Research article
UDC 34:004:349.2:004.8
EDN: https://elibrary.ru/mqtnqg
DOI: https://doi.org/10.21202/jdtl.2024.32

New Approaches to Researching AI Crime: Institutionalization of Digital Criminology

Fotios Spyropoulos

Philips University, Nicosia, Cyprus
Spyropoulos Law Firm, Athens, Greece

Keywords

artificial intelligence,
crime,
criminal deed,
cybercrime,
digital criminology,
digital society,
digital technologies,
ethics,
law,
technoethics

Abstract

Objective: the article deals with modern scientific approaches to the "digital society", identifies new criminological perspectives, such as that of digital criminology in an ever-changing hybrid world, in the scientific study of the potential use of AI by criminals, including what is referred to here as AI crime.

Methods: this article is an essay commonly used in humanities and social sciences, as the author aims to present provocative arguments to encourage readers to rethink AI issues in relation to criminality in the "hybrid world" based on a non-systematic literature review. The arguments should be supported by relevant references to "digital criminology" and its non-binary way of thinking in favour of a techno-social approach.

Results: the era of divided perspectives is coming to an end, and it's time for synergies, especially at the interdisciplinary level. The «mirror of artificial intelligence» can help identify flaws and solutions, ensuring the future of AI and human society is decided by the people. In a digital society, technology is integrated into people's lives, including crime, victimization, and justice. Digital technologies blur the boundaries between online and offline realities, creating a human-technological hybrid world where crimes occur in virtual networks. AI has potential for social good and Sustainable Development Goals, but concerns about human rights violations need to be addressed. Multidisciplinary approaches are needed to ensure safe use, address education inequalities, enhance justice, and identify online behavior as deviant or criminal. In the context of emerging technoethics, the idea that this unofficial norm, derived from a popular belief, will be the 'touchstone' for characterising online mediated behaviour as deviant/crimninal, is missing - or rather in the process of being formed.

Scientific novelty: the author aims to provide some insightful thoughts on formulating the right questions and interesting reflections from a technoethical perspective on the phenomenon of the use of information and communication technologies for criminal purposes under the catalytic influence of AI, recognising the social challenges arising from technological disruption (e.g. prediction and prevention through the transformation of policing, increased surveillance and criminal justice practises) in "digital society".

Practical significance: some of the initial ideas of this theoretical material can be used in the elaboration of proposals for amendements and additions to the current crime legislation, as well as in pedagogical activity, especially in the implementation of educational courses or modules on crime in the context of the digital transformation of society.

For citation

Spyropoulos, F. (2024). New Approaches to Researching AI Crime: Institutionalization of Digital Criminology. *Journal of Digital Technologies and Law, 2*(3), 636–656. https://doi.org/10.21202/jdtl.2024.32

Contents

Introduction

Let us begin by reflecting on the many and varied ways in which digital technologies have permeated everyday life in recent years, leading to the conclusion that nowadays "life is digital". "We are increasingly becoming digital data subjects, whether we like it or not, and whether we choose this or not" (Lupton, 2015).

Moreover, in the digital era, we witness the increasing use of technology and artificial intelligence (further – AI) to solve problems, while improving productivity and efficiency. For decades, computer scientists have been so captivated by the unlimited potential of new technologies that the negative effects of these systems have been probably downplayed or often ignored entirely (Hayward & Maas, 2020)[1]. Known as techno-

[1] Schneier, B. (2008, March 20). Inside the twisted mind of the security professional. Wired. https://clck.ru/3CzSKg

optimism (Danaher, 2022), this failure to effectively balance reward and risk was famously highlighted in "Don't be evil"[2], the former motto of the Google Code of Conduct.

But almost recently, scientists have been invigorated by a number of new research approaches that address how crime will be transformed by the impact of what Greenfield (2017) emphatically refers to as the "radical new technologies and AI of the networked era".

Technologists and criminologists are now realising that Artificial Intelligence systems will open up a plethora of new opportunities for serious criminal exploitation, in addition to enabling questionable policing practices (Hayward & Maas 2020; Ionescu et al., 2020; Broadhurst et al., 2019). Namely, the increase in the rate of crimes committed in the digital world, prove that the fast-evolving technology creates new opportunities for perpetrators while at the same time contributing to a rise in the levels and complexity of crime[3] (Lee & Chua, 2023; Di Nicola, 2022). It does so largely oblivious of the many social challenges posed by technological disruption (e.g. prediction and prevention by transforming policing, enhanced surveillance and criminal justice practices) (Brown, 2006a; Hayward, 2012; Holt & Bossler, 2014).

1. Artificial intelligence: problems of definition

Artificial intelligence can be an elusive concept - a phenomenon that is seemingly ubiquitous but at the same time strangely opaque. In popular culture and news reporting on AI, fanciful narratives often prevail, referring to iconic 'killer robots' or dystopian surveillance systems (Hayward & Maas, 2020). In people's everyday lives, however, AI operates on a much more prosaic level, controlling everything from smart TVs to language translation applications. According to K. Piper[4], "the conversation about AI is full of confusion, misinformation, and people talking past each other – in large part because we use the word 'A.I' to refer to so many things".

The borderline between what counts as AI proper and other forms of technology can be blurred. Moreover, the term 'intelligence' in the context of the AI paradigm is a loaded and deeply contested philosophical and scientific concept not mentioned when the philosophical and technical arguments converge in the debates about whether we will ever develop an AI that has consciousness and is complex enough in the right way to merit our moral concerns and protection (Boddington, 2017). Perhaps it is this generality and uncertainty that confuses people, not least because each supposed AI future raises its own set of concerns about safety, ethics, legality and liability.

---

2 Mayer, D. (2016). Why Google Was Smart To Drop Its 'Don't Be Evil' Motto. Fast Company.

3 Ife, C. C., Davies, T., Murdoch, S. J., & Stringhini, G. (2019). Bridging information security and environmental criminology research to better mitigate cybercrime. arXiv preprint arXiv:1910.06380. https://clck.ru/3CzSMo

4 Piper, K. (2018). The case for taking AI seriously as a threat to humanity, Vox. https://clck.ru/3CzSPd

The so-called "dual-use" aspect of technology is not an entirely new problem when it comes to cybercrime or (cyber-)security. While AI can be used to attack governments, it is also used by them to improve their capabilities. However, there are new vulnerabilities related to how AI can be abused and used maliciously. Systems for crime prevention and detection are among the many legitimate uses of AI (Dilek et al., 2015; Li et al., 2010; Lin et al., 2017; McClendon & Meghanathan, 2015). However, there is also a chance that the technology will be abused and used to further illegal activity (Kaloudi & Li, 2020; Sharif et al., 2016; Mielke & Chen, 2008; van der Wagen & Pieters, 2015). The critical issue is the ability of human attackers to use non-ASI (artificial superintelligence), systems to automate, enable and enhance cybercrime as we know it, as well as the ability to open totally new channels for cybercrime.

If society is to overcome this confusion, what is required are clear answers to straightforward questions: "What exactly is AI?" "What are its capabilities and limits?" & "What are the consequences of its proliferation and use in society, both as a tool for criminal or illegitimate ends, and as a means of security and social control?"

2. An approach to technoethics

The term 'technoethics' was coined in 1974 by the Argentine-Canadian philosopher Mario Bunge (1977) to refer to the special responsibilities of technologists and engineers for the development of ethics as a branch of technology.

"Ethics" can be defined as a code or set of principles by which people live. Ethics is about what is considered morally right and what is considered wrong. When people make moral judgements, they utter normative or prescriptive statements about what should be done, about moral duty and obligation, not descriptive statements about what is done. Ethical theory or moral philosophy, then, is the doctrine of the rules or principles underlying moral decisions, a justification for moral judgements. The application of ethical theory can help users, even to the point of determining how people should behave in various applications of technology.

Accordingly, technoethics is the interdisciplinary field that attempts to determine an appropriate standpoint or attitude or philosophy in the application of technology in real-life situations. Among several ethical theories, the most relevant to technological applications are consequentialism, deontologism and utilitarianism. Technoethics is concerned with the impact of ethics on technology, technological change, technological progress and its applications. This applies both to established areas such as bioethics, computer ethics or engineering ethics, as well as to new fields of research such as neuroethics (Heller, 2012).

Rocci Luppicini (2008) underlines the fact that, "...technoethics is based on the premise that it is crucial to promote dialogue aimed at determining the ethical use of technology, guarding against its misuse and devising thoughtful principles that help guide new technological advances for the benefit of society in a variety of social contexts and ethical dimensions".

To conclude with, technoethics is a rapidly developing area of ethics due to the rapid development of technologies and their integration into everyday life. It draws extensive knowledge from research fields such as information and communication, social sciences, technology and science studies, applied ethics and philosophy to discover the ethical benefits of technology, protect against its misuse and outline common principles that guide new advances in technological development and application for the benefit of society.

In answering the question of why we need technoethics and technological consciousness, there is no question that with the advancing technology of AI and ML we are confronted with technologies that are capable of learning and creating if they have a consciousness of their own. Therefore, we need to address the issues of technological consciousness and technoethics in order to find answers to the emerging moral dilemmas related to technology and to guide these advancing technologies in such a way that they benefit humanity, because after all, every single algorithm that promises a clear benefit can easily be misused to harm.

3. Ethical successes, failures and challenges in artificial intelligence

Technological progress has always been at the heart of the dynamics of the economic system, directly or indirectly affecting all economic and productive activities. The significant changes that are taking place are bringing about changes in a range of productive and economic activities. At the same time, they act as a powerful factor of imbalance and the creation or reproduction of new inequalities and inequities both at the level of the labour market, the structure of employment and the economy, and at the level of the socio-economic development of economies, sectors, regions and countries at the European and international levels.

The issues arising from technological developments and in particular from developments in the field of artificial intelligence are increasingly occupying scientific institutions, companies and public authorities. According to Dell Technologies' research department, which has studied future developments in collaboration with the Institute for the Future, one of the conclusions they have reached is that "people's dependence on machines will have evolved into a collaborative relationship, with people bringing skills such as creativity, passion and entrepreneurship"[5].

When we speak of ethical issues and challenges of technology and AI, there tends to be an implicit assumption that we are speaking of morally bad things. And, of course, most of the AI debate revolves around such morally problematic outcomes that need to be addressed. However, it is worth highlighting that technology and new advances in AI promises numerous benefits (Berendt, 2019)[6]. Many AI policy documents focus

5 Barbaschow, A. (2019, October 8). Machines as consumers: The future according to Dell Technologies. ZDNET.

6 Faggella, D. (2020). Everyday examples of artificial intelligence and machine learning. Boston, MA: Emerj. https://clck.ru/3CzSZw

on the economic benefits of AI that are expected to arise from higher levels of efficiency and productivity. These are ethical values insofar as they promise higher levels of wealth and wellbeing that will allow people to live better lives and can thus be conducive to or even necessary for human flourishing (see more EU's High-Level Expert Group on AI[7]).

But in contrary, the promise of improving efficiency, reducing costs and accelerate research and development has recently been tempered by concerns that these complex, opaque systems may do more harm than good to society. There are numerous accounts of the ethical issues of AI, mostly developments of a long-standing tradition of discussing ethics and AI in the literature (Coeckelbergh, 2019; Dignum, 2019; Müller, 2020), but increasingly also arising from a policy perspective[8]. The most common ethical issues indicatively are: a) Data privacy violations b) Sensitive information disclosure c) Misinformation and Deep Fakes˙ d) Lack of Oversight and Acceptance of Responsibility˙ e) Use of AI (facial recognition, replacement of jobs, health tracking, data provenance, amplification of existing bias in AI technology, lack of explainability and interpretability etc.

To sum up, it is important to underline that the legal and ethical issues that confront society due to Artificial Intelligence (AI) include privacy and surveillance, bias or discrimination, and potentially the philosophical challenge is the role of human judgment. Concerns about newer digital technologies becoming a new source of inaccuracy and data breaches have arisen as a result of its use. So, critical decisions have to be made to ensure we are protecting personal freedoms and using data appropriately.

Fears (justifiable or unjustifiable?) arise from the ever-increasing dominance of machines with artificial intelligence, characterised by 'superintelligence'. But the real danger is not the dominance of superintelligent machines, but of machines that are not yet 'intelligent' enough to cope with the tasks assigned to them. Machine intelligence will continue to improve, but it will fall far short of human intelligence, at least for the foreseeable future. This will reinforce the need for human skills and values to bridge the gap and mitigate the risk posed by powerful artificial intelligence in today's comprehensive and complex human societies. The key to addressing the above risks is to invest and enrich the human factor, but also to monitor artificial intelligence responsibly. In this way, it will be worthwhile to maintain development and societal trust in the technology. Human values are often missing in the moral values of machines with artificial intelligence. To reconcile them, citizens must achieve dominance over both by putting the former (machine values) in the service of the latter (human values). AI should not be used as a scapegoat for human moral failures. Through the "mirror of artificial intelligence", which is a very helpful

7 EU's High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. Brussels: European Commission. https://clck.ru/3CzSbj

8 Ibid.

diagnostic tool for society, people can learn as much as possible about its weaknesses and limitations, as well as about new insights and solutions it offers. The future of artificial intelligence and human society will not be decided for humans, but by humans. AI and the dominance of robots should not decide for humans, but humans must decide what is right and wrong.

The "digital society" has recently become popular in the social sciences and refers to a society characterised by information flowing through global networks at unprecedented speeds. But the most important feature of the digital society is it that recognises these technologies as an embedded part of the larger social entity and acknowledges the incorporation of digital technologies, media and networks into our daily lives (Lupton, 2015a, 2015b), including in the commission of crime, victimisation and justice. Namely Baym (2015) notes that the distinguishing features of digital technologies are the manner in which they have transformed how people engage with one another. This enmeshment of the digital and social has also been referred to as the digitalization of society in which 'technology is society, and society cannot be understood or represented without its technological tools' (Castells, 1996).

On the other hand, Digital criminology refers to the rapidly developing scientific field that applies criminological, social, cultural theory, the theory of technical systems and the corresponding research methods, in the study of crime, delinquent/deviant behavior and justice in the digital society (Stratton et al., 2017). Moreover, it renegotiates criminological theories in search of new scientific ideas that challenge the classical dichotomies – internet vs. physical world, virtual vs. real-both for the prevention and treatment of crimes in the digital environment, on the internet as well as more generally in the context of new technologies, in the context of the development of technoethics. So, in the field of digital criminology the boundaries of modern criminological theory and research are expanded and a broader and ongoing discussion of technology, sociality, crime, deviance and justice is fostered in new conceptual foundations and empirical directions in cyberspace and digital crime mapping.

4. Criminological challenges and perspectives in the "hybrid" world

Although more than fifteen years have passed since the dominance of social networks, the emergence of augmented reality and artificial intelligence, much of criminological research still traditionally focuses on information systems and internet technologies, viewing them either as targets of crime or as mere tools for the commission of otherwise traditional crimes (Hayward & Maas, 2020; Holt & Bossler, 2014). Moreover, many approaches are based on an inherent dualism, where cybercrime continues to be seen as a mirror or online version of its counterparts in the physical world, differing in means of commission and spatial extent, but not in essence and nature (Grabosky, 2001).

4.1. CrAIme terminology and typology

AI-based Cybercrime (Wang, 2020), AI cybercrime (Hoanca & Mock, 2020), AI Crime (further – AIC) (King et al., 2020), "harmful AI" (Hibbard, 2015; Johnson & Verdicchio, 2017), "malevolent AI"[9], malicious Use and abuse of AI (Blauth et al., 2022) and so on are some of the terms one comes across when reading the relevant academic literature and trying to find the position of AI in the criminological milieu.

For the majority of researchers, the use of AI can enable existing forms of crime ("cyber-enabled crime") or establish new forms of crime ("cyber-dependent crime") (Akdemir & Lawless, 2020; Grabosky, 2001). AI potentially enables attacks that are larger in scale and scope than previously possible with other technologies (Blauth, et al., 2022). Therefore, the term "AI-enabled crime" is preferred, as the possibilities exist both in the cybercrime domain (with overlaps with traditional cybersecurity terms) and in the rest of the world (some of these threats emerge as extensions of existing criminal activities, while others may be novel). The term "AI crime" proposed by King et al. (2020) to describe the situation in which AI technologies are repurposed to facilitate criminal acts by focusing on behaviours that are already defined as criminal in the respective legislation, on the other hand, is considered a term that is too limited to create a broad typology which is not limited to acts that constitute a crime in each state. For example, the creation and dissemination of misinformation/ false news may be harmful under certain national laws, but not necessarily a criminal offence. Therefore, the notion of "malicious use and misuse" of AI (King et al., 2020)[10] is seen as a very interesting alternative.

Within this vast range of possibilities, Hoanca & Mock (2020) classify AI cybercrime into three general and loosely overlapping areas: using AI to commit cybercrime online, using AI via new cybercrime channels that reach into physical space, and using AI or knowledge of AI to strike at the core of other AI systems, by corrupting data or algorithms. These are not three separated areas: they largely overlap, and the extent of their overlap will continue to increase. While, Hayward & Maas, (2020) in an attempt expand the criminological paradigm by taking into account the "tech-crime nexus" qualify the use of the term 'criminal uses of AI' and they identify three categories: (1) crimes with AI, (2) crimes on AI, and (3) crimes by AI. According to them, AI falls under

[9] Yampolskiy, R. V. (2016). Taxonomy of pathways to dangerous AI. arXiv:1511.03246v2, 143–148. https://clck.ru/3CzVKL

[10] Ciancaglini, V. (2020). Malicious uses and abuses of artificial intelligence. Trend Micro Research. United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol's European Cybercrime Centre (EC3). https://clck.ru/3CzSmK

the first AIC category, where it can be a powerful instrument for "malicious" criminal use by introducing new threats or altering the intrinsic characteristics of already-existing ones. It is possible for current threats to spread in a physical setting[11]. Attacks that attempt to fool or "hypnotise" AI systems by taking advantage of and reverse-engineering system vulnerabilities fall under the second AIC category of crimes "on" AI. It has long been possible to "poison" the training data used by a system. Famously, after users fed the Microsoft Twitter[12] chatbot "Tay" a slurry of right-wing phrases, the chatbot turned racist within a day [13]. In the third AIC category, "Crimes by AI", the crucial aspect is the thorny issue of the legal status of AI – and its potential misuse as a "criminal shield/facilitator". A typical paradigm of such a case, according to Hayward & Maas (2020), is the case of a group of artists who published a random shopping bot on the dark web in 2015 – with the unsurprising result that it ended up buying drugs and was arrested by the Swiss police[14].

4.2. A Technoethics approach in the case of AI Crime

Efforts to reach an understanding of ethical aspects of different types of technology are challenged by the tendencies within academia to create information groups in separate fields and disciplines. Technoethics thus helps to connect separate knowledge bases around a common theme (technology, in our case AI). It is holistic in nature and provides an umbrella for all subfields of applied ethics that focus on technology-related areas of human activity, including economics, politics, globalisation, health and medicine, and research and development. Technoethics (further – TE) proposes that what should be changed is, strictly speaking, man's view of himself and his view of reality. Here lie the deepest reasons for the failure of the techno-scientific paradigm, which respects neither the nature of human beings nor the nature of beings in general. We must abandon techno-science, which implies the primacy of science over technology, and embrace a new relational paradigm that is gaining ground in postmodernity. Technoethics arose from the demand to stop the tendency inherent in much of technology to separate itself from freedom and instead to affirm technology as a spiritual activity, an outstanding product of the human spirit, and to recognise it as a driver and not as a mere recipient

11 See also Brundage, M., Avin, S., Clark, J. et al. (2018). The malicious use of artificial intelligence. https://clck.ru/3CzSuH

12 The social network blocked in the territory of the Russian Federation for disseminating unlawful information.

13 Gershgorn, D. (2016). Here's how we prevent the next racist chatbot. Popular Science. https://clck.ru/3CzSxm

14 See also Kasperkevic, J. (2015). Swiss police release robot that bought ecstasy online. The Guardian. https://clck.ru/3CzSzB

of theoretical developments in ethics. And one could say that its main contribution is to address new kinds of ethical questions. It is therefore not surprising that many of the current debates about technological progress are taken up by technoethics. They thus inevitably raise important questions about rights, privacy, responsibility and risks that need to be answered appropriately. Moreover, unlike traditional applied ethics, which emphasises ethical concern for living beings, TE is "biotechnocentric".

The scientific debates around AI-enabled future crime is mainly organized into three non-exclusive categories according to the relationship between crime and AI:

– Defeat to AI – e.g., breaking into devices secured by facial recognition.

– AI to prevent crime – e.g., spotting fraudulent trading on financial markets.

– AI to commit crime – e.g., blackmailing people with "deepfake" video (Caldwell et al., 2020).

And despite the fact that Artificial intelligence (AI) research and regulation seek to balance the benefits of innovation against any potential harms and disruption, one unintended consequence of the recent surge in AI research is the potential re-orientation of AI technologies to facilitate criminal acts, AI Crime (i.e. AIC is theoretically feasible thanks to published experiments in automating fraud targeted at social media users, as well as demonstrations of AI-driven manipulation of simulated markets)[15, 16] (Nguyen et al., 2015). The importance of AIC as a distinct phenomenon has not yet been acknowledged. The literature on AI's ethical and social implications focuses on regulating and controlling AI's civil uses and the AIC research that is available is scattered across disciplines, including socio-legal studies, computer science, psychology, and robotics etc. This lack of research focused on AI Crime undermines the scope for projections and solutions in this new area of potential criminal activity committed by AI, concerns the possibility of new crimes in the category of 'white collar crime' (LoPucki, 2017), but also raises questions about the legal personality of AI – as well as concerns about the use of such machines as "facilitators", their criminal liability, namely where the limits of liability models may undermine legal certainty, as it may be the case that agents, whether artificial or not, may engage in criminal acts or omissions without sufficiently matching the conditions of liability for a particular offence to constitute a (specifically) criminal offence (King at al., 2020; Bayern, 2016; Williams, 2017; McAllister, 2018).

[15] Huang, S., Papernot, N., Goodfellow, I., Duan, Y., & Abbeel, P. (2017). Adversarial attacks on neural network policies. arXiv preprint arXiv:1702.02284. https://clck.ru/3CzT6s

[16] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. https://clck.ru/3CzT8m

A tecnoethical approach thus raises critical issues and questions to consider, especially concerns about destabilised concepts. The underlying concept of criminal law that is destabilised is the idea of criminal liability. AI as an "independent" criminal facilitator raises serious questions about basic legal norms such as the voluntarily committed offence (actus reus), criminal intent (mens rea) and various questions about the knowledge threshold. A second concept that seems to be shaken by this is the importance of social control, the idea of democratic values and the limits of the state's protection of human rights: scalable, comprehensive, inescapable surveillance and the potential use of AI and robotics for law enforcement[17] (Zardiashvili et al., 2019), including critical examinations of how to ensure democratic accountability for ML-based predictive policing technologies. The hidden state: ubiquitous yet tacit surveillance, AI drones and "smart-city" sensors creates new forms of "wide surveillance" that are ubiquitous, yet subtle, tacit, and deniable (Hayward & Maas, 2020). The oracle state: from detection and enforcement, to prediction and prevention with AI systems to be able to pick up on subtle patterns to offer (ostensibly) accurate predictions of future behaviour, including criminal conduct (Danaher, 2022).

However, the primary and exclusive focus on cyberspace, with direct and unambiguous reference to the Internet and "virtual or AI" technologies (categories of cybercrime that are easily and unambiguously distinguished from corresponding categories in "non-cyberspace"), also obscures the diverse and embedded nature of digital data and communication in modern societies (Jaishankar, 2008), where drift in the digital environment results from the dynamic intertwining between the characteristics of the technology and its use (Goldsmith & Brewer, 2014); the "desire for representation" of the deviant "virtual" self (Yar, 2012) is closely related to the broader trends of both self-created subjectivity through new communication platforms and artificial intelligence – the ability of machines to think, communicate and make decisions in ways that were previously only possible for humans (networked reality, networked portability and networked matter, etc.)[18].

S. Brown (2006a), in light of all these challenges, proposes a digital criminology that goes beyond the conventional framework and turns instead to "techno-social theories" (Latour, 1993; Lash, 2002; Haraway, 1987, 1991; Castells, 2001) because one feature of digital technologies is the way they have changed the way people interact with each other (Baym, 2015). Significantly, as she notes, analyses of cybercrime seem to be trapped in absolute distinctions between "virtual" and "embodied, real" crime,

[17] Interpol and UNICRI. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://clck.ru/3CzTGP

[18] Institute for the Future (IFTF). (2019). Future of connected living – augmented humans in a networked world: Research Report. https://clck.ru/3CzTPY

with understandings of the "new" cybercrime relying almost exclusively on metaphors and the "translation" of "old" legal and theoretical frameworks (Aas, 2007; Hayward, 2012; Wood, 2016). In criminology, "nowhere is the vision of the criticality of the nature of the world as a human-technical hybrid..." in which all crimes occur in networks that differ only in the degree of virtuality/reality (embodiment) (Brown, 2006b). Consequently, criminologists today must understand crime and criminality at the blurred intersections of biology/technology, nature/society, object/acting subject and artificial/human. Rather than focusing the study of cybercrime on technology as a dissemination tool that has increased criminal opportunities and networks, it is now suggested that "digital/online (criminal) activities are best understood as processes, i.e., phenomena that are in constant dialogue and change with other phenomena/technologies within a human/technological hybrid world" (Brown, 2006a).

Conclusions

The era of divided perspectives and dichotomies may be coming to an end. Perhaps it is now time for synergies, especially at the interdisciplinary level. Why cling to dichotomies when we can harmonise approaches and perspectives? And all this in the context of the "digital society" that recognises technology as part of the wider social entity and accepts the integration of digital technologies, media and networks into people's lives, including the commission of crime, victimisation and justice.

Baym (2015) elaborates on the blurring of boundaries between online and offline realities, noting that the main characteristic of digital technologies is that they have transformed the way people interact with each other in a networked reality, in a world that is now perceived as a human-technological hybrid (Brown, 2006a) where all crimes occur in networks that differ only in the degree of virtuality/embodiment.

Moreover, all issues raised by the use of this technology are not purely technical but concern a wide range of scientific and non-scientific fields, and its safe use cannot be ensured without a multidisciplinary approach.

Artificial Intelligence has enormous potential to be used for social good and achievement of the Sustainable Development Goals. Even as it is being used to help address many of humanity's most critical social issues, its use is also raising concerns about infringement of human rights like the right to freedom of expression, right to privacy, data protection, and non-discrimination. AI-based technologies offer major opportunities if they are developed in respect of universal norms, ethics and standards, and if they are anchored in values based on human rights and sustainable development. For instance, reliable and transparent artificial intelligence can be an effective 'vehicle' for eliminating inequalities in the educational process, as it can be used to create programmes tailored to learning needs and improve the speed of learning.

Moreover, artificial intelligence can also play an important role in the field of justice by creating automated judicial systems, as well as in the field of jurisprudence in general. For example, in the criminal justice field, the use of AI systems for providing investigative assistance and automating decision-making processes is already in place in many judicial systems across the world.

In the context of emerging technoethics, the idea that this unofficial norm, derived from a popular belief, will be the 'touchstone' for characterising online mediated behaviour as deviant/crimninal, is missing - or rather in the process of being formed.

The moral values of machines with artificial intelligence too often lack the broader human values. To reconcile them, citizens must gain dominance over both and put the former (machine values) in the service of the latter (human values). AI should not be used as a scapegoat for human moral failings. Through the "mirror of artificial intelligence", which is a very helpful diagnostic tool for society, people can learn as much as possible about its flaws and limitations, as well as new insights and solutions it offers. The future of artificial intelligence and human society will not be decided for the people, but by the people.

References

Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/intr-10-2019-0400

Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, *7*(1), 297–309. http://dx.doi.org/10.1017/S1867299X00005729

Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.

Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, *10*, 44–65. https://doi.org/10.1515/pjbr-2019-0004

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/access.2022.3191790

Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3407779

Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.

Bunge, M. (1977). Towards a Technoethics. *Monist*, *60*(1), 96–107.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.

Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, *2019*, 31–34. https://doi.org/10.26116/techreg.2019.003

Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, *35*(54), 8. https://doi.org/10.1007/s13347-022-00550-2

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102
Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Greenfield, A. (2017). *Radical Technologies*. London: Verso.
Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538
Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, *17*(2), 1–25. https://doi.org/10.1177/1741659020917434
Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*(3), 441–462. https://doi.org/10.1093/bjc/azs008
Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, *3*(1), 14–27. https://doi.org/10.4018/jte.2012010102
Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209
Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, *27*(2), 55–61. https://doi.org/10.1109/mmul.2020.2994403
Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, *27*(4), 575–590. https://doi.org/10.1007/s11023-017-9417-6
Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
Lash, S. (2002). *Critique of Information*. London: Sage.
Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093
Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, *37*(10), 7108–7119. https://doi.org/10.1016/j.eswa.2010.03.004
Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. https://doi.org/10.1109/iiai-aai.2017.46
LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities. Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
Luppicini, R. (2008). The Emerging Field of Technoethics. In R. Luppicini, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. https://doi.org/10.4018/9781605660226.ch001
Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528
Lupton, D. (2015b). *Digital Sociology*. 1st ed. London & New York: Routledge.
McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, *101*, 2527–2573.

McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, *2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101

Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. https://doi.org/10.1109/isi.2008.4565058

Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.

Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition,* 7–12 June, 427–436. https://doi.org/10.1109/cvpr.2015.7298640

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.

Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's[19] technological unconscious. *Theoretical Criminology*, *21*(2), 1–18. https://doi.org/10.1177/1362480616643382

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, *2*(4), 179–185. https://doi.org/10.21552/delphi/2019/4/7

[19] The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation

Author information

Fotios Spyropoulos – PostDoc, PhD, Associate Professor of Criminal Law & Criminology, Faculty of Law, Philips University; Senior Partner of Spyropoulos Law Firm
Address: 4-6 Lamias Street, 2001, P.O. Box 28008, Nicosia, Cyprus; Alexandras Avenue 81, 11474, Athens, Greece
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 30, 2024
Date of approval – April 15, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024

Научная статья
УДК 34:004:349.2:004.8
EDN: https://elibrary.ru/mqtnqg
DOI: https://doi.org/10.21202/jdtl.2024.32

Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии

Фотиос Спайропулос

Университет Филипс, Никосия, Кипр
Spyropoulos Law Firm, Афины, Греция

Ключевые слова

искусственный интеллект,
киберпреступность,
право,
преступление,
преступность,
техноэтика,
цифровая криминология,
цифровое общество,
цифровые технологии,
этика

Аннотация

Цель: опираясь на современные научные подходы к «цифровому обществу» и новые подходы в криминологии, выявить и определить цифровую криминологию, направленную на изучение возможных способов использования искусственного интеллекта преступниками, в том числе в рамках так называемой ИИ-преступности.

Методы: проблемы связи искусственного интеллекта с преступностью в «гибридном мире» переосмысливаются в статье преимущественно с учетом междисциплинарности, на уровне которой аргументы подкрепляются соответствующими отсылками к «цифровой криминологии» и ее небинарному образу мышления в рамках технософиального подхода, несистематического обзора литературы.

Результаты: в исследовании отмечается, что в цифровом обществе технологии интегрируются в жизнь людей, включая сферы преступности, виктимизации и правосудия, стирая границы между онлайн- и офлайн-реальностью, создавая гибридный мир человека и технологий, где преступления происходят в виртуальных сетях. Показано, что искусственный интеллект обладает потенциалом для достижения целей социального благополучия и устойчивого развития, однако необходимо учитывать риски, связанные с нарушением прав человека. Обосновывается необходимость междисциплинарного подхода для обеспечения безопасного использования технологий, борьбы с неравенством в сфере образования, помощи в осуществлении правосудия и распознавании девиантного или преступного поведения в сети. Подчеркивается, что в контексте зарождающейся техноэтики пока отсутствует или, скорее, находится в процессе формирования идея о том, что эта неофициальная норма, основанная на обыденных представлениях, станет «опорным камнем» для характеристики опосредованного онлайн-поведения как девиантного или преступного.

Научная новизна: в статье с точки зрения техноэтики выдвигается ряд подходов к феномену использования информационно-коммуникационных технологий в преступных целях под влиянием искусственного интеллекта. При этом отмечены социальные вызовы, возникающие в результате технологических сбоев (например, прогнозирование и предотвращение преступлений путем трансформации деятельности органов охраны правопорядка, усиления наблюдения и практики уголовного правосудия) в «цифровом обществе».

Практическая значимость: идеи, лежащие в основе данного исследования, могут быть использованы при разработке предложений по внесению изменений и дополнений в действующее уголовное законодательство, а также в педагогической деятельности, особенно при реализации образовательных курсов или модулей по проблемам преступности в контексте цифровой трансформации общества.

Для цитирования

Спайропулос, Ф. (2024). Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии. *Journal of Digital Technologies and Law*, *2*(3), 636–656. https://doi.org/10.21202/jdtl.2024.32

Список литературы

Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/intr-10-2019-0400

Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, *7*(1), 297–309. http://dx.doi.org/10.1017/S1867299X00005729

Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.

Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, *10*, 44–65. https://doi.org/10.1515/pjbr-2019-0004

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/access.2022.3191790

Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3407779

Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.

Bunge, M. (1977). Towards a Technoethics. *Monist*, *60*(1), 96–107.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.

Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, *2019*, 31–34. https://doi.org/10.26116/techreg.2019.003

Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, *35*(54), 8. https://doi.org/10.1007/s13347-022-00550-2

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102
Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Greenfield, A. (2017). *Radical Technologies*. London: Verso.
Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538
Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, *17*(2), 1–25. https://doi.org/10.1177/1741659020917434
Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*(3), 441–462. https://doi.org/10.1093/bjc/azs008
Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, *3*(1), 14–27. https://doi.org/10.4018/jte.2012010102
Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209
Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, *27*(2), 55–61. https://doi.org/10.1109/mmul.2020.2994403
Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, *27*(4), 575–590. https://doi.org/10.1007/s11023-017-9417-6
Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
Lash, S. (2002). *Critique of Information*. London: Sage.
Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093
Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, *37*(10), 7108–7119. https://doi.org/10.1016/j.eswa.2010.03.004
Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. https://doi.org/10.1109/iiai-aai.2017.46
LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities. Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
Luppicini, R. (2008). The Emerging Field of Technoethics. In R. Luppicini, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. https://doi.org/10.4018/9781605660226.ch001
Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528
Lupton, D. (2015b). *Digital Sociology*. 1st ed. London & New York: Routledge.
McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, *101*, 2527–2573.
McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, *2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101

Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. https://doi.org/10.1109/isi.2008.4565058

Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.

Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition,* 7–12 June, 427–436. https://doi.org/10.1109/cvpr.2015.7298640

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.

Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's[1] technological unconscious. *Theoretical Criminology*, *21*(2), 1–18. https://doi.org/10.1177/1362480616643382

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, *2*(4), 179–185. https://doi.org/10.21552/delphi/2019/4/7

[1] Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Сведения об авторе

Фотиос Спиропулос – научный сотрудник, PhD, доцент в области уголовного права и криминалистики, факультет права, Университет Филипс; старший партнер юридической компании Spyropoulos Law Firm
Адрес: Кипр, 28008, г. Никосия, ул. Ламиас, 4-6; Греция, 11474, г. Афины, Александрас авеню, 81
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.81 / Криминология
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 30 апреля 2024 г.
Дата одобрения после рецензирования – 15 мая 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.