DOI:
УДК 343.01 (045)

L. Chimchiuri,
lawyer

THE EVOLUTION OF CYBERCRIME LEGISLATION

Sokhumi State University
Ana Politkovskaia St, 9, 0186, Tbilisi, Georgia
E-mail: lika.chimchiuri@sou.edu.ge

The purpose *of the article is analyzes the evolution of cybercrime legislation in several jurisdictions, with a focus on how laws are changing to reflect the complexities of cyber threats in a linked digital landscape.* ***Research methods:*** *this study uses a comparative analysis to identify major legislative developments across North America, Europe, Asia, and the rest of the developing world.* ***Results:*** *the fast development of digital technology has fueled the growth of cybercrimes such as hacking, phishing, and online fraud, posing new problems to judicial systems around the world. The study identifies comparable legislative frameworks, such as criminalizing unauthorized access to computer systems, as well as variations in approaches to penalties, jurisdiction, and enforcement roles. The paper goes further into the effectiveness of these laws in discouraging cybercrime, the difficulty of cross-border enforcement, and the delicate balance between crime prevention and individual privacy rights.* ***Discussion:*** *the article is to provide insights into the creation of strong legal frameworks that can keep up with the ever-changing nature of cyber risks by highlighting new trends and best practices. This analysis not only throws light on present legislative measures but also explores the implications for future policymaking in cybercrime prevention and punishment.*

Key words: *evolution of cybercrime; cybercrime; legislation; comparative analysis; international cooperation.*

Problem statement and its relevance. Cybercrime is a growing concern for countries around the world, affecting individuals, businesses, and governments alike. To combat this evolving threat, countries have been enacting cybercrime legislation to address the various forms of online criminal activities. According to a report by the United Nations Conference on Trade and Development (UNCTAD), 156 countries, representing 80 percent of the global community, have implemented cybercrime legislation.

However, the adoption rates vary across regions, with Europe leading at 91 percent and Africa at the lowest with 72 percent. This discrepancy highlights the need for a unified global approach to tackling cybercrime.

Law enforcement agencies and prosecutors face significant challenges in enforcing cybercrime laws, especially when it comes to cross-border enforcement. The ever-changing cybercrime landscape and the resulting skills gap pose a constant hurdle for authorities. Collaboration and knowledge sharing among countries are essential to address these challenges effectively.

This article examines how various countries are updating their laws to combat cybercrime, focusing on North America, Europe, Asia, and developing regions. By comparing these legal approaches, we aim to understand the similarities and differences in how countries criminalize unauthorized access, handle penalties, and manage enforcement roles.

Research methodologies such as dogmatic methods and comparative legal analysis, evaluating the perspectives of experienced experts in the field. This study not only highlights the current legislative measures but also discusses the challenges of cross-border enforcement and the balance between preventing crime and protecting privacy rights.

Summary of the main research material. *Fighting cybercrime in the early 20th century.* In the early 20th century, the concept of cybercrime was virtually nonexistent. The era was characterized by the nascent stages of electronic communication and computing, with technologies such as the telegraph, telephone, and early computers emerging. Consequently, the primary focus was on addressing conventional crimes, and the legal frameworks of the time did not account for the digital landscape that would later develop.

However, as early as the 1930s, with the invention of the first programmable computers like the Zuse Z3 and the development of cryptographic techniques during World War II, the seeds of future cyber-related issues were sown. These advancements hinted at the potential for unauthorized access and manipulation of data, but the legal and societal understanding of such threats was minimal.

Cybercrime poses significant challenges due to the internet's scale, accessibility, anonymity, portability, global reach, and the absence of capable guardians. With billions online, easy access to tools, and global connectivity, offenders can operate at unprecedented scales, evade detection through anonymity, and exploit jurisdictional complexities. Law enforcement faces hurdles in data retrieval, surveillance, and cooperation across borders. Effective responses require a multifaceted approach, including legal measures, technological safeguards, social norms, and industry cooperation [1].

Legislation during this period was rudimentary and primarily focused on protecting physical property and traditional forms of communication. For instance, laws against wiretapping, which emerged in the early 20th century, were some of the earliest forms of legislation that tangentially addressed issues related to electronic communication. The Communications Act of 1934 in the United States is one example, primarily aimed at regulating telephone and radio communications, inadvertently laying a foundation for future cybercrime laws.

Enforcement was equally rudimentary, as law enforcement agencies lacked the expertise and technology to tackle electronic crimes. The focus remained on traditional crimes, with the understanding of electronic and digital vulnerabilities being very limited. The notion of a "hacker" or a cybercriminal was yet to be conceived, and as such, there was no structured approach to combating such threats.

Cybercrime has evolved alongside technology, exemplified by Sergei Tšurikov's 2008 hack of RBS WorldPay, which led to a $9.4 million theft. Modern cybercrimes are organized, financially motivated, technologically advanced, and transnational, exploiting the pervasive digital technology in daily life. Initially focused on computer manipulation and telecommunication theft, cybercrime has expanded with technology to include hacking, botnets, and network-based crimes. The increasing connectivity and the Internet of Things introduce new vulnerabilities, continually presenting fresh challenges for cybersecurity [1].

The internet's evolution from military digitization in the 1960s to widespread e-governance, e-commerce, and cyber-crime, highlighted by significant cyber laws like the 2001 EU Convention on Cybercrime, underscores its impact on global communication and security [2].

The United States has taken significant steps to combat cybercrime through the implementation of key legislation. One such law is the Computer Fraud and Abuse Act (CFAA), enacted in 1986. The CFAA serves as the primary federal statutory mechanism for prosecuting cybercriminals, including hackers. It prohibits unauthorized access to computers, obtaining national security information, damaging computer systems, and trafficking in passwords, among other offenses. Penalties for CFAA violations range from fines to imprisonment, with the severity depending on the nature of the offense.

Another crucial piece of legislation is the Electronic Communications Privacy Act (ECPA), passed in 1986. The ECPA regulates how federal and state law enforcement agencies can obtain access to electronic evidence. It governs the disclosure of stored communications, records, and subscriber information held by service providers. The ECPA also updated the Wiretap Act to allow interception of electronic communications with proper authorization.

In March 2018, the United States enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The CLOUD Act addresses the challenges faced by law enforcement agencies in accessing electronic information stored by U.S.-based global providers. It allows foreign partners to enter into bilateral agreements with the United States, facilitating direct access to critical electronic evidence for investigations related to serious crimes such as terrorism, violent crime, sexual exploitation of children, and cybercrime.

Mechanisms of combating cybercrime in the 2nd half of the 20th century

The second half of the 20th century saw the rise of computers and the internet, bringing about new forms of crime that traditional law enforcement methods struggled to address. The initial mechanisms for combating cybercrime during this period evolved as both technology and criminal tactics advanced.

In the 1970s and 1980s, as computers became more common in businesses and government, the first computer crime laws were introduced. For example, the U.S. enacted the Computer Fraud and Abuse Act (CFAA) in 1986, which made unauthorized access to computer systems a federal offense. Similarly, other countries started to draft legislation aimed at defining and punishing various forms of cybercrime.

Cybercrime often mirrors real-world crime motivations, suggesting traditional criminological theories like rational choice and deterrence may still apply. However, unique aspects of cybercrimes, such as the necessity of technological knowledge, might limit the applicability of these theories to some extent [3].

As cybercrime grew more sophisticated, traditional police forces recognized the need for specialized units. These units were equipped with the technical skills and knowledge required to investigate and prosecute cybercrimes. For instance, the U.S. Federal Bureau of Investigation (FBI) established its Computer Analysis and Response Team (CART) in 1984, focusing on computer-related offenses. Similar specialized units were developed in other countries.

The creation of Computer Emergency Response Teams (CERTs) marked a proactive approach to cyber threats. The first CERT was established at Carnegie Mellon University in response to the Morris Worm attack in 1988. These teams focused on identifying vulnerabilities, responding to incidents, and disseminating information about threats and best practices to prevent cyber-attacks.

Efforts to combat cybercrime also included educating the public about the risks associated with using computers and the internet. Governments and organizations launched campaigns to raise awareness about safe online practices, phishing scams, and the importance of strong passwords. These educational efforts aimed to reduce the number of potential victims and make it harder for cybercriminals to succeed.

Law enforcement and cybersecurity professionals developed new technologies and tools to detect, track, and analyze cyber threats. This included the use of intrusion detection systems, encryption, and forensic software to investigate cybercrimes and secure computer systems.

The second half of the 20th century laid the groundwork for modern cybersecurity practices. Through early legislation, specialized law enforcement units, international cooperation, CERTs, public education, and technological advancements, significant strides were made in combating the growing threat of cybercrime. These efforts provided the foundation for the more sophisticated and coordinated approaches used today.

Various specialized institutions are dedicated to countering cybercrime at national and transnational levels. In the United States, the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) and the Federal Bureau of Investigation's (FBI) Cyber Division play crucial roles in investigating and mitigating cybercrimes. These units employ innovative techniques and tools while leveraging legal authorities to combat cyber threats effectively.

International cooperation is also vital in tackling cybercrime, as cyber threats transcend national borders. The United States has developed strategies and frameworks for cooperation with other countries to combat cybercrime collectively. Through mutual legal assistance treaties (MLATs) and bilateral agreements, countries can collaborate on inves-

tigations, share intelligence, and facilitate the extradition of cybercriminals. The United States also participates in international forums and initiatives to promote information sharing and capacity building in the fight against cybercrime.

Jurisprudence and case law have played a significant role in shaping cybercrime legislation and its interpretation. Landmark cases such as United States v. Jones (2011), Riley v. California (2014), and Carpenter V. United States (2018) have addressed key Fourth Amendment issues related to privacy rights in the digital age. These cases have provided guidance on the constitutional limits of law enforcement's ability to conduct electronic surveillance and obtain evidence in cyberspace.

The evolution of cybercrime legislation reflects the global recognition of the growing threat posed by cybercriminals. Countries, including the United States, have enacted laws to prevent, detect, and prosecute cybercrimes. However, challenges remain, including regional variations in legislation adoption rates and the dynamic nature of cyber threats. Continued international cooperation, information sharing, and the development of innovative tools and strategies are crucial to effectively combat cybercrime and protect individuals, businesses, and governments worldwide.

Effective action against cybercrime requires strong political leadership to foster public-private collaboration on a national and global scale, addressing legal and technical barriers, and ensuring robust judicial and policing systems. A multifaceted, understandable international response is essential, balancing security and freedom, and promoting practical good practices [4].

Cooperation Against Cybercrime in the 21st Century

In the 21st century, the interconnected nature of the digital world necessitates international cooperation to combat cybercrime effectively. Cyber threats are borderless, impacting individuals, businesses, and governments globally. Therefore, a coordinated effort among nations is crucial for addressing these challenges comprehensively.

The Budapest Convention, the first international treaty on cybercrime, harmonizes domestic laws, establishes investigative procedures, and facilitates international cooperation. It covers illegal access, data interference, computer-related fraud, and more. Benefits include a legal framework for international collaboration, membership in the Cybercrime Convention Committee, and access to capacity-building programs. States can accede by demonstrating implementation of the Convention's provisions and completing internal procedures [5].

There is no universally accepted definition of cybercrime. The most common approach is to define the key terms used in cybercrime investigations. Examining frequently-used definitions will allow us to identify key concepts and use those definitions consistently in a country's cybercrime strategy [5]. The lack of a broadly acknowledged definition of cybercrime poses a fundamental challenge in the realm of cybersecurity. Countries' legal systems differ widely, with each having its own set of laws and classifications. What is regarded a cybercrime in one jurisdiction may not be classified the same way in another.

One of the primary ways countries cooperate against cybercrime is through international legal frameworks. Instruments such as the Budapest Convention on Cybercrime provide a comprehensive guide for countries to develop national legislation and promote international cooperation. The convention facilitates the harmonization of laws, making it easier for countries to collaborate in investigations and prosecutions. By providing a common standard, it helps bridge gaps between different legal systems.

Effective cybercrime prevention and prosecution rely heavily on information sharing. Nations, through organizations like INTERPOL and Europol, share intelligence on cyber threats and coordinate joint operations to dismantle cybercriminal networks. This real-time information exchange enhances the ability to respond swiftly to emerging threats. For example, coordinated international actions have successfully disrupted major ransomware groups and other cybercriminal organizations.

Positive outcomes to cybercrime investigations depend on the successful collection, analysis, and attribution of digital evidence, which refers to data stored on, received, or transmitted by electronic devices, including evidence from digital devices or records obtained from online service providers [5].

Developing nations often lack the resources and expertise to combat sophisticated cyber threats. International cooperation involves capacity-building initiatives where developed nations and organizations provide technical assistance and training to improve the cybersecurity capabilities of developing countries. This includes setting up cybercrime units, training law enforcement officers, and sharing best practices in cybercrime investigation.

Cybercrime often targets critical infrastructure and private sector entities, making public-private partnerships essential. Governments collaborate with tech companies, cybersecurity firms, and other private sector stakeholders to enhance overall cybersecurity resilience. These partnerships facilitate the sharing of threat intelligence and the development of innovative solutions to combat cybercrime. For instance, joint initiatives between government agencies and cybersecurity companies have led to the creation of more effective tools for detecting and preventing cyber attacks.

Despite significant progress, several challenges remain. Differences in legal definitions of cybercrime, varying levels of technological advancement, and issues of jurisdiction complicate international cooperation. Additionally, balancing the need for security with the protection of privacy and civil liberties remains a delicate task.

To develop a cybercrime strategy, it is essential to start with a stocktaking audit, assessing current processes, resources, and skills to combat cybercrime. This includes evaluating legal frameworks, existing cybercrime policies, technological infrastructure, human resource capabilities, and cooperation mechanisms with international and regional partners. Identifying gaps and weaknesses in these areas provides a foundation for strategic improvements, ensuring a comprehensive approach to enhancing cybercrime resilience and response capabilities [5].

To overcome these challenges, ongoing dialogue and collaboration are essential. Regular international conferences, such as the Internet Governance Forum and regional cybersecurity summits, provide platforms for countries to discuss and resolve these issues. Enhancing mutual legal assistance treaties (MLATs) and developing new international agreements can also streamline cooperation efforts.

The collaboration between government agencies, international partners, and private sectors is crucial in combating cybercrime effectively. By promoting inter-agency information sharing, expanding international networks, and fostering public-private partnerships, countries can enhance their cybercrime response capabilities. Public awareness campaigns, like the UK's Get Safe Online program, play a vital role in educating individuals and businesses about common cyber threats and how to protect themselves. These initiatives aim to empower citizens to safeguard their digital assets against fraud, identity theft, viruses, and other online risks [5].

Conclusions. In today's world, cybercrime remains an unsolved problem as technology advances, opportunities for cybercrime increase. Numerous loopholes in both international law and domestic legislation must be addressed and eliminated promptly to protect legal benefits. Addressing the global threat of cybercrime necessitates a coordinated and collaborative multinational effort. This involves developing worldwide cooperation and standardization, including collaboration among governments, businesses, and individuals to boost cybersecurity, share information, and build common frameworks. To achieve this, it is necessary to establish international standards, develop and adopt norms for defining and combating cybercrime, harmonize legal definitions, improve information sharing, strengthen international cooperation, enhance cross-border law enforcement collaboration, promote public-private partnerships, and raise global awareness of cybersecurity.

Institutions such as the United Nations, Interpol, and the International Telecommunication Union (ITU) must support and participate in these initiatives to increase global cooperation against cybercrime. By supporting these efforts, the international community can work together to establish a safer and more resilient cyberspace through a collaborative approach to combating cybercrime at the global level.

Cybercrime legislation is constantly evolving to keep up with new digital threats. As technology advances, laws must quickly adapt to address emerg-

ing challenges. This study examined cybercrime laws worldwide, focusing on North America, Europe, Asia, and developing countries. Despite differences in penalties and enforcement, most regions have similar laws against unauthorized computer access. However, enforcing these laws across borders is challenging, and balancing crime prevention with privacy rights is delicate. To fight cybercrime effectively, countries need robust, adaptable laws and international cooperation. These laws should protect people and organizations, respect individual privacy, and create a safe online environment.

The fight against cybercrime requires ongoing updates to legislation and global teamwork. As technology continues to advance, lawmakers must be proactive and flexible to stay ahead of cybercriminals, ensuring that legal frameworks remain effective and relevant in protecting society.

References

1. Clough Jonatan. 2015. *Principles of Cybercrime.* 2nd ed. Cambridge: Cambridge University Press.

2. Halder Debarati. 2022. Cyber Victimology: Decoding Cyber-Crime Victimisation. New York: Routledge.

3. Jahankhani Hamid, ed. 2019. *Cyber Criminology*. Springer International Publishing.

4. Padallan Jocelyn O. 2022. Cyber Security. Oakville: Arcler Press.

5. Stock Jürgen. Secretary General, 2021. INTERPOL National Cybercrime Strategy Guidebook.

6. Cybercrime Legislation Worldwide. URL: https://unctad.org/page/cybercrime-legislation-worldwide.

7. Cybersecurity Laws and Regulations Report 2024 USA. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa.

8. Schatz Legislation To Help Fight Cybercrime Signed Into Law. URL: https://www.schatz.senate.gov/news/press-releases/schatz-legislation-to-help-fight-cybercrime-signed-into-law.

9. State Cybercrime Legislation in the United States of America: A Survey. URL: https://scholarship.richmond.edu/jolt/vol7/iss3/4/.

10. United States of America - Octopus Cybercrime Community. URL: https://www.coe.int/en/web/octopus/-/united-states-of-america.

Ліка Чімчіурі

ЕВОЛЮЦІЯ ЗАКОНОДАВСТВА ПРО КІБЕРЗЛОЧИННІСТЬ

Сухумський державний університет
вул. Анни Політковської, 9, 0186, Тбілісі, Грузія
E-mail: lika.chimichurri@sou.edu.ge

Метою *статті є аналіз еволюції законодавства про кіберзлочинність у кількох юрисдикціях, з акцентом на те, як закони змінюються, щоб відобразити складність кіберзагроз у пов'язаному цифровому ландшафті.* ***Методи дослідження:*** *у цьому дослідженні використовується порівняльний аналіз для визначення основних законодавчих змін у Північній Америці, Європі, Азії та решті країн, що розвиваються.* ***Результати:*** *швидкий розвиток цифрових технологій сприяв зростанню кіберзлочинів, таких як хакерство, фішинг і онлайн-шахрайство, створюючи нові проблеми для судових систем у всьому світі. Дослідження визначає порівняльні законодавчі рамки, такі як кримінальна відповідальність за несанкціонований доступ до комп'ютерних систем, а також відмінності в підходах до покарань, юрисдикції та функцій правозастосування. У документі розглядається ефективність цих законів у боротьбі з кіберзлочинністю, труднощі транскордонного правозастосування та тонкий баланс між запобіганням злочинності та правами особи на конфіденційність.* ***Обговорення:*** *стаття має надати уявлення про створення міцної правової бази, яка зможе йти в ногу зі постійними змінами природи кіберризиків, висвітлюючи нові тенденції та найкращі практики. Цей аналіз не тільки проливає світло на поточні законодавчі заходи, але й досліджує наслідки для майбутньої політики щодо запобігання кіберзлочинності та покарання.*

Ключові слова: *еволюція кіберзлочинності; кіберзлочинність; законодавство; порівняльний аналіз; міжнародне співробітництво.*

Стаття надійшла до редакції 31.05.2024