Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 15th International Scientific and Practical Conference. Volume IV, 79-82

The Genesis of the Criminal's Personality in the Digital Age

Jelena Djubina
Riga Stradiņš University
Riga, Latvia
064676@rsu.edu.lv

Abstract. **The aim of this research is to analyze and understand the issues of a criminal's personality in the digital age to promote more effective crime prevention. It aims to analyze contemporary problems and challenges related to the identification of criminal individuals in the context of digital technologies. This research can contribute to criminology, sociology, and psychology by elucidating how the use of such technology can impact the fight against criminally inclined individuals through digital identification means. The tasks of the research involve analyzing the influence of the digital era on the genesis of a criminal's personality in the mechanism of criminal acts. The novelty of the research is linked to the concentration of the crime prevention system on exploring the mechanism of forming a criminal's personality in the digital age. The research approach will enable a deeper understanding of how the digital era influences the potential formation of personality. The research will employ methods such as theoretical methods based on the analysis of scientific research and publications, exploration of criminal identification processes in the field of digital technology, and the use of content analysis to assess the effectiveness of applied identification technologies. The author assumes that digital technologies provide powerful tools for identifying criminals but are associated with several legal issues. A balance between the use of digital technology, the effectiveness of appropriate methods, and respect for human rights and freedoms is crucial. Recommendations will be provided in the conclusion, focusing on improving legal regulations for identification technologies, considering the identified problems. An analysis of the effectiveness of existing methods and technologies will also be conducted, addressing ethical and legal issues. A special training program and implementation procedure for law enforcement agencies on the ethical and legal aspects of using digital identification methods will be proposed.**

Keywords: cybercrime, digital crime, genesis, prevention.

I. INTRODUCTION

The research into the causes of crime, as influenced by the interplay of personality, society, and the environment, integrates into criminology—an interdisciplinary science that melds sociological and legal perspectives. This multifaceted approach not only enriches criminology with fresh insights but also lays the groundwork for future explorations in the field.

The development of unique theoretical and practical crime monitoring methods, including an interdisciplinary socio-legal methodology alongside modern data analysis techniques, aims to enhance the scientific and practical facets of crime data systematization. These innovations further the advancement of contemporary crime theory and its prevention strategies.

The advent of new technologies brings with it a plethora of ethical dilemmas, from their development to the unforeseeable outcomes of their deployment and the societal impact therein. Computer technologies, in particular, endow society with new possibilities and capabilities previously unattainable. Such technological breakthroughs compel society to contemplate adjustments to regulatory frameworks, to adapt to novel situations brought about by these technologies, and to aptly incorporate new terminologies into practice.

In the digital age, the rapid evolution of technology prompts a societal reevaluation of established viewpoints. The ease and speed with which data can now be exchanged globally, the heightened potential for anonymity, the ability to obliterate electronic materials, and software technologies that facilitate the concealment of one's digital footprint all contribute to a scenario where criminals can operate undetected. The onset of the information and digital technology era necessitates a reexamination of the foundational concepts that shape the criminal personality, underscoring the need for an interdisciplinary approach. The objective of this research is to amalgamate scientific data (research), conduct legal studies, process law enforcement information, and integrate insights from sociology, aesthetics, and ethics, presenting a comprehensive analysis of the challenges at the intersection of technology and criminology.

II. METHODS

Particular attention is devoted to employing modern methods and technologies in combating crime, alongside pinpointing the limitations and ethical quandaries emanating from the use of digital identification tools. The research employs the following research methodologies: Literature review: This entails a thorough analysis of contemporary scientific research and

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol4.8189

publications focusing on cybercrime and the digital identification of criminals. This review provides foundational knowledge and situates the research within the current scholarly discourse [1]. Empirical methods: These involve the collection and analysis of data regarding existing identification technologies, assessing their effectiveness, and identifying issues linked to their application. This method grounds the research in practical, real-world technology applications and their implications [1]. The research also incorporates monographic, analytical, and documentary methods of analysis, alongside the interpretation of legal norms and concepts related to cybercrimes. Utilizing these methods offers a comprehensive understanding of the topic at hand, furnishing objective and valuable insights while ensuring a multifaceted approach [1]. Document and data analysis facilitate the classification and categorization of criminal individuals and the mechanisms of their formation. This process helps in identifying common characteristics and emerging trends. Qualitative data analysis enables the drawing of conclusions from various data sets, including historical events and/or social circumstances, thus providing a nuanced understanding of the factors contributing to the development of criminally inclined personalities. Furthermore, an evaluation of the efficacy of current methods and technologies is undertaken. This evaluation aims to highlight ethical and legal issues related to digital identity, offering a holistic view of the challenges faced in the digital age. By integrating these diverse methods, the research aims to contribute significantly to the fields of criminology and digital ethics, proposing solutions that balance technological advancements with ethical considerations and legal compliance.

III. MATERIALS

On the official website of the European Union Agency for Criminal Justice Cooperation (Eurojust) [8], cybercrime is defined as a growing and fast-evolving crime area, which accounts for a substantial share of Eurojust's overall casework [8]. The growing overlap between crimes originating on the Internet and cyber-enabled crimes such as terrorism and money laundering poses significant challenges for law enforcement agencies in tracking and apprehending cybercriminals [8]. This includes the loss of electronic data crucial for successful cybercrime investigations, the difficulty in locating perpetrators who actively conceal their physical whereabouts, legal ambiguities, and the lack of specific regulations aimed at preventing digital criminal activities. Furthermore, differences in the legal frameworks among EU member states often present serious obstacles to international cybercrime investigations, and there is no common legal basis for expedited evidence exchange.

Analyzing scientific research conducted in Nigeria, scholars describe a very high youth population, which constitutes more than 70% of Nigeria's total population, and a high level of unemployment. Youth who are not studying or working contribute to the rise in crime, especially in the growing level of cybercrime. Cybercrimes, such as fraudulent electronic mails, identity theft, hacking, cyber harassment, spamming, and Automated Teller Machine spoofing, are more prevalent in Nigeria than other types of crimes, locally referred to as "Yahoo Yahoo" [4], In 2020, internet fraud crimes, such as online romance scams, interception of business transactions for fraud purposes, hacking of government and private bank accounts, and fraudulent investment schemes, were widespread. These crimes have been gaining momentum since 2000, with the advent of the internet, computers, and mobile phones. By 2020, Nigeria had become a "hotspot," ranking third in global internet crime rates [4].

Cybercrime is defined as any unlawful behavior directed at compromising the security of computer systems and the data they process, or any unlawful behavior committed through or against computer systems or networks [4]. Youth feel empowered and unpunished in this realm, demonstrating their wealth acquired through criminal means, enticing new recruits into this criminal business, and showing them how to quickly become wealthy without exerting any effort. Youth rapidly and adeptly acquire computer technologies and internet skills, mastering cyberspace to explore its opportunities and understand the legality of their actions. Once they realize that their illegal activities lead to quick monetary gains, they become engrossed in the process, remaining unemployed but contributing to the increase in crime. Cybercrimes are more characteristic of youth, as they quickly acquire digital literacy combined with readily available hacking tools [4]. Young unemployed graduates or high school dropouts, living in poor socio-economic conditions, mainly participate in internet frauds. They lack motivation to pursue education due to financial constraints and view computer fraud as an alternative means of livelihood. To become internet fraudsters, all one needs is a computer, phone, and internet connection, and youth are taught these skills by those already involved in such crimes. This rapid learning of internet fraud basics is termed "web freestyle" [4].

Due to high unemployment and rapidly increasing crimes, Nigerian authorities have decided to increase job opportunities in the private sector that align with youths' knowledge and skills in computer technologies, redirecting youth intellect away from criminal activities. However, scholars have also acknowledged that the consequences of youth unemployment amidst the rise in cybercrimes among Nigeria's youth have not been adequately studied. Therefore, it was decided to conduct deeper research on this issue to identify the impact of youth unemployment on the cybercrime threat in Nigeria.

Delving into theory, in countries where youth constitute a significant portion of the population, the population often faces youth unemployment, making them more vulnerable to recruitment into various terrorist and criminal groups prone to violence and crimes associated with the large youth population. In countries with a large youth population neglected by authorities, crime, led by youth, tends to rise. The Nigerian government must strive to ensure that the country's youth contribute positively to society. This situation indicates that cybercrime has become a profitable enterprise and an alternative source of income for unemployed youth.

In Italy, there is a notably high level of cybercrime, particularly cyberbullying. Cyberbullying encompasses various forms of electronic aggression, harassment, blackmail, insult, humiliation, defamation, theft or alteration of personal data, illegal acquisition of such data, manipulation, and damage to personal data of minors [2]. Additionally, individuals in cyberspace have learned to spread online content aimed at minors or their family members. The goal of distributing such content is to deliberately tarnish and isolate the minor or group of minors, exposing them to serious violence, harm from attacks, or mockery [2]. The internet serves as a powerful tool for criminally inclined individuals to commit property-related offenses such as fraud, theft, money laundering, and to engage in illegal activities, including human trafficking, with organized crime adapting its methods from the real world to cyberspace. In the financial-economic sector, cybercrime includes so-called "white-collar" crimes.

The Italian State Police attempted to outline the profile of the cyber-criminal, identifying him as "a non-violent subject, with a low need to contain anxiety, determined by the fact that the crime does not take place in a physical place, strictly contact with the victim, but in the digital environment" (Lorusso, 2011) [2]. This detachment allows the criminal not to identify with a criminal persona and, consequently, not to associate their actions with crimes. Furthermore, Italian legislation includes an article providing punishment for cyberstalking, seen as the digital equivalent of the crime of persecution [2]. The article has been

reinforced with stricter punishment measures if the crime is committed using IT tools such as email, SMS, malware, and social networks. Psychology identifies several profiles of stalkers: 1) The resentful, who seeks revenge for a partner's abandonment through repeated persecutory conduct; 2) The affection seeker, who attempts to establish a friendly, dependent relationship, often found in patient-doctor contexts; 3) The incompetent suitor, who may start as a work or university colleague and becomes persistently annoying through unwanted attention; 4) The rejected, who, after refusal from an ex-partner or suitor, tries persistently to maintain any form of relationship; 5) The predator, one of the most violent types, whose desire is solely sexual, planning and hunting their victim [2]. The emergence of the internet introduced the cyberstalked, a sophisticated type of stalker who influences their victim remotely, via information technologies, thus widening the gap between the criminal and their victim. This capability allows the criminal to transcend physical boundaries; they do not physically touch the victim and lack any feelings of compassion towards them. Additionally, in Italy, cybercrimes such as "online revenge," involving the illegal distribution of sexually explicit images and videos, are prevalent, with punishment measures also being tightened [2].

Researchers have conducted an analysis of risk factors for juvenile cybercrime, focusing not on traditional crimes but on cybercrimes such as hacking attacks and sexting committed by minors. In these studies, hacking is considered a form of cyber-dependent criminal activity, whereas cyberbullying and sexting are viewed as forms of criminal behavior involving cybersecurity [5]. For various types of cybercriminal behavior, it has been found that perpetrators demonstrate relatively low internal moral and social values. Similar to traditional crimes committed by minors, cybercrimes have identified risk factors such as peer influence on deviant behavior among minors, directed towards cyberbullying and hacking, as well as peer pressure directed towards sexting. Significant risk factors for cyberbullying included prior offenses and victimization in both online and offline environments. Additionally, the influence of the dark web, especially in cyberbullying, and a very high level of computer addiction were identified. Studies have shown that these risk factors were mitigated among minors attending middle or high school. However, to draw accurate conclusions, further in-depth research is needed.

IV. RESULTS AND DISCUSSION

Cybercrime is distinguished by the fact that cybercriminals do not necessarily need to be physically present at the scene of the crime. It refers to "a crime in which the behavior or material object of the crime is connected to IT or telematic systems, i.e., software that receives data, for example, from mobile devices and displays it on a computer or smartphone screen, or is committed using such a system" [2]. Due to the rapid growth of various types of cybercrimes, changes have been made to Italian legislation, particularly to the Penal Code, to increase punishments for actions where crimes are committed using information technology tools. These changes provide legal grounds for prosecuting the illegal distribution of sexually explicit materials, images, and videos. Analyzing various studies, it can be concluded that the criminological assessment of criminal behavior should consider the influence of virtual space on the cognitive processes of criminal personalities. Cybercrime significantly differs from traditional crime and undoubtedly requires special and ongoing attention in the field of criminological research.

Researchers in the USA have proposed their own methodology for tracking criminals committing crimes in cyberspace. This methodology is based on the mathematical concepts of identification codes, ensuring a reduction in resources from law enforcement agencies without compromising the ability to unambiguously identify a suspect when they become "active" in activities related to terrorism or narcotics. This method operates under the assumption that when an individual becomes "active" in drug trafficking or human trafficking activities, their friends/accomplices will have some knowledge of their individual plan. Accordingly, even if an individual is not under direct surveillance by law enforcement agencies (such as phone call records, movements, social interactions with others) but is on the list of friends/accomplices of the person involved in drug-related activities, those involved in drug-related activities can be unambiguously identified [3].

With increasing attention, research on the Dark Tetrad (D4) is gaining momentum [7]. The Dark Tetrad encompasses a set of personality traits that combine negative characteristics such as narcissism, Machiavellianism, psychopathy, and sadism. These traits share common features, including a lack of empathy and low agreeableness towards others. Machiavellianism is characterized by selfishness, a tendency towards manipulation, and motivation to exploit others. Narcissism is defined by a strong sense of self-worth, presumed superiority, and interpersonal domination. Individuals displaying psychopathic traits often exhibit impulsiveness and are inclined towards sensation-seeking and antisocial behavior. Those with sadistic inclinations derive pleasure from intentionally inflicting psychological and physical pain on others [7]. Consequently, relationships with individuals exhibiting heightened D4 traits can be problematic and pose risks to the physical and emotional well-being of those interacting with them.

Individuals with elevated D4 traits show a greater propensity for cyberstalking intimate partners, monitoring their behavior, phones/computers, or using apps to observe their activities, with sadistic tendencies being a primary indicator of such behavior. Online platforms, where individuals can seek new and short-lived acquaintances to satisfy their goals and needs, are highly characteristic of individuals with elevated levels of D4 traits. However, scientists cannot definitively say whether people with elevated D4 traits prefer online searches or offline encounters. They advise society to be cautious in choosing dating partners and to identify individuals with heightened D4 traits at an early stage to avoid potential victimization.

With the rapid advancement of information technology, particularly the significant growth in computer gaming, society is witnessing a rise in aggression and criminal behavior among individuals, primarily impacting the younger generation. Various studies have shown that children engrossed in computer games become aggressive and antisocial, leading to the development of criminal personality traits. Many psychologists argue that computer games with aggressive content cultivate an aggressive and destructive behavioral pattern in individuals. In many computer games, adolescents can engage in actions that are socially disapproved, providing them with emotional release that they cannot find in their external environment. Computer games often include auditory signals, which also exert additional psychological influence, potentially even provoking psychological disorders [6]. Furthermore, such auditory signals, when encountered in the external environment, can trigger bursts of aggression, which could serve as a catalyst for the commission of violent criminal offenses, including causing grievous bodily harm and even murder.

As minors often exhibit heightened emotional arousal, which quickly escalates into aggression and mental instability, leading to affective outbursts, they are susceptible to the influence of external factors and experienced criminals, as well as groups such as terrorists and drug-related entities. These groups easily

persuade minors to engage in unlawful activities, presenting a significant problem at present.

V. CONCLUSIONS

With the rapid development of digital technologies, society has witnessed a decline in humanity and empathy, leading to an increase in virtual relationships. The cyber realm offers an opportunity for criminally inclined individuals to commit illegal actions with confidence in remaining unpunished. The high level of criminal activity facilitated by the internet has prompted legislators to swiftly respond with effective amendments to legislative acts, aiming to prevent the dangers posed by cyberspace and its influence on the world at large. Given that cybercrime significantly differs from conventional crime, studies must consider the influence of virtual space on the cognitive processes of criminally inclined individuals, such as acquiring new knowledge and making appropriate decisions. These processes involve various cognitive functions that aid in acquiring knowledge and understanding the surrounding world, including perception, attention, memory, and reasoning.

In a world where digital technologies are rapidly advancing, constructing a criminological profile of offenders, whose activities are geared towards property crimes or crimes against individuals, proves challenging. It is difficult to establish the behavior of such criminals, their physique, the clothing they wore at the time of committing any cybercrime, and also to determine the psychological profile of the offender. Virtual reality allows criminals to blend in, as cyberspace lacks a clear description of appearance, emotions, or feelings. Moreover, individuals committing cybercrimes likely experience emotional inadequacy and seek compensation specifically within cyberspace, where they can affirm themselves and receive recognition from strangers. Perhaps, to reduce cybercrime, society needs to engage schoolchildren in various clubs and sports sections, and involve students in cultural and mass work to prevent them from constantly being in cyberspace and to deter the temptation to commit cybercrimes.

In conclusion, it remains a fact that only specific individuals commit criminal offenses. Understanding what happens at their psychological and biological levels is crucial for studying the criminal's personality to subsequently reduce the likelihood of criminal offenses. Major global organizations such as The International Criminal Police Organization (Interpol), The United Nations Office on Drugs and Crime (UNODC), and Drug Trafficking Organizations (DTO) have developed methodologies aimed at activities related to drug trafficking or terrorist groups in cyberspace. These organizations analyzed judges' comments on verdicts, created a network of individuals involved in drug distribution, studied the network of drug-related criminals, analyzed court transcripts, and identified key participants to create a social network. These combined actions yielded positive results for further tracking individuals involved in terrorist groups and drug trafficking. If such coordinated efforts are applied in countries where the number of various cybercrimes is rapidly increasing, it is my view that fruitful results will be achieved in the near future.

Additionally, it is worth noting that in practice, it is very difficult to consider all the factors that can become causes and lead to the commission of criminal offenses. Therefore, one of the main tasks before science is to identify the determinants for specific criminal offenses, namely to identify the causes and conditions of the crime.

REFERENCES

[1] K.Martinson and A.Piper. “Methodology of scientific activity: an interdisciplinary perspective”. Riga, RSU, pages 608. 2021.

[2] F.Greco; G.Greco. “INVESTIGATIVE TECHNIQUES IN THE DIGITAL AGE: CYBERCRIME AND CRIMINAL PROFILING”. European Journal of Social Sciences Studies. June 2020. DOI: 10.5281/zenodo.3877668

[3] K.Basu, A.Sen. “Social Networks. Identifying individuals associated with organized criminal networks: A social network analysis”. NetXT Lab, School of Computing, Informatics and Decision Systems Engineering, Arizona State University, 699, South Mill Ave., Tempe, AZ, USA. Jan 2021.

[4] Obianagwa, Christopher Ewuzie; Ngoka Ruth Obioma; Gift, Uwaechia Onyinye; Hayford, Ezugwu Ikechukwu; Okpala Joy Chinaza; et al. “Youth Unemployment and Cybercrime in Nigeria”. African Renaissance; London. United Kingdom Vol. 20, Iss. 2, 177–199. Jun 2023. DOI:10.31920/2516-5305/2023/20n2a9

[5] Inge B. Wissink, Joyce C.A. Standaert, Geert Jan J.M. Stams, Jessica J. Asscher, Mark Assink. “Risk factors for juvenile cybercrime: A meta-analytic review. Aggression and Violent Behavior”. Volume 70, 101836. May–June 2023. https://doi.org/10.1016/j.avb.2023.101836

[6] Zabarniy, Maksym; Topchii, Vasyl; Korniakova, Tatiana; Topchii, Oksana; Topchii, Vitalii. “Criminological Analysis of Determinants of Criminal behavior”. Journal of Forensic Science and Medicine 9(2):p 144-152. Apr–Jun 2023. DOI: 10.4103/jfsm.jfsm_84_22

[7] Richelle Mayshak, Dominika Howard, Michelle Benstead, Anna Klas, David Skvarc, Travis Harries, Brittany Patafio, Abby Sleep, Ross King, Shannon Hyder. “Dating in the dark: A qualitative examination of dating experiences in Dark Tetrad personalities School of Psychology”. Deakin University, 1 Gheringhap Street, Geelong, VIC, 3220, Australia. Computers in Human Behavior Volume 143. June 2023. https://doi.org/10.1016/j.chb.2023.107680

[8] European Union Agency for Criminal Justice Cooperation (Eurojust). 2002. [Online]. Available: https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime [Accessed: March 24, 2024].