstvennogo universiteta* [*Bulletin of Baikal State University*], 29 (3), 379–387.

Begishev, I.R., Khasimova, Z.I. (2018). Kriminologicheskie riski primeneniia iskusstvennogo intellekta [Criminological risks of using artificial intelligence]. In *Vserossiiskii kriminologicheskii zhurnal* [*All-Russian Criminological Journal*], 12 (6), 767–775.

Denisov N.L. (2019). Kontseptual'nye osnovy formirovaniia mezhdunarodnogo standarta pri ustanovlenii ugolovnoi otvetstvennosti za deianiia, sviazannye s iskusstvennym intellektom [The conceptual framework for the formation of an international standard in criminalizing acts related to artificial intelligence]. In *International Criminal Law and International Justice* [*International Criminal Law and International Justice*], 4, 18–20.

Efremova, E. (2017). *Iskusstvennyi intellekt nauchilsia delat' feikovye video* [*Artificial intelligence has learned to make fake videos*]. Available at: https://www.ridus.ru/news/266977

Etzioni, O. (2016). *Interv'iu* [*Interview*]. Available at: www.hardnews24.ru/intervyu-orenetcioni-direktor-instituta-iskusstvennogo-intellekta-im-allena

Grishin, D. (2016). *Zakon o robotekhnike* [*Law on Robotics*]. Available at: www.echo.msk.ru/programs/tochka/1893198-echo

Ilchenko S. (2017). *Offering sex. Predlagat' intim. Kak roboty razvodiat liudei na seks i den'gi* [*How robots play people for sex and money*]. Available at: www.dsnews.ua/society/potolkuem-malost-kogda-boty-nachnut-upravlyat-lyudmi-20072017220000

Khisamova, Z.I. (2019). Ugolovnaia otvetstvennost' i iskusstvennyi intellekt: teoreticheskie i prikladnye aspekty [Criminal liability and artificial intelligence: theoretical and applied aspects]. In *Vserossiiskii kriminologicheskii zhurnal* [*All-Russian Criminological Journal*], 13(4), 564-574.

Larina, E.S., Ovchinsky, V.S. (2018). *Iskusstvennyi intellekt. Bol'shie dannye. Prestupnost'* [*Artificial Intelligence. Big data. Crime*]. Moscow, Book World, 416 p.

Larina, E.S., Ovchinsky, V.S. (2019). *Iskusstvennyi intellekt. Etika i pravo. Sud'ia s iskusstvennym intellektom* [*Artificial Intelligence. Ethics and law. A Judge with Artificial Intelligence*]. Moscow, Book World, 192 p.

Morkhat, P.M. (2018). Iunit iskusstvennogo intellekta kak elektronnoe litso [Artificial Intelligence Unit as an Electronic Entity]. In *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriia: Iurisprudentsiia* [*Bulletin of Moscow State Regional University. Series: Jurisprudence*], 2, 61–73.

Noskov, A. (2019). *Kaliforniia zapreshchaet dip feiki pered vyborami 2020* [*California prohibits deepfakes before the 2020 election*]. Available at: https://hightech.plus/2019/10/08/kaliforniya-zapreshaet-dipfeiki-pered-viborami-2020

O razvitii iskusstvennogo intellekta v Rossiiskoi Federatsii (vmeste s "Natsional'noi strategiei razvitiia iskusstvennogo intellekta na period do 2030 goda"): Ukaz Prezidenta RF ot 10 okt. 2019 g. № 490 [On the development of artificial intelligence in the Russian Federation (together with the National Strategy for the Development of Artificial Intelligence for the period until 2030): Decree 490 of the President of the Russian

Federation dated October 10, 2019]. In *Sobranie zakonodatel'stva RF. 2019. № 41. St. 5700* [*Collection of Legislation of the Russian Federation. 2019. No. 41. Art. 5700*].

Shestak, V.A., Volevodz, A.G., Alizade, V.A. (2019). O vozmozhnosti doktrinal'nogo vospriiatiia sistemoi obshchego prava iskusstvennogo intellekta kak sub''ekta prestupleniia: na primere ugolovnogo zakonodatel'stva SSHA [Concerning the possibility of doctrinal perception of artificial intelligence by the common law system as a subject of crime: based on the example of US criminal law. In *Vserossiiskii kriminologicheskii zhurnal* [*All-Russian Criminological Journal*], 13(4), 197–206.

Shestak, V.A., Volevodz, A.G. (2019). Modern needs of the legal support of artificial intelligence: a view from Russia. In *Vserossiiskii kriminologicheskii zhurnal* [*All-Russian Criminological Journal*], 13(2), 197–206.

Sukhodolov, A.P., Bychkova, A.M., Ovanesyan, S.S. (2019). Zhurnalistika s iskusstvennym intellektom [Journalism Featuring Artificial Intelligence]. In *Voprosy teorii i praktiki zhurnalistiki* [*Theoretical and Practical Issues of Journalism*], 8(4), 647–667. DOI: 10.17150/2308-6203.2019.8(4).647-667.

Sukhodolov, A.P., Bychkova, A.M. (2019). Tsifrovyye tekhnologii i narkoprestupnost': problemy protivodeystviya ispol'zovaniyu messendzhera «Telegram» v rasprostranenii narkotikov [Digital technologies and drug-related crime: problems of counteracting the use of "Telegram" messenger for trafficking drugs]. In *Vserossiiskii kriminologicheskii zhurnal* [*Russian Journal of Criminology*], 13(1), 5–17. DOI: 10.17150/2500-4255.2019.13(1).5-17.

Sukhodolov, A.P., Bychkova, A.M. (2017). «Feikovye novosti» kak fenomen sovremennogo mediaprostranstva: poniatie, vidy, naznachenie, mery protivodeistviia ["Fake news" as a phenomenon of modern media space: concept, types, purpose, countermeasures]. In *Voprosy teorii i praktiki zhurnalistiki* [*Problems of journalism theory and practice*], 6 (2), 143–169.

Sukhodolov, A.P., Bychkova, A.M. (2018). Iskusstvennyi intellekt v protivodeistvii prestupnosti, ee prognozirovanii, preduprezhdenii i evoliutsii [Artificial Intelligence in Combating Crime, its Forecasting, Prevention and Evolution]. In *Vserossiiskii kriminologicheskii zhurnal* [*All-Russian Criminological Journal*], 12 (6), 753–766.

Technological Convergence, Artificial Intelligence and Human Rights. Recommendation of Parliamentary Assembly of the Council of Europe (2017). *No. 2102.* Available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

Уголовная политика в отношении преступлений, совершенных с использованием технологий искусственного интеллекта: состояние, проблемы, перспективы

А.П. Суходолов[а], А.В. Бычков[б], А.М. Бычкова[в]

[а]Байкальский государственный университет
Российская Федерация, Иркутск
[б]Иркутский институт (филиал) «Всероссийский государственный университет юстиции (РПА Минюста России)»
Российская Федерация, Иркутск
[в]Байкальский государственный университет
Российская Федерация, Иркутск

Аннотация. Целью работы является исследование уголовной политики в отношении преступлений, совершаемых с использованием технологий, основанных на алгоритмах искусственного интеллекта. Описаны разновидности данных преступлений: фишинг, использование дронов, синтезирование фейковой информации, посягательства посредством автоматизированных автономных систем и ботов. С учетом того, что технологии искусственного интеллекта способны к самообучению и самостоятельным действиям без непосредственного вмешательства и контроля со стороны человека, ключевой проблемой уголовной политики в отношении преступлений, совершаемых с использованием алгоритмов искусственного интеллекта, является вопрос о субъекте уголовной ответственности. Анализируются существующие в официальных документах и научной литературе концепции по данной проблематике, в развитие научной дискуссии предлагается актуализировать правовую конструкцию «невиновное причинение вреда». Перспективы уголовной политики в этом направлении обозначены в создании принципиально новой разновидности бланкетных норм: от «закона как текста» к «закону как коду» и его исполнению технологическими платформами.

Ключевые слова: искусственный интеллект, технологии искусственного интеллекта, субъективизация искусственных систем, субъект уголовной ответственности в высокотехнологичных преступлениях, совершенствование уголовного закона, невиновное причинение вреда, «закон как код».

Научная специальность: 12.00.00 – юридические науки.