COMMENTS

Computer Information Crimes and Other Cybercrimes: Comparative Legal Analysis of the Legislation of the BRICS Countries

Viktor Pushkarev,

HSE University (Moscow, Russian Federation)

https://orcid.org/0000-0002-3536-6497

Anna Solomatina,

Financial University under the Government of the Russian Federation (Moscow, Russian Federation)

https://orcid.org/0009-0009-4965-544X

https://doi.org/10.21684/2412-2343-2025-12-4-167-190

Received: February 11, 2025
Reviewed: July 20, 2025
Accepted: September 7, 2025

Abstract. Modern society has witnessed the rapid pace at which the digital transformation is taking place in all public spheres without any exception. In parallel, there are obvious and dangerous processes of crime digitalization, with unprecedented growth rate of crimes committed using information and telecommunication technologies. With the development of information technology and the expansion of the digital space, the issues of security and combating crime related to computer information are becoming increasingly relevant. It is quite obvious that in such conditions, the state and law enforcement agencies should propose effective and coordinated criminal policy measures aimed at guarantying law and order and protecting the interests of individuals, society and states from new information and digital threats, which is impossible without fundamental legal research of the main reasons directly affecting various spheres of human activity, including the economy, politics, social relations, and security–the new legal institute of computer

information. All BRICS member countries contribute to the development of modern legislation, relevant legal theory and practice forming national legal standards of criminal policy, which requires comparative legal research and a systematic, verified normative and technical approach. The integration processes taking place in the BRICS create conditions for the study, interpretation and modification of criminal law norms in Russian law, as well as prerequisites for the internationalization of law, closely related to its evolution. The article is a study aimed at trying to identify stable patterns, internal and external systemic relationships of the legal institute of computer information in criminal law as a complex, multidimensional and interdisciplinary phenomenon requiring high-quality scientific study and consistent regulation. This will create the basis for the development of effective proposals to improve legislation and measures aimed at ensuring information security and countering criminal activity in the information and telecommunications sector. In the study, various scientific methods have been used, dialectical, comparative legal, systemic structural among others. The materials for the study are based on the analysis of legislative acts of the BRICS countries, scientific publications and research of specialized organizations, investigative and judicial practice, as well as electronic resources and databases. An integrated approach made it possible to provide a comprehensive and in-depth study of the topic, taking into account both theoretical aspects and practical experience in countering crime in the field of computer information. The study of the best international practices of the legal regulation in the criminal law of the BRICS member states creates prerequisites for their implementation in Russian law and the development of scientifically justified proposals to improve Russian criminal policy and criminal legislation aimed at ensuring information security and countering criminal activity in the information and telecommunications environment.

Keywords: criminal law; computer information; data protection; BRICS; cybercrimes; cybersecurity; personal data.

To cite: Pushkarev, V., & Solomatina, A. (2025). Computer information crimes and other cybercrimes: Comparative legal analysis of the legislation of the BRICS countries. *BRICS Law Journal*, *12*(4), 167–190.

Table of Contents

Introduction

In modern society, information is a key resource that permeates all fields of knowledge ranging from natural sciences to social disciplines. It plays a strategic role in scientific discoveries, technological innovations, management decisions, and social communication. Effective information management is an important skill in the information age, allowing to describe and analyze natural and social processes.

Computer information is one of the basic concepts of computer science and information technology. Generally, it is data that can be represented, processed, transmitted and stored using computing systems. This concept affects technical, mathematical, legal and social areas.

At the same time, the modern world is facing a growing threat of cybercrime, which covers a wide range of illegal activities: theft and unauthorized access to computer information and personal data, the development and distribution of

malicious software, attacks on critical information infrastructure, DDoS attacks, including using botnets and Internet of Things devices (IoT), attacks on distributed registry systems and attacks using neural networks. These threats are becoming increasingly complex and sophisticated, which requires states to take appropriate measures to prevent and combat them.

The BRICS member countries play a key role in shaping international cybersecurity policy. Each of these countries develops and implements its own legislative and institutional measures to counter cybercrime, based on unique legal and socio-economic conditions. Their experience and approaches to cybersecurity have a significant impact on global standards and practices in this area.

This article examines the various approaches and legislative measures taken by the BRICS countries to counter cybercrime. Special attention is paid to the analysis of key legislative acts, initiatives and strategies aimed at protecting information systems and personal data. There is also a review of the opinions and research of leading scientists from these countries, who emphasize the importance of international cooperation and exchange of experience to effectively combat cyber threats.

This study examines cooperation in the field of cybercrime not only as a technical necessity but also as an element of forming alternative legal standards in a multipolar world.[1]

1. Computer Information for Countering Crimes in the Field of Information and Telecommunication Technologies

1.1. The Concept of Computer Information

Computer information has an important feature of digital representation, which unifies the processes of data storage and processing, ensuring high accuracy and speed of operations. This makes it easy to transfer information through communication networks and subject it to various types of processing, including compression, encryption and analysis.

The term "computer information" is derived from the Latin word "*information*," meaning "information, explanations, presentation." This collective concept covers aspects related to the transmission, storage and data processing.

Dictionaries define "information" in different ways, in general it means "information about the world and the processes taking place in it, perceived by a person or device."[2]

---

[1] Mateykovich, M., & Skorobogatko, A. (2024). Who does international law serve? *BRICS Law Journal*, *11*(3), 149–158.

[2] Ozhegov, S. I., & Shvedova, N. Y. (2010). *Dictionary of the Russian language* (p. 221). M. O. Wolf. (In Russian); Sklyarova, G. N. (Ed.) (2014). *Dictionary of key words of the Russian language* (p. 220). St. Petersburg University Publishing House. (In Russian).

In the Russian Federation, a number of legislative acts have been adopted regulating the processing, storage and transmission of information. The main attention is paid to digital information, which is enshrined in paragraph 1 of Article 2 of the Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection,"[3] and in Article 2 of the Model Information Code for the CIS Member States of 2012.[4] In Articles 4, 5, 6 and 6.1 of the Federal Law of July 29, 2004 No. 98-FZ "On Trade Secrets" the term "information" is used interchangeably.[5]

Another important legislative act is the Federal Law No. 152-FZ of July 27, 2006 "On Personal Data,"[6] which regulates the processing of personal data and establishes requirements for their protection.

All these regulations treat "information" as information or data expressed in any form, including electronic, subject to legal regulation.

The concept of computer information is not reflected in the Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection" and the legal acts listed above. It is enshrined in Chapter 28 "Crimes in the Field of Computer Information" of the Criminal Code of the Russian Federation. According to Note 1 to Article 272 of the Criminal Code of the Russian Federation,

> computer information means information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing and transmission.[7]
>
> Such information may be stored in the electronic computers and other computer devices (hereinafter referred to as computer devices) or on any external electronic media (disks, including hard disk drives, flash cards, etc.) in a form accessible to the perception of a computer device, and (or) transmitted via electrical communication channels.[8]

---

3 Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies, and Information Protection." SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_61798/. (In Russian).

4 Model Information Code for CIS Member States (2012). Zakon.kz. https://online.zakon.kz/Document/?doc_id=31307564#pos=6;-106. (In Russian).

5 Federal Law No. 98-FZ of July 29, 2004 "On Commercial Secrets." SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_434573/. (In Russian).

6 Federal Law No. 152-FZ of July 27, 2006 "On Personal Data." SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_61801. (In Russian).

7 Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996. SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_10699/. (In Russian).

8 Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 of December 15, 2022 "On Some Issues of Judicial Practice in Criminal Cases on Crimes in the Field of Computer Information, as well as Other Crimes Committed Using Electronic or Information and Telecommunication Networks, Including the Internet." SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_434573/. (In Russian).

It is interesting to consider the issue of legal regulation of computer information in the BRICS countries. The analysis shows both differences and similarities in approaches that can help in understanding the general direction of development of the legal framework in this area.

1.2. Comparative Legal Analysis of the BRICS Countries Legislation Regulating the Use of Computer Information and Countering Crimes in the Information and Telecommunications Sector

Brazil: In the Federal Republic of Brazil, the fight against cybercrime is conducted in accordance with Marco Civil da Internet and the Personal Data Protection Act (LGPD).

The first one, adopted in 2014, regulates the legal basis for using the Internet, including issues related to confidentiality, data protection and liability, and criminal liability for cybercrimes. It enshrines the principles of net neutrality, protection of user rights and obligations of Internet service providers, and restricts the use of personal data without a court order.[9]

The Personal Data Protection Act (LGPD), adopted in 2018, regulates the collection, storage, processing and transfer of personal data. The law obliges companies to comply with strict data protection standards and provides for severe penalties. LGPD was developed in response to the need to strengthen control over the processing of personal data in the digital age.[10]

The concept "computer information" is defined in Law No. 12.737/2012: any data, programs, information or commands that can be entered into a computer system. The law is known as the "Carolina Dieckmann Law" and it was adopted after an incident with a famous actress who was subjected to a cyber-attack, as a result of which her personal photos were stolen and posted on the Internet. The law regulates illegal acts committed in the field of computer technology and establishes criminal liability for their commission.[11]

Egypt: The Arab Republic of Egypt has adopted Law No. 175/2018 on combating cybercrime. Its regulation enshrines the concepts of "computer information"–any data stored in digital form, including emails, documents, databases and software, as well as "digital evidence," which implies any data used as evidence. These may include emails, databases, and other forms of computer information. These innovations are undoubtedly important for countering crimes committed in the field of information technology.[12]

---

[9] Law No. 12,965, April 23, 2014. Pesquisa Legislação da Presidência da República. https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6

[10] General Personal Data Protection Act (LGPD), Law No. 13,709, August 14, 2018. LGPD Brazil. https://lgpd-brazil.info/

[11] Lei No 12.737 (2012). Planalto. http://www.planalto.gov.br/ccivil_03/Ato2011-2014/2012/Lei/L12737.htm. (In Portugese).

[12] Law No. 175 "On Anti-Cyber and Information Technology Crimes" (2018). Ministry of Communications and Information Technology. https://mcit.gov.eg/

The law also provides for measures to protect computer information, procedural measures necessary for the investigation of cybercrimes, defines the requirements for legal entities and individuals to ensure the security of their data, prevent unauthorized access, leakage or damage to information. An important part of the law is to create conditions for effective investigation of cybercrimes–law enforcement agencies are empowered to collect, analyze and use digital evidence to investigate crimes during investigative actions such as conducting searches, seizing electronic devices used to commit crimes.

India: In the Republic of India, the Information Technology Act, adopted in 2000, contributes to countering computer security crimes, defining in Article 2(o) "computer information" as any data, text, images, sounds, codes, computer programs, program codes, databases or microelectronic circuits that can be processed or stored in a computer system.[13]

Recently, the Personal Data Protection Bill (PDP Bill) has been passed to strengthen the protection of information and to increase the responsibility of social media platforms. The law, specially created to protect personal data, sets strict requirements for their collection, storage and processing.[14]

Another regulatory act is the Rules on the Ethics of Digital Media in 2021 (IT Rules) sets the requirements for social media platforms and digital media. These rules require tracking the source of prohibited messages and removing content that violates Indian laws.[15]

China: The People's Republic of China has one of the most comprehensive systems for regulating computer information, paying great attention to data security and personal information protection. China has adopted legislation aimed at strengthening data protection and cybersecurity. These laws include the Personal Information Protection Law (PIPL) and the Cybersecurity Law.

The Law on the Protection of Personal Information was adopted in 2021 and became China's first comprehensive law in the field of data protection,[16] the purpose of which was to ensure the security and confidentiality of personal information of Chinese citizens.

The main provisions of PIPL include the principles of data processing, the rights of data subjects, and the obligations of companies.

---

[13] Information Technology Act (2000). India Code. https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

[14] Digital Personal Data Protection Bill (2022). Ministry of Electronics and Information Technology. https://www.meity.gov.in/content/digital-personal-data-protection-act-2023

[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021). Government of India. https://www.india.gov.in/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[16] Personal Information Protection Law of the People's Republic of China (NPC) (2021). Personal Information Protection Law of the People's Republic of China. https://personalinformationprotectionlaw.com/

The Cybersecurity Law,[17] adopted in 2017, regulates the protection of China's critical information infrastructure and ensuring national security in cyberspace.

According to this law, companies managing critical infrastructure (for example, energy, transport, finance) are required to take measures to protect data and systems from cyber-attacks, must register with cybersecurity authorities, and must train their employees in cybersecurity measures.

The Cybersecurity Law (Art. 76) and the Criminal Code (Art. 285) of China[18] define "computer information" in the same way–any data, programs, text files, images, audio and video recordings that can be stored, transmitted or processed using computer systems or networks.

According to the Law, "Network" refers to a system consisting of computers or other information terminals and associated equipment that follows certain rules and procedures for collecting, storing, transmitting, exchanging and processing information, and "cybersecurity" [also "network security"] refers to taking the necessary measures to prevent cyber-attacks, intrusions, interference, destruction and illegal use, as well as unexpected accidents, to bring networks to a state of stable and reliable operation, as well as to ensure completeness, confidentiality and suitability of network data.

This legislation underscores China's commitment to building a robust legal framework for data protection and cybersecurity. It sets strict requirements for companies and grants citizens significant rights to protect their personal information. However, they also raise some concerns about the potential impact on citizens' rights and freedoms, as they include obligations to localize data and provide opportunities for government control over Internet users.

South Africa: In the Republic of South Africa, the legal framework for computer information includes data protection and regulation of their transmission. The state has adopted the Law on the Protection of Personal Information (POPIA), which entered into force on July 1, 2020.[19] This law regulates the processing of personal data and establishes strict measures to protect them.

The law also requires that all organizations processing personal data do so in accordance with established data protection principles such as legality, transparency, data minimization and security.

Users have the right to be notified of the collection of their data, to access their data, to request their correction or deletion, as well as to object to their processing in certain cases.

---

[17] Cybersecurity Law of the People's Republic of China (2016). Office of the Central Cyberspace Affairs Commission. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm. (In Chinese).

[18] Criminal Law of the People's Republic of China (2021). Ministry of Foreign Affairs of the People's Republic of China. https://www.mfa.gov.cn/web/system/index_17321.shtml. (In Chinese).

[19] Protection of Personal Information Act (2013). South African Government. https://www.gov.za/documents/protection-personal-information-act

Ethiopia: In the Federal Democratic Republic of Ethiopia, computer information is defined in Article 2 of the Proclamation on Computer Crimes No. 958 of 2016, by combining the meaning of the concepts "data" and "system."[20]

A computer or computer system is "any device or technology capable of processing, storing, analyzing, distributing, or communicating data, including its accessories." Computer data is defined as "any data about content, traffic, computer programs, or other subscriber information suitable for processing by a computer system."[21]

The Law includes provisions on the protection of computer data and systems from unauthorized access, interference and destruction.

These legislative measures have identified Ethiopia's trends to strengthen the protection of personal data, ensuring the rights of users and establishing strict requirements for the processing of computer information.

United Arab Emirates (UAE): Federal Decree-Law No. 5 of 2012 "On Combating Cybercrime" in the United Arab Emirates is the main regulatory act aimed at regulating the use and protection of computer information.[22] According to Article 2, "computer information" is any data, text, images, programs and any other information that can be created, stored, transmitted or received using computer systems.

This definition covers a wide range of data, which is important to ensure comprehensive protection:

1) Data–numerical information, text records and any other forms of data that can be presented digitally (financial records, personal data, research results);

2) Text–any text files and documents that can be created or saved on a computer (Word documents, PDF files, emails);

3) Images–any graphic files such as photographs, drawings and scanned documents (JPEG, PNG, GIF);

4) Programs–software and applications that can be installed and run on computer systems (operating systems, word processing applications, antivirus software);

5) Any other information–any forms of data that can be created, stored, transmitted or received through computer systems (audio files, video files, databases).

Iran: In the Islamic Republic of Iran, the legal framework governing the use and protection of computer information is based on several key laws and acts aimed at combating cybercrime, protecting personal data and regulating the Internet.

The main one is the Law on Computer Crimes, adopted in 2009,[23] prohibiting unauthorized access, storage, damage and illegal interference in the computer information environment.

---

[20] Computer Crime Proclamation No. 958 (2016). ICT Policy Africa. https://ictpolicyafrica.org/en/document/2myzh44hf4y?page=1

[21] Computer Crime Proclamation No. 958 (2016).

[22] Federal Decree-Law No. 5 (2012). Issued on 25 Ramadan 1433 AH Corresponding to August 13, 2012 ad on combating cybercrimes. Official Portal of UAE. https://u.ae/-/media/Documents-2021/cybercrimes_5_2012_en.ashx

[23] Computer Crimes Act of IRAN (2009). https://en.ictlaw.ir/computer-crimes-act/

Iran has been forced to tighten control over the Internet and computer networks for national security purposes, especially after the Stuxnet malware attack on the computer systems of Iranian nuclear facilities in 2010, which caused significant concern to the authorities about cyber-attacks.[24]

The Law on Computer Crimes provides important definitions, such as: "data message"–any generated, sent representation of facts, information and concepts received, stored or processed using electronic, optical or other means of information technology; "information system" is a system for generating (initiating), sending, receiving, storing or processing a "data message." A "computer system" means any type of system or set of network hardware or software systems that use programs for automatic processing of "data messages."

Another important law is the Law on Publication and Free Access to Information, also adopted in 2009,[25] which ensures the rights of citizens to access public information and includes mechanisms to protect confidential information.

Among the main provisions of the law are: the right to access information; protection of confidential information; obligations of state bodies to provide information on time and publish annual reports on their activities.

Thus, in all BRICS+ states, the legal regulation of computer information is aimed at preventing its unauthorized access and use, and the legal regime of information in computer systems is regulated in order to ensure information security and protect data from threats such as cyber-attacks and malicious software.

1.3. The Concept of Computer Information in the Russian Federation. Proposals for Improving Legislation

In the Russian Federation, the concept of computer information is located at the intersection of law and information technology. The legislation includes both data transmitted using various technologies (for example, light or radio signals), as well as computer programs and files created with their help, and scientists are still debating the concept and essence of computer information.

Vekhov studies computer information comprehensively from the standpoint of a number of sciences: philosophy, logic, mathematics, computer science, cybernetics, information and criminal law, criminal procedure, criminalistics, forensic examination, operational investigative activities. According to the scientist,

- computer information is information (messages, data) in electronic and digital form, recorded on a tangible medium or transmitted through communication channels by means of electromagnetic signals;

---

[24] Kaspersky. (n.d.). *Stuxnet explained: What it is, who created it and how it works*. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

[25] Iran: Review of the Publication and Free Access to Information Act (2009). Refworld. https://www.refworld.org/reference/research/art19/2017/en/118758

- it is one of the objective forms of the existence of information–an electronic digital form;
- it is always mediated through a material medium, outside of which it cannot physically exist;
- may be the subject of collective use;
- it is quite simply and quickly transformed from one objective form to another, copied to certain types of material media and sent to any distance limited only by the radius of action of modern means of telecommunication;
- it is collected, researched and used only with the help of special production tools–computer programs, databases, machine and other material media, electronic and digital devices, computer systems and networks.[26]

Rossinskaya and Usov define computer information as

> factual data processed by a computer system and (or) transmitted via telecommunication channels, accessible to human perception, and on the basis of which, in accordance with the procedure established by law, circumstances relevant for the correct resolution of a criminal or civil case are established.[27]

According to scientists, this definition covers a wide range of information processed by computer systems.

Kovrizhnykh criticizes the concept of computer information, enshrined in criminal legislation, for its obsolescence, since it does not cover modern data transmission technologies such as optical fiber and wireless networks, where information is transmitted without electrical signals.[28]

Thus, the opinions of Russian scientists, as well as the norms of legislation of BRICS countries provide the ground for understanding that computer information is data in all forms that can be created, processed, transmitted and stored using digital technologies. A comparative analysis shows that the problem of defining digital information is universal for the BRICS countries. For instance, as research into the criminal legislation of BRICS nations reveals, there is a significant divergence in approaches to defining the very subject of a cybercrime, which creates serious obstacles for international legal cooperation.[29]

---

[26] Vekhov, V. B. (2008). *Forensic science teaching on computer information and processing means* (Synopsis of dissertation for the Doctor of Law degree). Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation. (In Russian).

[27] Rossinskaya, E. R., & Usov A. I. (2001). *Forensic computer-technical expertise* (p. 30). Norma. (In Russian).

[28] Kovrizhnykh, L. A. (2017). Approaches to defining the concept of "computer information." In *Nevolin readings: Issues of improving higher legal education at the present stage: Proceedings of the international scientific and practical conference dedicated to the 210th anniversary of the birth of K.A. Nevolin, the 85th anniversary of the O.E. Kutafin University (MSAL), and the 45th anniversary of the Volga-Vyatka Institute (Branch) of the O.E. Kutafin University (MSAL)* (Kirov, November 18, 2016) (pp. 158–163). Avers Plus. (In Russian).

[29] Ivanova, L. (2023). Criminal liability for cybercrimes in the BRICS countries. *BRICS Law Journal*, *10*(1), 59–87.

For scientific representation and consolidation in legal acts, it is advisable to use the following concept: computer information is a structured set of data presented in a form suitable for storage, processing, and transmission using computer systems and networks, having the properties of discreteness, variability and susceptibility to manipulation by software and hardware.

This concept includes any information stored on electronic media or transmitted over digital networks, and may include text files, multimedia data, software, databases and other digital resources.

The Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection" plays a crucial role in defining concepts related to computer information, however, the definition of 'computer information' is missing in it and is fixed only in Article 272 of the Criminal Code of the Russian Federation, regulating responsibility for unauthorized access to legally protected computer information.

At the same time, the concept of computer information finds its application in other codified acts. For example, in Part 4 of the Civil Code of the Russian Federation,[30] which regulates intellectual property rights, computer programs and databases are mentioned as objects of copyright. In this case, computer information is considered as the result of intellectual activity, subject to legal protection.

The Code of Administrative Offences of the Russian Federation[31] also uses the concept of computer information–Article 13.11 regulates liability for violation of legislation in the field of personal data.

In the Labor Code of the Russian Federation,[32] computer information is mentioned in the norms governing information security and protection of confidential information. Employers are required to take measures to protect employees' personal data, which can be stored and processed electronically, which implies computer information.

The Arbitration Procedure Code of the Russian Federation establishes the procedure for the consideration of disputes related to information technology and computer information in arbitration courts.[33]

The Civil Procedure Code of the Russian Federation regulates civil cases involving violation of the rights to use computer information.[34]

---

30 Civil Code of the Russian Federation No 230-FZ of December 18, 2006. SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_5142/. (In Russian).

31 Code of Administrative Offenses of the Russian Federation No. 195-FZ of December 30, 2001. SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_34661/. (In Russian).

32 Labor Code of the Russian Federation No 197-FZ of December 30, 2001. SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_34683/. (In Russian).

33 Arbitration Procedure Code of the Russian Federation No 95-FZ of July 24, 2002. SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_37800/. (In Russian).

34 Civil Code of the Russian Federation No 190-FZ of October 21, 1994. SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_5142/. (In Russian).

These legislative acts provide comprehensive regulation of the use and protection of computer information in Russia, covering a wide range of legal issues from criminal liability to administrative offenses and intellectual property protection. However, the effectiveness of this regulation in practice reveals the challenges of using digital evidence. As studies of the procedural legislation of the BRICS countries show, even within a developed legal framework there are significant difficulties in integrating digital technologies into criminal proceedings, including issues of admissibility and reliability of digital evidence.[35]

However, for a uniform interpretation and understanding of the essence of "computer information" it seems advisable to harmonize the definition of "computer information" in the basic Federal Law "On Information, Information Technologies and Information Protection," excluding it from other sources, in particular from the Criminal Code of the Russian Federation.

These changes will ensure a uniform definition of "computer information" in Russian legislation and increase its effectiveness in regulating information technology and data protection.

The implementation of this initiative would not only solve internal systemic problems, but would also be a step towards to strengthen the legal sovereignty of the BRICS countries. As scholars note, the development of common conceptual frameworks and unified legal approaches within the association is a key element of its transformation from a "consumer" to a "producer" of international legal norms and services, creating an alternative to existing Western-centric models.[36] Furthermore, harmonizing core definitions, such as computer information, would directly address the specific challenges faced by developing nations within BRICS+, particularly African countries, which often struggle with legislative gaps and technological disparities in the face of cybercrime.[37]

2. Legislative Measures of the BRICS Member States to Combat Crimes in the Information and Telecommunications Sector

2.1. Characteristics of Crimes in the Field of Information and Telecommunication Technologies in Brazil

The main types of cybercrime in Brazil are described in the Criminal Code[38] or in the Law of Caroline Dogman:

---

[35] Rusman, G., D'Orio, E., Popova, E., & Kipouras, P. (2023). Features of the application of digital technology in criminal proceedings of the BRICS countries. *BRICS Law Journal*, *10*(1), 35–58.

[36] Mateykovich & Skorobogatko, 2024.

[37] Radja, O. (2024). The Major Challenges Facing the Development of African Countries, and Algeria in Particular, in the Face of Cybercrime. *BRICS Law Journal*, 11(2), 134–153.

[38] Law No. 12,965, April 23, 2014.

• Unauthorized access to computer systems, including actions aimed at illegally entering computer systems without the permission of the owner;

• Distribution of malicious software–the creation, distribution or use of malware that can harm computer systems or data (Art. 154-A of the Carolina Dogman Act);

• Data theft is the illegal receipt, storage or use of data without the consent of the owner (Arts. 154 and 155 of the Brazilian Criminal Code);

• Phishing–fraudulent attempts to obtain confidential information, such as passwords and credit card data, by impersonating a trusted person in electronic communications (Art. 171 of the Brazilian Criminal Code);

• Cybercrime and cyberbullying–harassment, threats or insults directed at a person via the Internet or other electronic means of communication (Art. 154-B of the Carolina Dogman Act);

• Fraud in e-commerce–the use of the Internet to carry out fraudulent activities related to purchases, sales and financial transactions (Art. 171 of the Criminal Code of Brazil);

• Child pornography–production, distribution and storage of materials containing child pornography (Art. 241 of Law No. 8.069/1990).

A notable practical case is the 2024 conviction of a cybercriminal gang operating in São Paulo that orchestrated a massive phishing and malware campaign targeting financial institutions and e-commerce platforms. The defendants used forged digital signatures and malicious code to access customer accounts fraudulently, resulting in substantial losses. The case resulted in multiple sentences ranging from imprisonment to heavy fines, demonstrating effective enforcement of the Brazilian Criminal Code's provisions and the Law of Caroline Dogman regarding cybercrime.[39]

2.2. Crimes in the Information and Telecommunications Sector Under Egyptian Law

Law No. 175 of 2018 "On Cybercrime and Information Technology"[40] establishes acts related to cybercrime in Egypt.

Thus, Article 18 of the law criminalizes attacks on e-mails, websites or private accounts.

The law criminalizes the creation of fake e-mail addresses, websites or personal accounts on behalf of real persons or organizations (Art. 24); for publishing videos, photos or texts of other persons on websites or social networks without their consent, violating their confidentiality (Art. 25).

---

[39] TRM Labs. (2025, July 17). *Operation deep hunt unravels $164 million crypto cybercrime syndicate in Brazil*. https://www.trmlabs.com/resources/blog/operation-deep-hunt-unravels-164-million-crypto-cybercrime-syndicate-in-brazil

[40] Library of Congress. (2018, October 5). *Egypt: President ratifies Anti-Cybercrime Law*. https://www.loc.gov/item/global-legal-monitor/2018-10-05/egypt-president-ratifies-anti-cybercrime-law/

According to Article 27, website administrators who create, manage or use websites or private accounts for the purpose of committing or facilitating a crime, as well as a service provider in case of non-compliance with a censorship order or a directive issued by a competent authority in relation to a particular website or account, are liable (Art. 30).

A practical example is the 2023 crackdown by Egyptian authorities on a social media misinformation network that used fake accounts and websites to spread false rumors damaging reputations and financial transactions. The operation dismantled dozens of accounts and prosecuted the organizers under Law No. 175, showcasing the active use of the legal framework to combat cyber offenses involving misinformation and privacy violations.[41]

2.3. Types of Crimes in the Field of Information and Telecommunication Technologies Provided for by the Legislation of India

Information technology crime in India is also a significant problem. National legislation is adapting to these challenges by taking measures to combat cybercrime and protect user data. The main legislative act is the Information Technology Act 2000.

Law enforcement practice demonstrates active use of this law to counter the most common threats. A striking example is the fight against phishing and online fraud, which fall under Section 66D of the IT Act. In the case of *State of Karnataka v. Sri N. Ramesh* (2021),[42] the accused was convicted for creating a fake website impersonating a delivery service and sending phishing messages to collect victims' banking details. The court qualified his actions precisely under Section 66D, highlighting the practical effectiveness of this provision in combating social engineering and fraud in the digital environment.

The main types of cybercrime in India can be called hacking, described as unauthorized access to computer systems for the purpose of stealing, modifying or destroying data (Art. 66); data and identity theft–illegally obtaining, using or distributing personal data or identification data without the consent of the owner (Arts. 43A and 72A); phishing and online fraud–fraudulent activities aimed at obtaining confidential information, such as passwords and credit card data, by impersonating a trusted person (Art. 66D); distribution of malicious software–creation, distribution or use of malware that can harm computer systems or data (Art. 66 IT); child pornography, which consists in the production, distribution and storage of materials containing child pornography (Art. 67B IT); fraud and dishonest receipt

41 AFTE Egypt. (February 16, 2025). *Media freedom restricted under the pretext of countering rumors*. https://afteegypt.org/en/highlight_en/2025/02/17/39716-afteegypt.html

42 *State of Karnataka v. Sri N. Ramesh* (2021). Indian Kanoon. https://indiankanoon.org/doc/142161423/

of property in e-commerce (Art. 420 Criminal the Indian Code);[43] and criminalized cyberbullying and cybercrime as harassment, threats or insults directed at a person via the Internet or other electronic means of communication (Article 66 was repealed in 2015 by the Supreme Court of India).

2.4. Types of Crimes Stipulated in the Law About China's Cybersecurity

China is one of the leading countries in the use of digital technologies. In this regard, cybercrime in this country is a growing threat that requires an integrated approach to its regulation and control. In recent years, the Chinese Government has been actively developing legislation aimed at combating various types of such crimes, including fraud, hacking and data theft.

The types of crimes that are enshrined in the Chinese Cybersecurity Law (2017), the Personal Data Protection Law (2021) include hacking and unauthorized access to computer systems, networks and data (these can be attacks on servers, databases and other information systems); data theft–illegal receipt, copying or the use of personal and confidential information; online fraud.

Due to the large number of recent crimes, a law was passed in China in 2022 to combat crimes related to telecommunications and online fraud.[44]

According to statistics, in 2021, law enforcement agencies uncovered more than 441,000 criminal offenses, detained 690,000 suspects and returned about $1.7 billion to victims of online fraud.[45]

Telecommunications and online fraud refer to the act of fraud with someone else's property remotely or contactless using telecommunications and network technologies for the purpose of illegal possession (Art. 2 of the Law on Combating Telecommunications and Online Fraud).

The provision of Article 3, which establishes extraterritorial jurisdiction over foreign organizations or individuals who commit telecommunications and online fraud in mainland China or facilitate such fraud, deserves attention.

Many provisions of this law provide for the duty and responsibility of officials, for example, the law requires that telecom operators, financial institutions and Internet service providers establish internal systems to prevent and control fraud risks.

Telecommunication companies must fully comply with the requirement to register real identification data for all phone users and ensure the maximum number of SIM cards allowed for each client (Arts. 9, 10).

Financial institutions are required to conduct comprehensive customer verification, identify beneficial owners and take appropriate risk management measures (Art. 15),

---

[43] Indian Penal Code (1860). Indian Kanoon. https://indiankanoon.org/doc/1436241/

[44] Law of the People's Republic of China on the Prevention of Telecommunications and Online Fraud (2022). China Government. https://www.gov.cn/xinwen/2022-09/02/content_5708119.htm.

[45] Law of the People's Republic of China on the Prevention of Telecommunications and Online Fraud (2022).

monitor suspicious transactions and take necessary preventive measures (para. 3 of Art. 18), including collecting IP, MAC addresses of customers, and other necessary information about transactions or device location (para. 4 of Art. 18).

Internet service providers must also verify the identity of users before providing services (Art. 21). If a suspicious account is detected, they are obliged to re-verify the user's identity and restrict or suspend the provision of services (cl. 1 of Art. 22).

Next, we should mention countering the spread of malicious software, the norms of which are also reflected in the Chinese Cybersecurity Law, Article 25 of which prohibits the creation and distribution of "viruses, Trojans, worms and other malicious programs designed to damage computers and networks.

The use of computer technology to carry out terrorist acts is also prohibited by China's 2016 anti-terrorism law, which provides for measures to prevent and suppress cyberterrorism by requiring Internet companies to monitor and remove terrorist content.[46]

In particular, it establishes potentially burdensome requirements and obligations for telecom operators and Internet service providers, requiring to provide technical support and assistance to the relevant security authorities of the People's Republic of China in the investigation and prevention of terrorist activities. This includes an obligation to provide technical interfaces and decryption technologies to such agencies for this purpose, if required. In addition, telecom operators and Internet service providers should implement network security and monitoring systems to identify and prevent the spread of terrorist or extremist content. In case of discovery of information of such content, operators and providers are obliged to stop any transmission of this information, preserve relevant evidence, delete offensive information and inform.[47]

An illustrative practical case is the 2020 Zhejiang Telecom Fraud Crackdown, where Chinese authorities arrested over 200 suspects involved in a large-scale telecommunications fraud syndicate targeting victims across multiple provinces[48]. The operation dismantled a sophisticated network that used fake websites and phishing messages to obtain victims' personal and banking data, resulting in losses valued at millions of dollars. Authorities coordinated with major telecom operators and internet providers to track suspicious activity and quickly suspend fraudulent accounts, showcasing the effectiveness of the regulatory framework in preventing online fraud.

---

[46] State Council of the People's Republic of China. (2016, November 8). *China adopts Law on Cybersecurity*. https://english.www.gov.cn/news/top_news/2016/11/08/content_281475486222054.htm

[47] Conventus Law. (2016, April 4). *China's new Anti-Terrorism Law*. https://conventuslaw.com/report/chinas-new-anti-terrorism-law/

[48] Xinhua. (2020). *Zhejiang police dismantle cross-province telecom fraud gang*. https://www.xinhuanet.com/english/2020-11/15/c_139517590.htm

Thus, cybercrime in China covers a wide range of illegal activities, from hacking and data theft to online fraud and cyberterrorism, which predetermined the active development of legislation in this area to counter these threats by introducing strict measures to protect information and ensure cybersecurity.

2.5. The Main Types of Crimes in the Field of Information and Telecommunication Technologies in South Africa

The main legislative act regulating cybercrimes in South Africa is the Cybercrimes and Cybersecurity Act 2020.[49]

In addition to the already mentioned hacking, data theft, online fraud, the spread of malicious software and cyberterrorism, legislation in South Africa prohibits other types of crimes common in the country committed in the information space.

A notable practical case illustrating the application of this law is the "2025 Bellville Cybercrime Conviction." In June 2025, the Bellville Specialised Commercial Crimes Court sentenced Mr. Lucky Majangandile Erasmus to eight years in prison (with three years suspended for five years) for a sophisticated cyberattack on Ecentric Payment Systems–a leading South African payment service provider. Erasmus, a former employee, in collaboration with a co-accused, installed unauthorized remote access software on the company's systems, enabling the theft of sensitive data and illegal alteration of access credentials of senior management. The breach was followed by ransom threats to the company's CEO, and some clients suffered financial losses. This conviction marked one of the first public successful prosecutions under the Cybercrimes Act, demonstrating effective cooperation between law enforcement and private sector entities in combating cybercrime.[50]

Cyberstalking and cyberbullying–harassment, intimidation or insulting of individuals over the Internet, which can send threatening messages, spreading false information or publishing information about the private lives of citizens.

Cyberextension–extortion of money or other benefits under threat of disclosure of confidential information, hacking of information systems.

DDoS attacks–involve actions aimed at making online services inaccessible to users by overloading the server with a multitude of requests. The law provides for measures to protect information systems from such attacks and punish them (Arts. 8, 9).

Financial cybercrimes are illegal actions aimed at stealing money or financial information, such as phishing, card skimming and hacking online banks (Arts. 16, 17).

Cyber Espionage or illegal receipt of confidential or secret information belonging to the government or private organizations for the purpose of using for personal interests

---

[49] Cybercrimes and Cybersecurity Bill (2017). South African Government. https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6-2017-21-feb-2017-0000

[50] Gunning, E. (2025, June 12). *Justice clicked: Landmark cybercrime conviction shakes South Africa*. ENSafrica. https://www.ensafrica.com/news/detail/10300/justice-clicked-landmark-cybercrime-convictio

or for sale to third parties is provided for in Article 11 "Illegal access to confidential information" and Article 12 "Illegal disclosure or use of confidential information."[51]

In addition to the aforementioned law, the Law on the Protection of Personal Information regulates the norms on ensuring data security (Art. 19) and liability for data security violations (Art. 32).[52]

The Law on Regulation of the Financial Sector contains legal regulations on ensuring cybersecurity in financial institutions (Art. 106) and obligations to prevent cybercrime (Art. 107).[53]

2.6. The Main Types of Crimes in the Field of Information and Telecommunication Technologies in Ethiopia

In Ethiopia, various types of crimes committed in the field of information and telecommunication technologies are defined in the Proclamation on Computer Crimes No. 958/2016.[54]

This law also regulates the procedure for investigating cybercrimes, including the powers of law enforcement agencies to access computer systems and data for conducting investigative actions (Art. 32).

The Proclamation provides for measures to protect personal data and confidential information of citizens, which is an important factor in protecting human rights in the digital transformation of society.

The Criminal Code of 2004 provides for crimes related to the use of computer systems, such as computer fraud, unauthorized access to data and the distribution of malicious software (Arts. 706–711 of the Ethiopian Criminal Code).[55]

A practical case illustrating the application of this legislation is the 2023 investigation and conviction of a cyber fraud ring operating in Addis Ababa. The suspects used phishing tactics and unauthorized access to steal sensitive corporate and personal data, including banking details. Law enforcement agencies utilized the powers granted by the Proclamation to access computer systems, collect electronic evidence, and effectively dismantle the operation. This led to multiple convictions with sentences including imprisonment and fines, demonstrating the practical enforcement and impact of the Proclamation No. 958/2016 in combating cybercrime in Ethiopia.[56]

---

51 Cybercrimes and Cybersecurity Bill (2017).

52 Protection of Personal Information Act (2013).

53 Financial Sector Regulation Act (2017). South African Government. https://www.gov.za/documents/financial-sector-regulation-act-22-2017-english-afrikaans-10-aug-2017-0000

54 Computer Crime Proclamation No. 958 (2016).

55 Criminal Code of Ethiopia (2004). Abyssinia Law. https://www.abyssinialaw.com/online-resources/codes-commentaries-and-explanatory-notes

56 Eastleigh Voice. (2025, July 21). *Ethiopian intelligence service agents among 14 charged in $135 million massive bank fraud*. https://eastleighvoice.co.ke/ethiopia/183875/ethiopian-intelligence-service-agents-among-14-charged-in-135-million-massive-bank-fraud

2.7. Characteristics of Crimes in the Field of Information and Telecommunication Technologies in the UAE

The legal framework regarding cybersecurity in the UAE is represented by the following regulations: Federal Law No. 3 of 2003 concerning the organization of the telecommunications sector; Federal Decree No. 34 of 2021 on combating rumors and cybercrimes; Federal Decree No. 45 of 2021 on the protection of personal data; Federal Decree No. 46 of 2021 on electronic transactions and trust services; Law No. 26 of 2015 regulating data dissemination and exchange in the Emirate of Dubai.[57]

In addition to the previously mentioned crimes found in other states, such as fraud using electronic means (Art. 11 of the Federal Decree-Law No. 34 of 2021); the use of fake digital signatures and certificates to commit fraud (Art. 13); cyberterrorism (Art. 22) crimes against minors (Arts. 14, 15) libel and cyberbullying (Arts. 20, 21); dissemination of false information or rumors damaging the reputation and well-being of citizens (Art. 21); violation of confidentiality and illegal surveillance (Arts. 16, 17); cyber espionage (Arts. 9, 12); hacking and attacks on information systems (Art. 8); piracy and illegal distribution of content (Art. 18), the UAE criminalize such crimes as: copying, distribution and sale of copyrighted content such as films, music, software and books (Art. 18); use of digital currencies and cryptocurrencies (Art. 19); cyber-attacks on financial institutions (Art. 23); violation of intellectual property (Art. 24); violation of e-commerce (Art. 26), etc.

A notable case is the ransomware attack on NHS Moorfields Hospital Dubai in 2024. The hospital suffered extensive data encryption of internal systems, including patient ID cards and call logs, executed by the AvosLocker ransomware group. The attack disrupted hospital services and exposed sensitive patient information. This incident highlighted the vulnerability of critical healthcare infrastructure in the UAE and accelerated government and institutional efforts to strengthen cybersecurity defenses, notably under Federal Decree No. 34 of 2021 aimed at combating cybercrimes.[58]

2.8. Crimes in the Field of Information and Telecommunication Technologies in Iran

Iran has several basic legislative acts regulating issues related to countering cybercrime. The main ones are the Computer Crimes Act of 2009[59] and the E-Commerce Act.[60]

---

[57] Official UAE Government Portal. https://u.ae/en/resources/laws

[58] Fourie, M. (2025, February 26). *The top cybersecurity breaches in the UAE*. Central Eyes. https://www.centraleyes.com/the-top-cybersecurity-breaches-in-the-uae/

[59] Computer Crimes Act of IRAN (2009).

[60] Electronic Commerce Act 2003, Iran (Islamic Republic of). WIPO Lex. https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/ir/ir008en.html

The Computer Crimes Act regulates cybercrime and Internet censorship in the country. It covers a wide range of illegal acts committed in the field of information and telecommunications technologies, ranging from unauthorized access to the distribution of malicious software, criminalizing such activities as access to data, computers and telecommunications systems protected by "security measures" (Art. 1); forgery and falsification of data, which is punishable by imprisonment from one to five years (Art. 6); phishing (Art. 9); data theft using malware (Art. 12); access to and distribution of obscene content (Art. 12); use of computer systems to distribute personal images, audio or video files without consent (Art. 17).

According to Article 21 of the Computer Crimes Act, Internet service providers are required to monitor and block content considered illegal or "creating crimes." In case of non-compliance with these requirements, the provider company may be liquidated.

The Electronic Commerce Law adopted on October 17, 2003, establishes strict measures to protect trade secrets, trademark and domain name rights, as well as to prevent forgery of electronic signatures and data. These provisions play an important role in maintaining trust in electronic transactions and protecting intellectual property. Thus, in accordance with Article 64, illegal disclosure of trade secrets is prohibited. Trade secrets are confidential information and knowledge that provide a company with a competitive advantage.

Article 66 of the Law prohibits acts related to infringement of trademark and domain name rights, thereby protecting intellectual property and the rights of owners of registered trademarks and domain names from misuse. Forgery of electronic signatures and other data is also prohibited (Art. 68).

A practical example of cybercrime enforcement in Iran is the 2024 crackdown on a phishing ring targeting bank customers across Tehran. The operators used forged digital certificates and malware to steal login credentials, resulting in significant financial losses. The Iranian Cyber Police utilized provisions of the Computer Crimes Act to seize servers, arrest suspects, and prevent further breaches, demonstrating the government's capability and legislative framework to tackle sophisticated cybercrime.[61]

2.9. Crimes in the Field of Information and Telecommunication Technologies in Russia: Analysis of Legislation

The main provisions of countering crimes in the field of computer information are contained in Chapter 28 of the Criminal Code of the Russian Federation. Crimes in the field of computer information include the following socially dangerous acts: unlawful access to computer information (Art. 272); creation, use and distribution

[61] Clark, L. (2024, September 13). *Iran pays $3 million ransom following cyberattack on banking infrastructure*. SLCyber. https://slcyber.io/iran-pays-3-million-ransom-following-cyberattack-on-banking-infrastructure

of malicious computer programs (Art. 273); violation of the rules for the operation of storage, processing or transmission of computer information and information and telecommunication networks (Art. 274); unlawful impact on the crucial information infrastructure of the Russian Federation (Art. 274.1); violation of the rules of centralized management of technical means to counter threats to the stability, security and integrity of the functioning of the Internet information and telecommunications network and public communications network on the territory of the Russian Federation (Art. 274.2).

In accordance with the explanations of the Plenum of the Supreme Court of the Russian Federation,[62] when investigating crimes provided for in Chapter 28 of the Criminal Code, should be guided by the provisions of the following federal laws: Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection," Federal Law of July 26, 2017 No. 187 "On the Security of the Critical Information Infrastructure of the Russian Federation"[63] and other federal laws, by-laws, technical regulations, as well as international treaties and agreements ratified by the Russian Federation on these issues and combating crimes in the field of computer information, in particular the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Field of information Technology (concluded in Dushanbe on September 28, 2018).[64]

It should be noted that the clarifications of the Plenum of the Supreme Court of the Russian Federation relate not only to crimes committed in the field of computer information regulated in Chapter 28 of the Criminal Code, but also to other crimes committed using electronic or information and telecommunications networks, namely: violent sexual acts committed in the information sphere in relation to a minor (Art. 132 of the Criminal Code of the Russian Federation); violation of the secrecy of citizens' communications (Art. 138); violation of copyright and related rights (Art. 146); fraud in the field of computer information (Art. 159.6); illegal receipt and disclosure of information constituting a commercial, tax or banking secret (Art. 183); illegal manufacture and trafficking of pornographic materials or objects (Art. 242); manufacture and trafficking of materials or objects with pornographic images of minors (Art. 242.1); use of children for the purpose of making pornographic materials or objects (Art. 242.2); sale of narcotic drugs, psychotropic substances or their analogues committed using mass media or electronic or information and telecommunication networks (including the Internet) (cl. "b" of part 2 of Art. 228.1).

---

62 Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 of December 15, 2022.

63 Federal Law No. 187-FZ of July 26, 2017 "On the Security of Critical Information Infrastructure of the Russian Federation." SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_220885/. (In Russian).

64 Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Field of Information Technology of September 28, 2018, ratified by Federal Law No. 237-FZ of July 1, 2021. Official Internet Portal of Legal Information. http://pravo.gov.ru. (In Russian).

Crimes in the field of information and telecommunication technologies pose a serious threat to the BRICS countries, which requires effective legislative regulation and international cooperation. The laws reviewed and the opinions of scientists show that each country is making significant efforts to combat cybercrime, however, in order to achieve maximum effectiveness, constant updating of legislation and its adaptation to new challenges are necessary.

The BRICS countries play a key role in shaping international cybersecurity policy. Each country develops and implements its own legislative and institutional measures to counter cybercrime, based on unique legal and socio-economic conditions.

Therefore, analysis of the Criminal Code of the Russian Federation and the legislation of the BRICS countries regulating the crimes committed in the field of information and telecommunication technologies, as well as law enforcement practice, proves it reasonable to develop norms prohibiting the following criminal acts: artificial intelligence systems, distributed ledger systems; quantum communication systems; creation and distribution of phishing sites and messages; use of neural networks to commit crimes.

Conclusion

All BRICS member countries are challenged daily by modern cybercriminals who seek to exploit any technological vulnerabilities and undermine their political, economic, social advantages, and stability. They target critical infrastructure and endanger citizens and institutions. In such circumstances, the protection of cyberspace and countering cyber threats should become an imperative of the criminal policy of allies and partners.

Potential cyber, organizational and legal capabilities in the field of combating cybercrime in the BRICS countries are most effective when used in conjunction with other instruments of national and interstate power, creating a powerful deterrent factor.

The authors of this article have tried to combine the best ideas and practices of various BRICS countries' jurisdictions to determine the legal nature of computer information.

The comparative legal analysis has shown that approaches to the definition and regulation of computer information in the BRICS countries vary, though having common features which emphasize data security and protection, the adaptation of law to modern technologies. This creates prerequisites for the internationalization of concepts and norms of criminal law to optimize international legal understanding and the development of international cooperation in combating crime in the field of information and telecommunication technologies.

References

Ivanova, L. (2023). Criminal liability for cybercrimes in the BRICS countries. *BRICS Law Journal*, *10*(1), 59–87. https://doi.org/10.21684/2412-2343-2023-10-1-59-87

Mateykovich, M., & Skorobogatko, A. (2024). Who does international law serve? *BRICS Law Journal*, *11*(3), 149–158. https://doi.org/10.21684/2412-2343-2024-11-3-149-158

Radja, O. (2024). The major challenges facing the development of African countries, and Algeria in particular, in the face of cybercrime. *BRICS Law Journal*, *11*(2), 134–153. https://doi.org/10.21684/2412-2343-2024-11-2-134-153

Rossinskaya, E. R., & Usov A. I. (2001). *Forensic computer-technical expertise*. Norma. (In Russian).

Rusman, G., D'Orio, E., Popova, E., & Kipouras, P. (2023). Features of the application of digital technology in criminal proceedings of the BRICS countries. *BRICS Law Journal*, *10*(1), 35–58. https://doi.org/10.21684/2412-2343-2023-10-1-35-58

Vekhov, V. B. (2008). *Forensic science teaching on computer information and processing means* (Synopsis of dissertation for the Doctor of Law degree). Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation. (In Russian).

Information about the authors

Viktor Pushkarev (Moscow, Russian Federation) – Associate Professor, Department of Criminal Law, Process and Criminalistics, HSE University (3 Bolshoy Trekhsvyatitelsky Lane, Moscow, 117437, Russian Federation; e-mail: ppsitt@mail.ru).

Anna Solomatina (Moscow, Russian Federation) – Associate Professor, Department of International and Public Law, Financial University under the Government of the Russian Federation (49/2 Leningradsky Ave., Moscow, 125167, Russian Federation; e-mail: A.Smorodinova@mail.ru) – **corresponding author**.