Research article
DOI: https://doi.org/10.21202/jdtl.2023.9

Digital Trends of Criminology and Criminal Justice of the 21st Century

Mehrdad Rayejian Asli

Institute for Research and Development in the Humanities (SAMT)
Tehran, Iran

Keywords

Cyber criminology,
cyber victimology,
cyber space,
criminology,
criminal law,
criminal justice,
digitalization,
digital technologies,
risk

Abstract

Objective: to define the key trends in the development of criminology and criminal justice under significant broadening of digitalization and using modern technologies.

Methods: the priority of analytical method combined with descriptive method provided an optimal set of tools for searching and revealing the main digital trends in the development of criminology and criminal justice in the 21st century.

Results: the growing dependence was revealed between criminal-legal science and digital technologies, which leads to the change in essence and types of contemporary criminality, models of criminals' behavior, methods and mechanism of crime control and prevention in the light of requirements of criminal policy and justice. The dual role of the global digitalization trend is highlighted, the achievements of which are used both by the agencies of criminal justice system (in particular, for crime control, management and prevention) and criminals when implementing their criminal intents. It was determined that the essential transformation of criminology and criminal justice is largely caused by a dramatic development of digitalization in the 21st century, as well as by the modern technologies created on its basis, which appear to be more effective than the standard methods of traditional criminology, including quantitative and qualitative estimations, observation, interviews, polls, etc.

Scientific novelty: new spheres of criminal-legal knowledge are introduced, as well as the corresponding disciplines formed exclusively under the influence of digitalization, such as cyber criminology and cyber victimology; algorithmic (computational) criminology, based on actuarial justice and the theory of risks, is highlighted as the most recent trend in criminological science.

Practical significance: the account of trends and positive experience gained in the sphere of digitalization determines the successful solution of the tasks associated with crime counteraction, transformation of approaches to the content, goals and methodology of applied criminology and criminal justice. The global megatrend of digitalization essentially changes the appearance of the criminal-legal science, sets the new theoretical and applied directions of its development. Timely upgrade and adaptation of knowledge, skills and capabilities in compliance with the achievements of digitalization will allow criminology and criminal justice to correspond to the tasks of the new millennium.

For citation

Rayejian Asli, M. (2023). Digital Trends of Criminology and Criminal Justice of the 21st Century. *Journal of Digital Technologies and Law, 1*(1), 235–250. https://doi.org/10.21202/jdtl.2023.9

Content

Introduction

Digitalization is defined as “integration of digital technologies into everyday life by the digitization of everything that can be digitized” (Ochs & Reinmann, 2018). It is also defined as the adoption of digital technologies to modify a work in order to creating a value by using new, advanced technologies, and by exploiting digital network dynamics and the giant digital flow of information (Scuotto et al., 2019, Cho et al., 2021, Moneva et al., 2022, Khan et al., 2020, van de Weijer & Moneva 2022, Sampson, 2014). Digitalization can be realized in the form of the process of transforming something to digital as if it may arise by using digital technologies to upgrade processes (Cabada García et al., 2022; Abubotain & Chamakiotis, 2020, Lallie at al., 2021, Okutan & Çebi, Y., 2019, Solak & Topaloglu, 2015).

Considering the above definitions, digitalization can be applied in many branches of sciences, including, inter alia, humanities and social sciences. Meanwhile, criminal sciences are among human and social sciences through which digitalization can contribute a significant role. Two major fields of study in criminal sciences are criminology and criminal justice that have been influenced by digitalization and technologies in recent decades.

Since the decades of 80 and 90, new attitudes and theories emerged within the area of criminology in the light the development of social sciences and critical theories which had already led to critical criminology and other contemporary trends in this academic discipline. In the beginning of the twenty first century, criminology and criminal justice were evolved in the light of digitalization and technologies, specifically computer science. Consequently, a number of trends and even, sub disciplines in criminology and criminal justice have emerged. Among these new trends, three examples are explored in this article. These are as follows: Risk management theory and actuarial justice that emerged in the late decades of twenty century, cyber criminology and victimology, and also algorithmic or computational criminology that have come out in the recent two decades of third millennium.

In a broad sense and under the scope of mentioned-above definitions, the role and status of digitalization in criminology and criminal justice is understood by concepts and theories that their origins are traced back into the development of criminology. The author seeks to find and introduce the most significant samples and manifestations of the concepts and theories that could demonstrate the digitalization of these two important fields of study in criminal sciences with an emphasizing on the developments of the two first decades of 21st century. Accordingly, the present article consists of three main parts. First, the risk management, as a criminological theory that is linked to actuarial justice, will be explored in the context of digitalization. Second, cyber criminology and victimology, as two new subdsciplines of criminal sciences, will be examined in the light of computer science. Third, algorithmic or computational criminology will be surveyed as a recent development of criminology and criminal justice in the last two decades of the third millennium.

1. The Theory of Risk in the Context of Digitalization

Risk is an important key term that arises in several areas of criminology, including the function of criminal justice system, models of crime prevention, and criminal etiology based on rationale choice theory (O’Malley, 2009). Before risk becomes a central issue in criminal justice studies, it was addressed by classical criminologists in rational choice perspective of criminal behavior. The perspective presumes that criminal behavior is an advantage for offenders, and indeed, derived from their decisions based upon the free will. However, the theory, it has been argued, is applicable in certain types of crimes named utilitarian offences in which criminal behavior is committed for gain or profit. (McLaughlin & Muncie, 2019).

1.1. Administrative Criminology in the Light of Crime Prevention Requirements

Irrespective of the applicability of rational choice theory to certain types of crime, it is used as an explanation for a situational or opportunity-based prevention of crime. This type of crime prevention model became an element of 'administrative criminology' since 80s. It is defined as a trend in criminology that focused on enhancing the efficiency of the criminal justice system, particularly through situational or opportunity-based crime prevention (Halder, 2021). By utilizing the assumption that the offenders are rational actors who act based on a calculation, administrative criminology focuses on crime as an event in which the roles of offender, victim, and other circumstances are the components of criminal behavior (McLaughlin & Muncie, 2019). According to theoretical and applied dimensions of criminology and criminal justice, administrative criminology was based on an etiological perspective called as 'criminology of the criminal behavior' that is rooted in European (esp. French) approach to the study of crime and criminality. As Raymond Gassin, French criminologist, argues, la criminologie de l'acte (criminology of the criminal behavior) includes le passage à l' acte (the acting out theory) that explains criminal behavior as a process through which the behavior is formed from intention to act (Gassin, 1990). Thus, the theory accounts for criminal calculation that is an essential element in administrative criminology. Criminal calculation presumes that the offender acts based on a rational assessment. It requires a series of technical-technological measures and instruments to control and prevent crime and criminality. They form the model of situational or opportunity-based prevention which includes measures and techniques like CCTV and security alarms.

By introducing administrative criminology as a new trend in crime etiology and criminal policies, criminological studies and research have shifted to risk assessment of criminal justice system.

1.2. Risk Management and Actuarial Justice in the Light of Considerations of Recidivism

Early references to risk assessment have a critical attitude to clinical prediction and its use in forensics. At the same time, they addressed at risk factors from an ethological perspective (Pritchard et al., 2014). Today, risk assessment is redefined in the framework of actuarial justice. Actuarial justice is a criminological approach which is derived from actuaries. It denotes the software in computing (McLaughlin & Muncie, 2019), and is a theoretical model that employs concepts and methods similar to actuarial mathematics (Bosworth, 2005).

The prevalence of this model in criminal justice has been influenced by actuarial statistical modeling of risks, e.g. in the insurance industry (Metcalf, 2004). In criminology and criminal justice, actuarial justice means calculation techniques that forms the basis for criminal policies, particularly in the area of corrections and prison system. Thus, it is one of the models of criminal justice upon which rehabilitation, as a mechanisms of criminal sanctions, is redefined by the probabilistic calculations and statistical distributions for management of penal population, esp. within the prison system. In the light of this approach, management of the criminals are carried out based on the risk assessment technologies and practices (McLaughlin & Muncie, 2019). As a case study, measures and policies such as probation service, are a typical instance through which the risk management is applied to recidivism of dangerous criminals like sex offenders. For example, today, the United States courts use computer software to predict the possibility of repetition of crime in future. The results of this method are incorporated into sentencing decisions as well as into the prison system. Considering the variables of accuracy and fairness, critics argue that computer software may be racially biased, particularly in favor of white defendants over black ones (Dressel & Farid, 2018).

At a preventive level, by focusing on the situational or opportunity-based prevention of crime, risk management is linked to crime reduction (McLaughlin & Muncie, 2019) that refers to techniques and strategies for reducing the possibility of crime commission regarding its setting and circumstances. As Feeley, one of the founders of new penology, argues (Feeley, 2004), "Actuarial justice attempts to predict the future criminal behavior of a person currently being adjudicated in the criminal justice system, and then to implement policies toward that person that will reduce his/her ability to commit future crimes". The United States, as a typical case, has experienced various risk assessment measures based on actuarial justice. One of the significant methods of risk assessment which is used in this county is Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). Since 1998, it has been used to assess over one million individuals in the criminal justice system. It employs the recidivism prediction component of COMPA (the Recidivism Risk Scale) since 2000. As computer software, it predicts the risk of committing a crime by a person within two years of assessment from an individual's demographics and criminal record (Dressel & Farid, 2021). The risk assessment model has led to conceptualize 'prediction of crime' as a key term in criminology and criminal justice. Prediction of crime refers to the recidivism (repetition of crime) that contributes a significant role in crime control and policies. By using the measures and techniques of prediction of crime, more appropriate and accurate consequences could be expected from criminal justice policies.

Today, scholars acknowledge that the risk management and risk assessment instruments in prevention and prediction of crime should receive more attention from legal and judicial authorities[1]. Thus, it could be said that creating a jurisprudence of risk for judges and other related criminal justice agencies (e.g. prosecution services) seems necessary.

[1] *A Primer on Risk Assessmsnt Instruments for Legal Decision-Makers. Vandebilt Law School*. https://law.vanderbilt.edu/academics/academic-programs/criminal-justice-program/Primer_on_Risk_Assessment.pdf

2. Cyber Criminology and Victimology

The widespread use of technology and internet in the modern world, esp. in the third millennium, has made its criminal aspects an essential priority for all societies. One major aspect of technology and internet is cyber crime and victimization. This issue has attracted the criminologists' attention during the recent decades. Cyber criminology and victimology are considered as the achievements of this attention.

2.1. The Emergence of Cyber Criminology as an Explanation for the Etiology of Cyber-Crime

Cyber criminology is almost a new interdisciplinary field of study in criminal sciences that combines coursework in criminal justice and computer science to explore the growing problem of computer crime. With regard to the increasing developments in technology and science, crime and criminal behavior have consequently been changed. Therefore, redefinition of crime theories and typologies based upon these developments and changes seems inevitable. It means that cyber crime and criminals evolve over time as they learn from actions and experiences, and enhance their skills (Jahankhani, 2018). Cyber crime is defined as any criminal activity by using the technology and digitalization. They consist of illegally acts and actions, including to access to information, to intercept or damage data, to interfere with a computer system or device, and so on. They are usually divided into information-related crime and computer-network crime. Cyber criminology makes it possible to learn how computers may be used as a criminal tool and how crimes are committed by using the computer. As some authors have pointed out, "the seamless nature of the internet and the crimes being committed through its use has brought about a dire need to analyse cybercrimes differently from other crimes" (Maheshwari, 2021).

From a historical viewpoint, since the 1990s, criminologists have paid their attention to this issue that cyberspace has made as a new spot for crime and criminals. It has challenged the paradigm of mainstream criminology, which failed to explain new forms of deviance, crime, and social control within the cyberspace. As Jaishankar, a founder of cyber criminology, argues (Jaishankar, 2007), "criminology has been remiss in its research into the phenomena of cyber crime and has been slow to recognize the importance of cyberspace in changing the nature and scope of offending and victimization". He introduces cyber criminology as a radical discipline to explain and analyze the crimes in the internet. As an interdisciplinary field of study, cyber criminology is an area of study and research at the interface between computer or internet science and criminology. Jaishankar defines cyber criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007). In a book entitled "Cyber Criminology Exploring Internet Crimes and Criminal Behavior", edited by Jaishankar, he explains why did he academically coin the term ‘cyber criminology’ as an independent discipline to study and explore cyber crimes from a social science perspective, and the body of knowledge for dealing with cyber crimes that should be distinguished with cyber forensics (Jaishankar, 2011). As a pioneer of cyber criminology, Jaishankar developed the space transition theory to explain the causation of crimes in cyberspace (Jaishankar, 2011). According to this theory, the movement of persons from physical space to cyberspace and vice versa varies. In other words, people act or conduct differently when they move from physical space to cyberspace (Jaishankar, 2007).

Regarding the place of cyber criminology in the discourse of social and criminal science, some scholars have acknowledged that “Although cyber criminology is an evolving field of criminology which has not so far received adequate attention from mainstream criminology, the future holds great prospect for the new discipline. As virtual communities and electronic tribes proliferate the cyberspace and crime/disorder escalate, the discipline of cyber criminology will gain momentum and attention. It will remain active in the search for answers to the fundamental questions of the contexts and causes of crime and disorder in the cyberspace as well as the quest for social order” (Ndubuez, 2019).

2.2. The Necessity of a Cyber Victimology to Respond Cyber-Crime and Victimization

Alongside the development of cyber criminology, the necessity of a socio-legal perspective on victimization in the cyberspace area yields the emergence of a parallel field of study named ‘cyber victimology’. This term was coined by K. Jaishankar and Debarati Halder, Indian criminologists/victimologists, to study and research in victimization online in order to present practical solutions for the problem (Jaishankar, 2020; Halder, 2022).

In his chapter ‘Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology’, Jaishankar writes: “Notably, some scholars do not perceive cyber crime victimization as a new form of victimization and some do not holistically group them. Invariably, many countries are dealing with cyber crime victimization through their conventional laws, without creating specific laws. These kinds of new issues have paved way to study the cyber victimization from different perspectives. I emphasize the need to have a sub-discipline of Victimology i.e., Cyber Victimology to examine cyber crimes purely from victims’ /victimization perspective, as I believe cyber crime victimization is a new form of victimization. This chapter will dwell on the establishment of the new field of Victimology, which is referred to as Cyber Victimology” (Jaishankar, 2020).

As Jaishankar argues, cyber crime’s victimization is a new type of victimization (Jaishankar, 2020). The common ground of cyber criminology and victimology is to explore the dimensions of cyber criminal victimization. His Indian colleague, Halder, also argues that the characteristics of different groups of victims have developed a profile of cyber-crime victims. One of the most important findings of cyber victimology is to find out the effects of cyber crimes on different parts of the society. In other words, even individual cyber victimization can entail a greater harm to other member of society (Halder, 2022).

Regarding the issues of digitalization and technology, cyber criminology and victimology attract our attention to the internet and cyberspace that have changed and transformed the lifestyle and routine activities of millions of peoples. Meanwhile, these new sub-disciplines of social and criminal sciences point out that internet and technologies as the manifestations of modern world are prone to be misused (Jaishankar, 2020). In other words, internet and cyberspace can play a converse role by providing a setting for offenders and opportunities for their criminal activities. Considering several forms and functions of technologies relating to internet and cyberspace, crimes and criminal activities occurred in or by them are used by many various terms and phrases, inter alia, including computer crime, computer- related crime, digital crime, information technology crime, Internet crime, virtual crime, e-crime, and net-crime (Jaishankar, 2020).

Thus, internet and modern technologies play an undeniable role in cybersecurity and protection of this space[2]. Yet, criminological-victimological perspective should not be ignored in this regard, because these technologies may bring about criminal opportunities and online and offline victimization.

3. Algorithmic or Computational Criminology

The third orientation of digitalization of criminology that is introduced in this article has been influenced by mathematics and computer science. Algorithmic criminology and computational criminology are synonymous terms for this new sub-discipline that is a bridge between criminology and computer science. It also encompasses applied mathematics as computer-intensive simulations of criminal behavior (Berk, 2013). In the light of mathematics and computer science, criminological theories are animated to explain crime and law enforcement. Meanwhile, statistics can play a significant role in computational criminology. In addition to actuarial justice based on risk management/assessment theory, computational criminology is applicable in law enforcement and criminal justice system. It is also used in modeling and simulating criminal events like terrorism and cyber crimes in a complex setting. Computational criminology is applied by using computational topology and algorithms that provide information about crime pattern theory (Brantingham, 2011). It addresses criminological problems by using applied mathematics, computer science and criminology. The applicable methods in this area include algorithms, data mining, data structures and software development (Harris, 2014).

[2] *Don't Forget Victimology as a Cybersecurity Strategy.* https://www.secureworks.com/blog/dont-forget-victimology-as-a-cybersecurity-strategy

Alongside all these uses and applicability, the necessity of empirical research in criminology due to criminal etiology for study and research about causes of crime requires an algorithmic approach, specifically in order to prediction of crime. This concept is linked to recidivism which is one of the important issues in criminological discussions and theories. Preventing recidivism is a major goal of criminal sanctions or sentencing mechanisms such as probation and parole. These mechanisms are related to risk assessment variable in criminology that were discussed before. They require that the possibility of recidivism and the eligibility of offenders for receiving theses programs could be accurately examined and evaluated. The prediction of crime arises within these examination and evaluation processes by using forecasting exercises based upon algorithmic methods which are more impressive and effective, in comparison with conventional research methods in mainstream criminology, i.e. quantitative and qualitative data (observation, interview, questionnaire …).

Overall, crime and criminality follow laws and rules similar to those in non-criminal behavior (Brantingham, 2011). Therefore, a precise understanding these laws and rules depends on the use of modern methods and mechanisms like algorithmic and computational criminology.

Conclusions

Modern technologies, internet and cyberspace have changed the nature, types and circumstances of crime and criminals as well as the instruments of managing and controlling them. The new forms of criminality (e.g. cyber-crime) impose more serious threat and danger to all sectors of societies. This reality has a significant influence on the technologies of control and prevention of crime, so that these technologies have been transformed into the newfound forms of crime. Regarding these changes and developments in the third millennium, criminology needs making radical changes in its content, goals, and particularly in its methodologies in order to resolve, handle and respond to the crime and criminality issues and problems. Accordingly, criminology needs to be upgraded in the form of various disciplines and sub-disciplines in a manner conforming with the crimes of the millennium. The third areas of criminology and criminal justice that were discussed in this article have interactional relations and influences with each other. The common element of this interaction is the digitalization that has signified the emergence of contemporary areas of criminology in recent decades. From an interactional viewpoint, the risk management and risk assessment mechanisms in the light of actuarial justice requires the use and deployment of algorithmic or computational criminology. Moreover, cyber criminology and victimology, as another new trend in this major discipline of criminal sciences, have come out as a result of necessities and concerns of computer science and cyberspace in relation to cyber-crime, cyber-criminals, and cyber-victims.

References

Abubotain, F., & Chamakiotis, P. (2020). FinTech in the Saudi Context. *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*, 188–208. https://doi.org/10.4018/978-1-5225-9550-2.ch009

Berk, R. (2013). Algorithmic criminology. *Security Informatics*, *2*(1). https://doi.org/10.1186/2190-8532-2-5

Bosworth, M. (2005). Actuarial justice. In *Encyclopedia of prisons & correctional facilities* (Vol. 1, pp. 12–14). SAGE Publications, Inc. https://dx.doi.org/10.4135/9781412952514.n5

Brantingham, P. L. (2011). Computational Criminology. *2011 European Intelligence and Security Informatics Conference*. https://doi.org/10.1109/eisic.2011.79

Cabada García, M. J., Quezada Ramírez, S. I., Negrete Gómez, G. A., Villarreal Serrano, E., Colín García, D. L., Villar Cantón, C., Baca Luna, A., Díaz Villanueva, P. D., & Segura-Azuara, N. D. (2022). Social Media Campaign as a Tool for Patient Education of Disease Prevention and Health Promotion: Digital Health Campaign on Osteoporosis Knowledge. In M. Lopez (Ed.), *Advancing Health Education With Telemedicine* (pp. 183–208). IGI Global. https://doi.org/10.4018/978-1-7998-8783-6.ch010

Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*, *121*, 105840. https://doi.org/10.1016/j.childyouth.2020.105840

Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, *4*(1). https://doi.org/10.1126/sciadv.aao5580

Dressel, J., & Farid, H. (2021). The Dangers of Risk Prediction in the Criminal Justice System. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. https://doi.org/10.21428/2c646de5.f5896f9f

Feeley, Malcolm M. (2004). Actuarial justice and the modern state. *Punishment, Places and Perpetrators*, 78–93. https://doi.org/10.4324/9781843924760

Gassin R. (1990). *Criminologie*. Paris: Dalloz.

Halder, D. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimisation* (1st ed.). Routledge.

Harris, P. (2014). *Computational Analysis and Public Policy of Criminology* (First). Koros Press Limited.

Jahankhani, Hamid (2018). *Cyber Criminology*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-97181-0

Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *CERN European Organization for Nuclear Research – Zenodo*. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, *1*, 7–9. https://doi.org/10.5281/zenodo.18792

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press: Taylor & Francis Group.

Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In *An International Perspective on Contemporary Developments in Victimology* (pp. 3–19). https://doi.org/10.1007/978-3-030-41622-5_1

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, *148*, 105837. https://doi.org/10.1016/j.aap.2020.105837

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Maheshwari, R. (2021). Changing Paradigms of Victimization in Cybercrimes: An Analysis, *International Journal of Law Management & Humanities*, *4*(3), 2871–2883.

McLaughlin, E., & Muncie, J. (2019). *The Sage Dictionary of Criminology*. Sage: EBooks.

Metcalf, C. (2004). Managing Risk and the Causes of Crime. *Criminal Justice Matters*, *55*(1), 8–42. https://doi.org/10.1080/09627250408553585

Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, *126*, 106984. https://doi.org/10.1016/j.chb.2021.106984

Ndubuez, P. N. (2019). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace, *The Nigerian Journal of Sociology and Anthropology*, *14*(1), 32–48.

O'Malley, Pat (2009). Risk and Criminology. *Legal Studies Research Paper*, *9*(87), 1–29.

Ochs, T., & Riemann, U. A. (2018). IT Strategy Follows Digitalization. *Encyclopedia of Information Science and Technology* (4th ed., pp. 873–887). https://doi.org/10.4018/978-1-5225-2255-3.ch075

Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, *158*, 287–294. https://doi.org/10.1016/j.procs.2019.09.054

Pritchard, A. A., Blanchard, A. J. E., & Douglas, K. S. (2014). Risk Assessment. *Criminology*. https://doi.org/10.1093/obo/9780195396607-0095

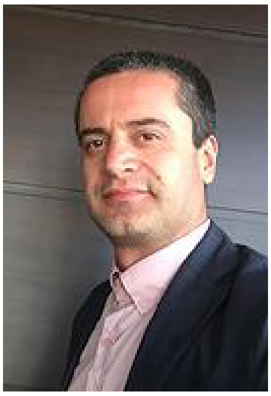
Sampson, F. (2014). Cyberspace. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 1–10. https://doi.org/10.1016/b978-0-12-800743-3.00001-3

Scuotto, V., Serravalle, F., Murray, A., & Viassone, M. (2019). The Shift Towards a Digital Business Model. *Women Entrepreneurs and Strategic Decision Making in the Global Economy*, 120–143. https://doi.org/10.4018/978-1-5225-7479-8.ch007

Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences*, *182*, 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787

van de Weijer, S. G., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, *8*, 100249. https://doi.org/10.1016/j.chbr.2022.100249

Author information



Mehrdad Rayejian Asli – Assistant Professor of Institution for Research and Development in the Humanities (SAMT); Deputy of Research in the UNESCO Chair for Human Rights, Peace and Democracy, Tehran, Iran
Address: 1463645851, SAMT Organization, Al-e-Ahmad Highway, Yadegar Bridge, Tehran, Iran.
E-mail: m.rayejian@samt.ac.ir
ORCID ID: https://orcid.org/0000-0003-0693-1888
Web of Science Researcher ID:
https://www.researchgate.net/profile/Mehrdad-Rayejian-Asli
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57195374005
Google Scholar ID: https://scholar.google.com/citations?user=WKgazNEAAAAJ&hl=en

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – December 13, 2022
Date of approval – January 18, 2023
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023

Научная статья
УДК 343.2/.7:343.9:004
EDN: https://elibrary.ru/zmirlt
DOI: https://doi.org/10.21202/jdtl.2023.9

Цифровые тренды криминологии и уголовного правосудия XXI века

Мехрдад Райеджиан Асли

Институт исследования и развития гуманитарных дисциплин
г. Тегеран, Исламская Республика Иран

Ключевые слова

Алгоритмическая криминология,
кибервиктимология,
киберкриминология,
киберпространство,
криминология,
риск,
уголовное право,
уголовное правосудие,
цифровизация,
цифровые технологии

Аннотация

Цель: определение ключевых трендов развития криминологии и уголовного правосудия в условиях значительного расширения цифровизации и применения современных технологий.

Методы: приоритет аналитического метода в его сочетании с описательным методом обеспечили оптимальный инструментарий для поиска и выявления основных цифровых трендов развития криминологии и уголовного правосудия в XXI веке.

Результаты: выявлена возрастающая зависимость уголовно-правовой науки от развития цифровых технологий, которая приводит к изменению сущности и типов современной преступности, моделей поведения преступников, методов и механизмов контроля и предотвращения преступности в свете требований уголовной политики и уголовного правосудия. Подчеркивается двоякая роль глобального тренда цифровизации, достижения которой используются как органами системы уголовного правосудия (в частности, для контроля, управления и предотвращения преступности), так и преступниками – при осуществлении своих преступных замыслов. Установлено, что существенная трансформация криминологии и уголовного правосудия вызвана в значительной степени резким развитием в XXI веке цифровизации и созданных на ее основе современных технологий, являющихся более эффективными, чем обычные методы традиционной криминологии, такие как количественные и качественные оценки, наблюдения, интервью, опросы и др.

Научная новизна: вводятся новые области уголовно-правового знания и соответствующие им дисциплины, образованные исключительно под влиянием цифровизации, такие как киберкриминология и кибервиктимология; в качестве новейшего направления криминологической науки выделяется алгоритмическая (вычислительная) криминология, основанная на страховом праве и теории рисков.

Практическая значимость: учет трендов и положительного опыта, полученного в области цифровизации, обусловливает успешное решение задач, связанных с противодействием преступности, трансформацию подходов к содержанию, целям и методологии прикладной криминологии и уголовного правосудия. Глобальный мегатренд цифровизации существенно меняет облик уголовно-правовой науки, задает новые теоретические и прикладные направления ее развития. Своевременное обновление и адаптирование знаний, умений и навыков согласно достижениям цифровизации позволит криминологии и уголовному правосудию соответствовать задачам нового тысячелетия.

Для цитирования

Райеджиан Асли, М. (2023). Цифровые тренды криминологии и уголовного правосудия XXI века. *Journal of Digital Technologies and Law*, *1*(1), 235–250. https://doi.org/10.21202/jdtl.2023.9

Список литературы

Abubotain, F., & Chamakiotis, P. (2020). FinTech in the Saudi Context. *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*, 188–208. https://doi.org/10.4018/978-1-5225-9550-2.ch009

Berk, R. (2013). Algorithmic criminology. *Security Informatics*, *2*(1). https://doi.org/10.1186/2190-8532-2-5

Bosworth, M. (2005). Actuarial justice. In *Encyclopedia of prisons & correctional facilities* (Vol. 1, pp. 12–14). SAGE Publications, Inc. https://dx.doi.org/10.4135/9781412952514.n5

Brantingham, P. L. (2011). Computational Criminology. *2011 European Intelligence and Security Informatics Conference*. https://doi.org/10.1109/eisic.2011.79

Cabada García, M. J., Quezada Ramírez, S. I., Negrete Gómez, G. A., Villarreal Serrano, E., Colín García, D. L., Villar Cantón, C., Baca Luna, A., Díaz Villanueva, P. D., & Segura-Azuara, N. D. (2022). Social Media Campaign as a Tool for Patient Education of Disease Prevention and Health Promotion: Digital Health Campaign on Osteoporosis Knowledge. In M. Lopez (Ed.), *Advancing Health Education With Telemedicine* (pp. 183–208). IGI Global. https://doi.org/10.4018/978-1-7998-8783-6.ch010

Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*, *121*, 105840. https://doi.org/10.1016/j.childyouth.2020.105840

Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, *4*(1). https://doi.org/10.1126/sciadv.aao5580

Dressel, J., & Farid, H. (2021). The Dangers of Risk Prediction in the Criminal Justice System. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. https://doi.org/10.21428/2c646de5.f5896f9f

Feeley, Malcolm M. (2004). Actuarial justice and the modern state. *Punishment, Places and Perpetrators*, 78–93. https://doi.org/10.4324/9781843924760

Gassin R. (1990). *Criminologie*. Paris: Dalloz.

Halder, D. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimisation* (1st ed.). Routledge.

Harris, P. (2014). *Computational Analysis and Public Policy of Criminology* (First). Koros Press Limited.

Jahankhani, Hamid (2018). *Cyber Criminology*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-97181-0

Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *CERN European Organization for Nuclear Research – Zenodo*. https://doi.org/10.5281/zenodo.18276

Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, *1*, 7–9. https://doi.org/10.5281/zenodo.18792

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press: Taylor & Francis Group.

Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. *An International Perspective on Contemporary Developments in Victimology*, 3–19. https://doi.org/10.1007/978-3-030-41622-5_1

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, *148*, 105837. https://doi.org/10.1016/j.aap.2020.105837

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Maheshwari, R. (2021). Changing Paradigms of Victimization in Cybercrimes: An Analysis, *International Journal of Law Management & Humanities*, *4*(3), 2871–2883.

McLaughlin, E., & Muncie, J. (2019). *The Sage Dictionary of Criminology*. Sage: EBooks.

Metcalf, C. (2004). Managing Risk and the Causes of Crime. *Criminal Justice Matters*, *55*(1), 8–42. https://doi.org/10.1080/09627250408553585

Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, *126*, 106984. https://doi.org/10.1016/j.chb.2021.106984

Ndubuez, P. N. (2019). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace, *The Nigerian Journal of Sociology and Anthropology*, *14*(1), 32–48.

O'Malley, Pat (2009). Risk and Criminology. *Legal Studies Research Paper*, *9*(87), 1–29.

Ochs, T., & Riemann, U. A. (2018). IT Strategy Follows Digitalization. *Encyclopedia of Information Science and Technology* (4th ed., pp. 873–887). https://doi.org/10.4018/978-1-5225-2255-3.ch075

Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, *158*, 287–294. https://doi.org/10.1016/j.procs.2019.09.054

Pritchard, A. A., Blanchard, A. J. E., & Douglas, K. S. (2014). Risk Assessment. *Criminology*. https://doi.org/10.1093/obo/9780195396607-0095

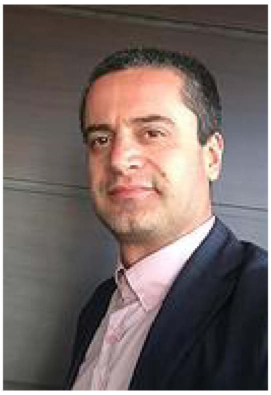
Sampson, F. (2014). Cyberspace. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 1–10. https://doi.org/10.1016/b978-0-12-800743-3.00001-3

Scuotto, V., Serravalle, F., Murray, A., & Viassone, M. (2019). The Shift Towards a Digital Business Model. *Women Entrepreneurs and Strategic Decision Making in the Global Economy*, 120–143. https://doi.org/10.4018/978-1-5225-7479-8.ch007

Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences*, *182*, 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787

van de Weijer, S. G., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, *8*, 100249. https://doi.org/10.1016/j.chbr.2022.100249

Сведения об авторе



Мехрдад Райеджиан Асли – доктор наук, доцент, Институт исследования и развития гуманитарных дисциплин
Адрес: 1463645851, Исламская Республика Иран, г. Тегеран, мост Ядегар, шоссе Аль-Ахмад
E-mail: m.rayejian@samt.ac.ir
ORCID ID: https://orcid.org/0000-0003-0693-1888
Web of Science Researcher ID:
https://www.researchgate.net/profile/Mehrdad-Rayejian-Asli
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57195374005
Google Scholar ID: https://scholar.google.com/citations?user=WKgazNEAAAAJ

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 13 декабря 2022 г.
Дата одобрения после рецензирования – 18 января 2023 г.
Дата принятия к опубликованию – 6 марта 2023 г.
Дата онлайн-размещения – 10 марта 2023 г.