

ARTIFICIAL INTELLIGENCE AND DIGITAL CRIMINALITY: OUTLINES OF A TECHNOETIC APPROACH

KHASANOVA V.V. 

Khasanova Victoria Valentinovna - Police lieutenant colonel, Deputy head of the department of administrative law and administrative responsibility of the department of internal affairs, Aktobe law institute of the ministry of internal affairs of the Republic of Kazakhstan named after Malkejar Bukenbayev, Aktobe, Kazakhstan.

E-mail: vikakiper85@bk.ru, <https://orcid.org/0000-0001-5579-1565>

Abstract. This article is devoted to the study of the phenomenon of digital criminology - an emerging field of scholarship that examines the potential for artificial intelligence (AI) to be used by offenders, including the category of offences conventionally referred to as AI-crime. The object of the study is crime, victimization, and justice under the conditions of digital society, where the boundaries between online and offline reality are increasingly blurred; the subject of the study is the risks and ethical dimensions of employing AI for criminal purposes. The aim of the work is to define the contours of digital criminology on the basis of an interdisciplinary, techno-social approach that integrates criminology, philosophy of technology, and cyberlaw. The methodological foundation of the study comprises comparative-legal, systemic, and structural-functional analysis, along with elements of predictive modeling. The article examines such manifestations of digital crime as automated cyberattacks, deepfake generation, algorithmic fraud, and the manipulation of user behavior through recommendation systems. It is shown that the emerging field of techno-ethics has yet to develop stable criteria for assessing deviant online behavior, and that existing legal mechanisms insufficiently account for the specific nature of algorithmic and autonomous forms of unlawful activity, including the problem of attributing responsibility where autonomous systems are involved. Particular attention is given to issues surrounding the legal classification of acts committed with the use of generative models, as well as gaps in the evidentiary basis for digital crimes. The article substantiates the need to improve criminal legislation, to develop specialized educational programs, and to train personnel capable of countering cybercrime in a «hybrid» world, where the line between human and machine agency is becoming increasingly indistinct, and where traditional models of guilt and intent require reconsideration.

Key words: artificial intelligence, cybercrime, law, crime, technoethics, digital criminology, digital technologies.

Introduction

The penetration of digital technologies into all spheres of everyday life allows us to say that «life has been digitized», and a person, despite his consent, is increasingly becoming a subject of digital data. For a long time, researchers in Computer Science were so fascinated by the endless potential of new technologies that the negative consequences of their use were underestimated or neglected [1] - this position was called «technooptimism» and is characterized by an inability to effectively compare benefits and risks. This was reflected in Google's corporate code under the previous slogan «Do not do Evi» [2].

Today, experts in the field of technology and forensics admit: AI systems open up new opportunities not only for serious crimes, but also for dubious practices in law enforcement. The growth of digital criminality shows that the rapid development of technologies simultaneously opens the way for offenders and complicates the structure of criminality [3]. At the same time, many of the social consequences of technological changes - in particular, in the areas of predicting and preventing crime, strengthening control and transforming criminal justice practices - remain little studied, although international organizations, including Interpol and UNICRY, are developing relevant recommendations for the use of artificial intelligence and robotics in law enforcement [4].

Materials and methods of research

The concept of «artificial intelligence» remains vague: in mass culture it is accompanied by images of «killer robots» and antiutopic control systems, and in reality AI works at a more everyday level - from consumer electronics to translation services. As K. Piper notes, the discussion of artificial

intelligence is often accompanied by confusion and disinformation, since the term itself is used to designate many different phenomena [5]. The terminological confusion is further exacerbated by the debate about the philosophical ambiguity of the concept of «intelligence» itself, especially about the possibility of creating AI with consciousness.

The problem of «dual purpose» of technologies is not new to the field of cybercrime and Cybersecurity: AI can be used both for attack and defense - including for the prevention and detection of offenses. While AI can be used to attack government structures, governments also use it to expand their capabilities, such as monitoring, tracking, and protecting critical infrastructure. At the same time, the spread of AI creates new gaps, as there are cases of its negative and evil use.

One of the legal areas of application of AI is crime prevention and detection systems, although there is also a reverse side to this-the likelihood of abuse of this technology for illegal activity. An illustrative example of the «dual expediency» of such systems is the case when an autonomous software agent, created by Swiss researchers, independently purchased a batch of a prohibited substance through one of the sites on the darkweb [6]. At the same time, research in the field of attacks used against artificial intelligence models shows that minor changes made specifically for input data can seriously distort the results of the work of such systems [7; 8], which opens up space for new types of abuse. The main problem is the use of systems that do not belong to the category of «artificial superintelligence» by criminals to automate, provide and expand the scope of certain types of cybercrime, as well as the emergence of previously absent, fundamentally new opportunities for committing offenses in the digital environment.

The term «technoetics» was introduced in 1974 by the philosopher Mario Bunge to designate the special responsibility of engineers and technologists in the development of the ethical component of technologies. Ethics is generally defined as a system of normative judgments about morally appropriate behavior rather than descriptive; while technoetics is an interdisciplinary field that establishes the appropriate attitude to the use of technologies in specific situations, combining deontological, conceptualist and utilitarian approaches. It covers both established areas such as bioethics, engineering ethics, computer ethics, and new areas such as Neuroethics.

According to R. Luppigini, the task of technoetics is to establish a dialogue on the ethical use of technologies, their protection from illegal use and the formation of principles that direct technological progress to the public good in various social contexts and ethical dimensions. It should be noted that technoetics is a rapidly developing field of ethics associated with the rapid development of technologies and their integration into everyday life; it relies on extensive knowledge of areas such as information and communication theory, Social Sciences, Technical and Natural Sciences, Applied Ethics and philosophy [9].

Results and its discussion

Technological progress, affecting economic dynamics, creates new forms of inequality at the level of the labor market, regions and countries. For example, a joint study by Dell Technologies and the Institute for the Future showed that a person's dependence on machines gradually develops into a cooperative relationship, in which a person brings such qualities as creativity, purposefulness and entrepreneurship. Discussions of AI ethics traditionally focus on negative effects, although there are many examples of the useful use of AI on a daily basis. It is also important to consider potential benefits, such as increased efficiency and productivity, which, according to the European Commission's high-level group of AI experts, contribute to well-being, which is itself an ethical value. Recently, such discussions are also considered more and more often from the point of view of politics. Among the main ethical issues, the following are distinguished: violation of data confidentiality; leakage of confidential information; spread of disinformation and deepfakes; lack of supervision and responsibility; risks associated with the use of facial recognition technologies, labor automation, monitoring of health status. The situation when the chatbot of one of the largest technological

companies began to make offensive and discriminatory statements as a result of interaction with users is a visual example of the intensification of algorithmic prejudice. Similar risks arise when using automatic content moderation systems, such as determining the language of hatred on the Instagram social network.

The real danger lies not in the hypothetical dominance of the «superintelligence», but in the fact that modern systems are not perfect enough to solve the tasks set: the intelligence of machines will continue to be improved, although in the near future it is unlikely to reach the level of human intelligence. The need to develop human skills and values capable of overcoming the resulting gap and mitigating the risks posed by powerful AI systems in the context of modern complex communities is growing. The key to eliminating such risks is to invest in human capital and conduct responsible monitoring of artificial intelligence, which will allow maintaining public confidence in this technology.

Despite the fact that more than fifteen years have passed since the widespread adoption of social networks, augmented reality technologies and artificial intelligence, a significant part of criminological research still traditionally focuses on information systems and Internet technologies, considering them either as objects of crime or as means of creating other, traditional types of criminal activity. Moreover, many approaches are based on internal dualism: cybercrime is still viewed as a mirror or network version of its counterparts in the physical world, differing from them in terms of creation and spatial scope, but not differing in essence and internal nature. This situation shows that the traditional criminological paradigm is not sufficiently adapted to describe qualitatively new deviant and criminal forms of behavior that arise at the junction of digital technologies and artificial intelligence. In this regard, the formation of an appropriate conceptual framework acquires direct practical significance not only for theoretical, but also for law enforcement activities, as well as for the development of measures to prevent relevant offenses.

In an attempt to determine the place of artificial intelligence in the system of criminological knowledge, a number of terms can be found in the relevant scientific literature that are used to describe the phenomenon in question: «cybercrime based on AI», «cybercrime based on AI», «AI-criminality», «harmful AI», «Evil used AI», «harmful and negative use of AI» [10] and a number of others. Such terminological diversity indicates both the relative novelty of the phenomenon itself and the lack of a single, generally recognized conceptual skeleton that can unite different research traditions [11].

Conclusion

The analysis confirms that the development of artificial intelligence and its integration into everyday life radically transform the structure of criminality, erase the boundaries between the online and offline worlds and form a new, «hybrid» reality in which classic criminological dichotomies are deprived of explanatory power. Digital criminology, which relies on a technosocial and non-binary approach, is an adequate methodological response to this criticism, which allows us to consider criminality, victimization and justice as phenomena inextricably linked with the digital infrastructure of society.

The main conclusion of the study is the thesis that the formation of technoetic norms has not been completed, which can serve as a criterion for assessing the deviant or criminal nature of behavior, which was indirect through digital technologies. In such conditions, an interdisciplinary approach that combines criminology, the philosophy of Technology, Law and ethics, capable of ensuring a balanced regulation in which technological progress does not contradict the principles of human rights and justice, becomes especially important.

The results obtained form the basis for further development of proposals for improving criminal legislation in terms of regulating legal relations related to the use of artificial intelligence, and can also be used in educational activities in the training of specialists in the field of digital criminology and law. The prospects for further research are associated with an empirical study of specific forms of AI-criminality, the development of criteria for the technoetic assessment of online behavior and the

References

1. Schneier B. Inside the twisted mind of the security professional. // Wired. — 2008. — 20 march. — URL: <https://www.wired.com/2008/03/securitymatters-0320/>
2. Mayer D. Why Google was smart to drop its «Don't Be Evil» motto // Fast Company. — 2016. — 9 february. — URL: <https://www.fastcompany.com/3056389/why-google-was-smart-to-drop-its-dont-be-evil-motto>
3. Ife C. C., Davies T., Murdoch S. J., Stringhini, G.. Bridging information security and environmental criminology research to better mitigate cybercrime. — 2019. — 35 p. — arXiv:1910.06380. — DOI: [10.48550/arXiv.1910.06380](https://doi.org/10.48550/arXiv.1910.06380).
4. Interpol and UNICRI. Artificial intelligence and robotics for law enforcement. INTERPOL, United Nations Interregional Crime and Justice Research Institute. — Lyon: INTERPOL; Turin: UNICRI, 2019. — 44 p. — URL: <https://www.interpol.int/content/download/13060/file/INTERPOL-UNICRI%201st%20AI%20and%20Robotics%20Report.pdf>
5. Piper K. The case for taking AI seriously as a threat to humanity. // Vox. — 2018. — 21 december. — URL: <https://www.vox.com/future-perfect/2018/12/21/18126576/ai-artificial-intelligence-machine-learning-safety-alignment>
6. Kasperkevic J. Swiss police release robot that bought ecstasy online. // The Guardian. — 2015. — 21 april. — URL: <https://www.theguardian.com/technology/2015/apr/21/swiss-police-release-robot-random-darknet-shopper-ecstasy>.
7. Huang S., Papernot N., Goodfellow I., Duan Y., Abbeel, P. Adversarial attacks on neural network policies. // — 2017. — arXiv:1702.02284. — DOI: [10.48550/arXiv.1702.02284](https://doi.org/10.48550/arXiv.1702.02284).
8. Goodfellow I. J., Shlens J., Szegedy C. Explaining and harnessing adversarial examples. // — 2015. — arXiv:1412.6572. — DOI: [10.48550/arXiv.1412.6572](https://doi.org/10.48550/arXiv.1412.6572).
9. Yampolskiy R. V. Taxonomy of pathways to dangerous AI. — 2015. — arXiv:1511.03246. — DOI: [10.48550/arXiv.1511.03246](https://doi.org/10.48550/arXiv.1511.03246).
10. Ciancaglini V. et.al. Malicious uses and abuses of artificial intelligence. Trend Micro Research, United Nations Interregional Crime and Justice Research Institute, Europol's European Cybercrime Centre. — 2020. — URL: https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf
11. Brundage M., Avin S., Clark J. et al. The malicious use of artificial intelligence: forecasting, prevention, and mitigation. // — 2018. — 101 p. — URL: https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

Әдебиеттер тізімі

1. Schneier B. Inside the twisted mind of the security professional. // Wired. — 2008. — 20 march. — URL: <https://www.wired.com/2008/03/securitymatters-0320/>
2. Mayer D. Why Google was smart to drop its «Don't Be Evil» motto // Fast Company. — 2016. — 9 february. — URL: <https://www.fastcompany.com/3056389/why-google-was-smart-to-drop-its-dont-be-evil-motto>
3. Ife C. C., Davies T., Murdoch S. J., Stringhini, G.. Bridging information security and environmental criminology research to better mitigate cybercrime. — 2019. — 35 p. — arXiv:1910.06380. — DOI: [10.48550/arXiv.1910.06380](https://doi.org/10.48550/arXiv.1910.06380).
4. Interpol and UNICRI. Artificial intelligence and robotics for law enforcement. INTERPOL, United Nations Interregional Crime and Justice Research Institute. — Lyon: INTERPOL; Turin: UNICRI, 2019. — 44 p. — URL: <https://www.interpol.int/content/download/13060/file/INTERPOL-UNICRI%201st%20AI%20and%20Robotics%20Report.pdf>

[UNICRI%201st%20AI%20and%20Robotics%20Report.pdf](#)

5. Piper K. The case for taking AI seriously as a threat to humanity. // Vox. — 2018. — 21 december. — URL: <https://www.vox.com/future-perfect/2018/12/21/18126576/ai-artificial-intelligence-machine-learning-safety-alignment>

6. Kasperkevic J. Swiss police release robot that bought ecstasy online. // The Guardian. — 2015. — 21 april. — URL: <https://www.theguardian.com/technology/2015/apr/21/swiss-police-release-robot-random-darknet-shopper-ecstasy>.

7. Huang S., Papernot N., Goodfellow I., Duan Y., Abbeel, P. Adversarial attacks on neural network policies. // — 2017. — arXiv:1702.02284. — DOI: [10.48550/arXiv.1702.02284](https://doi.org/10.48550/arXiv.1702.02284).

8. Goodfellow I. J., Shlens J., Szegedy C. Explaining and harnessing adversarial examples. // — 2015. — arXiv:1412.6572. — DOI: [10.48550/arXiv.1412.6572](https://doi.org/10.48550/arXiv.1412.6572).

9. Yampolskiy R. V. Taxonomy of pathways to dangerous AI. — 2015. — arXiv:1511.03246. — DOI: [10.48550/arXiv.1511.03246](https://doi.org/10.48550/arXiv.1511.03246).

10. Ciancaglini V. et.al. Malicious uses and abuses of artificial intelligence. Trend Micro Research, United Nations Interregional Crime and Justice Research Institute, Europol's European Cybercrime Centre. — 2020. — URL:

https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

11. Brundage M., Avin S., Clark J. et al. The malicious use of artificial intelligence: forecasting, prevention, and mitigation. // — 2018. — 101 p. — URL: https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ЦИФРЛЫҚ ҚЫЛМЫСТЫЛЫҚ: ТЕХНОЭТИКАЛЫҚ ТӘСІЛДІҢ КОНТУРЛАРЫ

ХАСАНОВА В.В. 

Хасанова Виктория Валентиновна - Полиция подполковнигі, ПО әкімшілік құқық және әкімшілік жауапкершілік кафедрасы бастығының орынбасары, Қазақстан Республикасы ІІМ Малкеджар Бөкенбаев атындағы Ақтөбе заң институты, Ақтөбе қ., Қазақстан.

E-mail: vikakiper85@bk.ru, <https://orcid.org/0000-0001-5579-1565>

Аңдатпа. Мақала цифрлық криминологияның феноменін зерттеуге арналған - бұл құқық бұзушылардың жасанды интеллектті (ЖИ) пайдалану әлеуетін зерттейтін, соның ішінде шартты түрде ЖИ-қылмыстылық деп аталатын қылмыстылықты қамтитын қалыптасып келе жатқан ғылыми бағыт. Зерттеу объектісі ретінде онлайн-және офлайн-шындық арасындағы шекараларды жоятын цифрлық қоғам жағдайындағы қылмыстылық, виктимизация және әділ сот алынады; пәні - ЖИ-ды қылмыстық мақсатта қолданудың тәуекелдері мен этикалық аспектілері болып табылады. Жұмыстың мақсаты - криминологияны, техника философиясын және киберқұқықты біріктіретін пәнаралық, техноәлеуметтік тәсіл негізінде цифрлық криминологияның шеңберін айқындау. Зерттеудің әдіснамалық негізін салыстырмалы-құқықтық, жүйелік және құрылымдық-функционалдық талдау, сондай-ақ болжамдық модельдеу элементтері құрады. Автоматтандырылған кибершабуылдар, дипфейктерді генерациялау, алгоритмдік алаяқтық және ұсыныстар жүйелері арқылы пайдаланушылардың мінез-құлқын манипуляциялау сияқты цифрлық қылмыстылықтың көріністері қарастырылады. Қалыптасып келе жатқан техноэтика девиантты онлайн мінез-құлықты бағалаудың тұрақты өлшемдерін әлі әзірлей алмағаны, ал қолданыстағы құқықтық тетіктер алгоритмдік және автономды құқыққа қайшы қызмет нысандарының ерекшелігін жеткіліксіз ескеретіні көрсетілген, оның ішінде автономды жүйелердің қатысуымен жауапкершілікті атрибуциялау мәселесі де қамтылған. Генеративті модельдерді пайдалана отырып жасалған әрекеттерді саралау мәселелеріне және цифрлық қылмыстардың дәлелдеу базасындағы олқылықтарға ерекше назар аударылған. Қылмыстық заңнаманы жетілдіру, мамандандырылған білім беру бағдарламаларын әзірлеу және адам мен машина агенттілігі арасындағы шекара барған сайын бұлыңғырланып бара жатқан «гибридті» әлем жағдайында киберқылмыспен күресу үшін кадрлар даярлау қажеттігі негізделген, сонымен қатар кінә мен қасақаналықтың дәстүрлі модельдерін қайта пайымдау қажет екені атап өтілген.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЦИФРОВАЯ ПРЕСТУПНОСТЬ: ОЧЕРТАНИЯ ТЕХНОЭТИЧЕСКОГО ПОДХОДА

ХАСАНОВА В.В. 

Хасанова Виктория Валентиновна - Подполковник полиции, Заместитель начальника кафедры административного права и административной ответственности ОВД, Актюбинский юридический институт МВД Республики Казахстан имени Малкеджара Букенбаева, г. Ақтөбе, Казахстан

E-mail: vikakiper85@bk.ru, <https://orcid.org/0000-0001-5579-1565>

Аннотация. Статья посвящена изучению феномена цифровой криминологии - формирующегося научного направления, исследующего потенциал использования искусственного интеллекта (ИИ) правонарушителями, включая преступность, условно именуемую ИИ-преступностью. Объектом исследования выступают преступность, виктимизация и правосудие в условиях цифрового общества, стирающие границы между онлайн- и офлайн-реальностью; предметом риски и этические аспекты применения ИИ в преступных целях. Целью работы является определение контуров цифровой криминологии на основе междисциплинарного, техносоциального подхода, объединяющего криминологию, философию техники и киберправо. Методологическую основу составили сравнительно-правовой, системный и структурно-функциональный анализ, а также элементы прогностического моделирования. Рассматриваются такие проявления цифровой преступности, как автоматизированные кибератаки, генерация дипфейков, алгоритмическое мошенничество и манипулирование поведением пользователей посредством рекомендательных систем. Показано, что формирующаяся техноэтика еще не выработала устойчивых критериев оценки девиантного онлайн-поведения, а действующие правовые механизмы недостаточно учитывают специфику алгоритмических и автономных форм противоправной деятельности, включая проблему атрибуции ответственности при участии автономных систем. Особое внимание уделено вопросам квалификации деяний, совершенных с использованием генеративных моделей, и пробелам в доказательственной базе цифровых преступлений. Обоснована необходимость совершенствования уголовного законодательства, разработки специализированных образовательных программ и подготовки кадров для противодействия киберпреступности в условиях «гибридного» мира, где грань между человеческой и машинной агентностью становится все более размытой, а традиционные модели вины и умысла требуют переосмысления.

Ключевые слова: искусственный интеллект, киберпреступность, право, преступность, техноэтика, цифровая криминология, цифровые технологии.