THE FEATURES OF THE USE OF INFORMATION TECHNOLOGIES IN CRIMINAL PROCEEDINGS IN THE BRICS COUNTRIES

ANNA DMITRIEVA,

South Ural State University (National Research University) (Chelyabinsk, Russia)

SHADI ALSHDAIFAT,

University of Sharjah (Sharjah, United Arab Emirates)

PAVEL PASTUKHOV,

Perm Institute of the Federal Penal Service (Perm, Russia)

https://doi.org/10.21684/2412-2343-2023-10-1-88-108

This article analyzes the information and technological advancements made by the BRICS countries in the field of criminal proceedings, specifically in the process of gathering evidence in criminal investigations. The relevance of the research topic is explained by the widespread proliferation of computer-related crimes and other crimes committed using computer technologies. With the increase in cybercrime, the number of digital traces left behind by criminal activity is also increasing. This calls for the development of a new approach for detecting, recording, erasing and investigating these digital traces. Given the transnational and cross-border nature of cybercrime, it is necessary to pursue a policy of interaction among the law enforcement agencies of the BRICS countries in order to effectively provide legal assistance in criminal cases, preserve the electronic data obtained from users of information and telecommunications systems and transfer the data to interested countries upon request. This will aid in the formation of a regulatory framework for the information technology sector that meets modern challenges and requirements. Additionally, it is critical to borrow best practices in order to harmonize the criminal and criminal procedure legislation of the BRICS countries, as coordinated activities will ensure closer cooperation between the countries in the socio-economic and cultural spheres, allowing for the achievement of greater results in these areas. Furthermore, the article demonstrates a new approach to the study of the comparative legal nature of the various legal systems in the BRICS countries. The conclusion reached

is that the harmonization of criminal procedure systems essentially comes down to the detection of electronic data, the recording of that data in electronic form, the storage of case materials and the submission of those materials to the court in electronic form. The legal consolidation of these steps will make it possible to introduce electronic document management, thereby enabling the optimization of criminal procedure activities, the objective recording of evidentiary information and the assurance of savings in material and procedural costs associated with criminal proceedings.

Keywords: BRICS; criminal procedure; information technology; information technology; harmonization of legislation; electronic document management.

Recommended citation: Anna Dmitrieva et al., *The Features of the Use of Information Technologies in Criminal Proceedings in the BRICS Countries,* 10(1) BRICS Law Journal 88–108 (2023).

Table of Contents

Introduction

The formation of the BRICS economic and geopolitical bloc is dependent on a variety of factors, among which the harmonization of legislation and cooperation in law enforcement activities in the provision of legal assistance in criminal proceedings play an important role. The quality and effectiveness of such interactions are dependent on knowledge of the specific features of the BRICS countries' legislation as well as the specifics of the activities of the various law enforcement agencies in those countries. In this article, we examine the most recent trends in improving the mechanisms of interaction in the field of criminal proceedings through the prism of the introduction of information technologies in the process of gathering evidence in criminal investigations. The relevance of the stated approach is indicated by the

fact that the new class of information technology crimes is transnational and cross-border in nature, capable of nullifying any positive results achieved and destroying any trust built between the countries at the stages of their unification into unions.

The need to develop common standards in law enforcement activities is indicated by the fact that economic disputes will inevitably occur in the BRICS countries and their resolution will require the creation of courts. In this regard, the unification of evidentiary activities in economic disputes and criminal cases becomes inevitable. In a situation where each country uses only its own countermeasures to combat traditional and high-tech crime, the effectiveness of these measures is low.[1] For a more successful fight, it is necessary to study the practices of other states, exchange positive experiences and unite the efforts of law enforcement agencies in the different countries. Only legal cooperation and joint efforts will allow us to resist new technological criminal challenges.

As practice shows, law enforcement agencies still have difficulties collecting electronic evidence when investigating criminal cases, both within the country and even more so when investigating cases that occur outside the country. When investigating criminal cases involving cross-border crimes, traditional mechanisms of cooperation between authorities are prohibitively slow compared to the ability of criminals to use means and methods of anonymization, move almost freely around different countries, repeatedly transfer non-cash funds, convert money into electronic or digital forms and change or hide electronic traces of their crimes.[2] Although it is frequently impossible to obtain electronic evidence from other countries, the existing legal mechanisms of cooperation between states, the sovereignty of the country and the extent and scope of guarantees for the private life of a person in today's criminal situations, are being increasingly criticized. This is particularly the case in situations when it is impossible to establish the circumstances of a crime committed through the information and telecommunications networks of another country.[3]

1. The Features of the Development of Information Technologies in Criminal Proceedings in China

On 7 November 2016, China passed a law known as the Cybersecurity Law in an effort to exercise greater control over the information and telecommunications

---

1 Berna Akcali Gur, *Cybersecurity, European Digital Sovereignty and the 5G Rollout Crisis*, 46 Computer L. & Sec. Rev. (Article 105736) (2022).

2 Albina A. Shutova et al., *Legal Measures for Crimes in the Field of Cryptocurrency Billing*, 7(25) Utopia y Praxis Latinoamericana 270 (2020); Ildar R. Begishev, *Limits of Criminal Law Regulation of Robotics*, 12(3) Vestnik of Saint Petersburg University. Law 522 (2021).

3 Alexandra Yu. Bokovnya et al., *Analysis of Russian Judicial Practice in Cases of Information Security*, 13(12) Int'l J. Engineering Res. & Tech. (Article 4602) (2020); Sergey V. Zuev et al., *Electronic Evidence in Criminal Proceedings* (2021).

environment.[4] According to this law, authorized Chinese government agencies have the right to monitor all content on the Internet that is accessible from within the borders of China. Furthermore, the law stipulates that all published content must be stored within China for at least six months. This applies to written blogs as well as social networks and videos. The law also pays great attention to the system of user identification. In addition to establishing liability for violations of the law, it sets forth general principles and measures to support and develop network security, including supervision, preventive measures and emergency response. This law is designed to ensure network security; protect the sovereignty of cyberspace and national security, defend social and public interests and protect the legitimate rights and interests of citizens, legal entities and other organizations in order to promote the healthy development of informatization of the economy and society as emphasized in the first article of the document.

In early 2021, China adopted several laws to ensure the cybersecurity of the digital space, including the Personal Information Protection Law,[5] the Data Security Law[6] and the Law on Cryptography.[7]

The Anti-Terrorist Act of 2015 obliges telecom operators and Internet service providers to provide backdoors and decryption codes to the authorities, as well as block and take down websites on the Internet without legal proceedings. Telecom operators and providers who violate the provisions of the act are subject to fines ranging from 200,000 to 500,000 yuan (2.3 to 5.8 million rubles).[8]

A brief analysis of the information technology environment of the People's Republic of China (PRC) shows that the state has access to a huge amount of data on their citizens and their life activities, which ultimately affects the collection of information concerning the crimes that are currently under investigation. Although the main goals of China's state policy in cyberspace are stated to be "regulating the national cyberspace" and "striving to find a balance between formal non-interference of the state in cyberspace, legislative protection of personal data turnover and the need to collect and use information about citizens," in practice, there is actually a significant amount of control exerted by the state over its citizens.[9] As a result,

---

4 The Law of the People's Republic of China on Cybersecurity (2016) (Dec. 20, 2022), available at https://www.npc.gov.cn/.

5 The Law on the Protection of Personal Information (the Law on the Protection of Personal Information) (2021) (Dec. 20, 2022), available at https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021.

6 Ella Gorian, *Genesis of Data Security Mechanism in China: The Next Step to Data Nationalism*, 8(2) China & WTO Rev. 255 (2022).

7 The Law of the People's Republic of China on Cryptography (2021) (Dec. 20, 2022), available at https://chinalaw.center/administrative_law/china_cryptography_law_2019_russian/.

8 The Law of the PRC on Combating Terrorism (2021) (Dec. 20, 2022), available at https://www.6laws.net/6law/law-gb/95.htm.

9 *China Passes Controversial New Anti-Terror Laws*, BBC, 28 December 2015 (Dec. 20, 2022), available at http://www.bbc.com/news/world-asia-china-35188137.

Chinese zones have developed information networks that are open to government agencies but closed to outside influence.

Before the adoption of amendments to the Main Criminal Procedure Law of China in 2012, neither the criminal procedure legislation nor the law enforcement agency were prepared to use electronic data as a type of evidence, as the legislation did not provide for regulatory consolidation of the processes of collecting, withdrawing, storing and transmitting information nor did it provide for measures to protect information from copying or modification. As a result, to prevent abuse of investigative powers, proposals were put forward on the need for judicial authorization of the process of collecting, withdrawing and further viewing and copying of electronic data.[10]

Due to the acuteness of the problems that have arisen with the active introduction of audio and video recording tools, as well as the growth of high-tech crimes, the need for legal consolidation and establishing a unified procedure for collecting, analyzing, storing and using electronic data in criminal proceedings has also become increasingly acute. Amendments and additions in 2012 to Article 42 of the Criminal Procedure Code (CPC) of the People's Republic of China establish that evidence in a criminal case is defined as any factual data revealing the true circumstances of the case.[11]

Thus, since the second edition of the Main Criminal Procedure Law of China (2012), "electronic data" has been recognized as evidence, although the criminal procedure law does not disclose this understanding. Several authors have drawn attention to this particular matter.[12] This gap was eliminated by the Regulation of the Supreme People's Court of the PRC, the Supreme People's Prosecutor's Office of the PRC and the Ministry of Public Security of the PRC, titled "On the Resolution of Certain Issues Related to the Collection, Receipt and Analysis of Electronic Data in Criminal Cases." Article 1 of this regulation defines electronic data as follows: "Electronic data – information collected in the framework of a criminal case, stored and transmitted in electronic form, which can serve as evidence in a criminal case."

Initially, the evidentiary value of electronic data was often questioned, and the procedure stipulated in regulatory acts was reasonably criticized. However, at the same time, other scientists, on the contrary, optimistically noted that the era of electronic evidence would soon arrive and that there would be a historical leap in the theory of evidence.[13] The specified list should provide strict rules for the collection of electronic evidence, as well as protection against copying and making changes.

---

[10] Chen Yongsheng, *Legislative Rules for the Use of Electronic Data of Search and Arrest Results*, 36 Modern L. 111 (2014).

[11] Criminal Procedure Code of the People's Republic of China (1979) (Dec. 20, 2022), available at https://asia-business.ru/law/law1/criminal/proceduralaw.

[12] I. Yuan, *Problems of Considering Evidence under the New CPC of the People's Republic of China*, 3 Socio-Pol. Sci. 137, 137–38 (2017).

[13] Jai Dai, *'Wings' of Anti-Corruption Technologies and Information*, Daily Prosecutor's Newspaper, 3 December 2011.

According to Chen Yongsheng, the main reason for not accepting electronic data as evidence in a criminal case is the "variability and inconstancy of form and content" of these types of files. Skeptics believed that the procedure set out in the joint provisions on electronic data is not sufficiently dependable in the storage and protection of electronic information and raises doubts about its authenticity and integrity. Given this, the viewpoint of Dai Shijian and Liu Jingxin as expressed in the book *Guide to the Study of Electronic Evidence* is interesting.[14] They are of the opinion that the procedure for storing electronic data should differ from the procedure for storing other evidence established in Article 50 of the Main Criminal Procedure Law of China.

Due to the special characteristics of the above-mentioned type of evidence, electronic data is collected and extracted by two investigators (Art. 7 of the joint regulation on electronic data). Authorized bodies must comply with the technical standards and legal requirements stipulated in the law when collecting and withdrawing evidence under the threat of its inadmissibility. Therefore, when the original data carrier has been extracted, it is sealed and a transcript of the storage status of the original media is made. It is important that the information be protected using some type of original electronic data carrier as well as by photographing the data. If it is impossible to withdraw the original media and the electronic data contained there, a transcript is made indicating the reasons for the impossibility of withdrawal, the source of electronic data and the location of its storage. Electronic data located outside the territory of China can be extracted via the Internet. At the end of the criminal investigation, the original media or collected electronic data must be transferred together with the case file in a sealed state. In addition, backup copies are sent to the People's Prosecutor's Office and the court. When a criminal case is considered by the People's Prosecutor Office and the People's Court, the collected evidence is analyzed and checked for authenticity, legality and relevance.

Therefore, officially securing electronic data as evidence in China is an important step in combating the growing number of cybercrimes and demonstrating the process of modernizing Chinese legislation. The technical modernization of evidence storage in Chinese criminal proceedings is cutting-edge. In our opinion, China's experience with implementing technical innovations should be of interest to both process scientists and law enforcers.

As a result of information technology development in China since 2014, public security agencies, the People's Prosecutor's Office and the People's Court have developed mechanisms for modernizing and improving criminal procedure procedures, as well as improving the level of law enforcement in general. For instance, using the Internet as a platform, "the Internet Society of China," was successfully able to implement a technology that allows for the reception of reports regarding violations of the law and the emergence of harmful information. Furthermore, in 2016,

[14] Shijian Dai & Jingmin Liu, *Guidelines for the Study of Electronic Evidence* 209 (2014).

the public security authorities of the PRC created an online platform called 'Cyber Police' for receiving reports of violations of the law.[15] The Decision of the Standing Committee of the National People's Congress representatives of 28 December 2000 to ensure security on the Internet, the Criminal Code of China among other laws of China, including "On penalties (penalties) for violations of public order" and "methods of regulation of information of planting the Internet" serve as the platform's legal basis for its operations.[16]

Thus, the first step in the use of information technologies by public security bodies in pre-trial proceedings begins with the fact that when registering a message, application or complaint, a citizen is given a special number, according to which he or she has the right to independently monitor the progress of the audit and decisions made through a computer that is connected to the Internet.[17] As part of the implementation of this procedure, the Chinese legislator has made it possible for the applicant to track the progress of consideration of the submitted application in almost real-time, while at the same time responding to the actions or omissions of authorized officials. Article 2 of section 3 of the Declaration, titled "Improving the Level of Informatization" focuses on alternative ways of notifying applicants and participants in criminal proceedings about the progress of consideration of a crime report and the subsequent progress of the criminal investigation. In order to accomplish this, the legislator proposed using the website of public security agencies, a public WeChat account, as well as computer information terminals located in public security agencies and police stations. Thus, the legislator of the People's Republic of China has made a successful attempt to ensure the implementation of the applicant's right to access information about the progress of consideration of the application adopted by the public security bodies.

The use of modern technologies in the criminal process of the PRC takes place within the context of improving the production of investigative and other procedural actions, as well as the use of technical means of audio and video recording of information.[18] To increase confidence in law enforcement agencies and implement the principles of openness and transparency in criminal procedure, departmental legislation provides for the need to conduct investigative actions using audio and video recording tools. It should be noted that the introduction of video recording of investigative actions has been a priority task of public security agencies and

---

[15] Cyberpolice (Dec. 20, 2022), available at http://www.cyberpolice.cn/wfjb/.

[16] Xuechen Chen & Xinchuchu Gao, *Analysing the EU's Collective Securitisation Moves Towards China*, 2(20) Asia Europe J. 195 (2022).

[17] Explanations of the Ministry of Public Security of the People's Republic of China "On Changing and Improving the Procedure for Initiating a Criminal Case" of 29 December 2015, Official website of the Ministry of Public Security of the People's Republic of China (Dec. 20, 2022), available at http://www.mps.gov.cn/n16/n1237/n1342/n803715/4946200.html.

[18] Dai & Liu 2014, at 209–15.

the People's Prosecutor's Office since 2007.[19] A special report of the Standing Committee of the National People's Congress in 2014 directed the introduction of video recordings of investigative actions that were conducted with the participation of a suspect. The CPC, departmental regulations, Order No. 127 of the Ministry of Public Security "On the Procedural Requirements for the Investigation of Criminal Cases by Public Security Agencies"[20] and the Rules for the Application of the Criminal Procedure Code by the People's Procurator[21] also provide for similar procedures.

The Ministry of Public Security has enacted regulations that provide for the use of video recordings of interrogations of suspects in all criminal cases and expanded the grounds for using video recordings of interrogations to include the following: (a) if the suspect is a minor, or suffers from deafness or blindness and if the investigator or prosecutor has reason to believe that the suspect suffers from a mental disorder; (b) if the investigator has reason to believe that the suspect may abscond from the investigation; (c) if the suspect denies involvement in the crime that has been committed and claims the use of force in the course of the investigations; in such cases, video recordings of the interrogations may be used as a means of defense; (d) if the results of the investigation have garnered a great deal of public response; and (e) other difficult situations.

The Order of the Ministry of Public Security No. 127 and the Regulations of the Supreme People's Prosecutor's Office have established the following mandatory requirements for the production of video and audio recordings: (a) mandatory video recording during the interrogation of the suspect; (b) continuous recording; and (c) mandatory recording of the interrogation.

The Regulations of the Supreme People's Prosecutor's Office provide for the duty of the prosecutor, according to which it is the responsibility of the Prosecutor General to apply and monitor the progress of video and audio recordings of the interrogation of a suspect and the inspection of the scene.

Moreover, departmental regulations provide for the right of an investigator or People's Prosecutor to conduct a video survey of the scene of an accident in "major criminal cases."[22]

---

[19] In 2005, a meeting of representatives of the People's Prosecutor's Office of the provinces of the People's Republic of China was held, at which the phased introduction of video recording of interrogations of suspects was considered. Within the framework of this agreement, by 2007, all interrogations in cases related to the jurisdiction of the People's Prosecutor's Office must be recorded on video or audio of the procedural event.

[20] Order of the Ministry of Public Security of the People's Republic of China No. 127 of 3 December 2012 "On Procedural Requirements for the Investigation of a Criminal Case by Public Security Bodies."

[21] The Regulation of the Supreme People's Prosecutor's Office "Rules for the Application of the Norms of the Criminal Procedure Code by the People's Prosecutor's Office of the People's Republic of China."

[22] Under these types of criminal cases, the legislator understands the infliction of serious harm to the health or death of the victim, crimes related to a serious violation of civil rights, the commission of a crime as part of an organized group and crimes related to illicit trafficking in narcotic substances and their sale (Art. 203 of the Order of the Ministry of Public Security No. 127).

The prosecutor in cases investigated by public security agencies has the right, as part of their oversight activities, to view a video recording of any investigative action and question its results based on the revealed shortcomings of the viewed video recording of the procedural event.

The use of video recordings of investigative actions in criminal proceedings is aimed not only at finding accusatory but also exculpatory evidence. Thus, the ruling of the Supreme People's Court of China mandated that the investigator and prosecutor be required to hand over copies of the interrogations of suspects to lawyers upon request. Furthermore, it was made clear by the Guangdong Provincial Supreme People's Court that both the prosecutor and the lawyer have the right to use the obtained audio and video recordings as evidence. The disclosure of such information cannot be considered a violation of the confidentiality of the investigation; hence, the lawyer's ability to use this right cannot be restricted in any way.[23]

The issue of the legal status of video recordings of investigative actions as evidence is controversial among Chinese procedural specialists. For instance, Jia Jihong considers the use of video recording as a way to objectively reflect the evidence base in a criminal case and the first step towards building an adversarial process at the stage of preliminary investigation.[24] The results of investigative actions conducted with video recordings have been used as evidence in China since 1997.

We agree with the opinion that a video recording objectively documents the course and results of an investigation, and when it is freely provided to the defense party in response to a request made by that party, it serves as an additional guarantee for the protection of the constitutional rights of the individual involved in criminal proceedings. It also places an additional barrier to the use of illegal violent methods of collecting evidence during the preliminary investigation,[25] in terms of spreading false information about torture, beatings and human rights violations during criminal proceedings using replication through foreign human rights foundations and opposition media.

In the current scientific understanding of the criminal process in China, the use of technological means is considered one of the types of investigative actions that apply modern scientific knowledge and the most cutting-edge technological methods of investigating crimes.

---

[23] Chongyi Fan & Siyuan Li, *On the Rules of Using Electronic Evidence in Criminal Proceedings in China* (Dec. 20, 2022), available at http://www.ahxb.cn/c/3/2016-02-01/2536.html; The Supreme Court is Right, Guangdong, Explanation No. 324 of 2013 "On the Possibility of Lawyers Copying the Video Recording of the Suspect's Interrogation" (Dec. 20, 2022), available at http://www.360doc.com/content/14/1119/21/12424821_426512603.shtml.

[24] Yuan 2017; J. Jiang, *Legal Status of Video and Audio Recordings During the Investigation of a Criminal Case* (Dec. 20, 2022), available at http://www.lawtime.cn/article/lll1141064611141115550o385150.

[25] For more information, *see Леонтьев А.В.* О проблемах эффективности защиты прав человека при проверке заявлений о пытках // СПС «Гарант» [Alexander V. Leontiev, *On the Problems of the Effectiveness of Human Rights Protection when Verifying Allegations of Torture*, Garant] (Dec. 20, 2022), available at https://base.garant.ru/57600211/.

The Order of the Ministry of Public Security No. 127 in Article 254 supplemented the list of grounds for carrying out these activities to include the following: (a) premeditated murder, intentional infliction of harm to health, serious violent crimes, sexual crimes, robberies, kidnappings, arson and explosions; (b) serious interregional crimes; (c) major criminal cases in the field of telecommunications, computer networks and other communication channels; (d) other serious crimes for which the sanction of the article provides for more than seven years of imprisonment.

According to the position held by the Supreme People's Prosecutor's Office, the following may also serve as grounds: (a) the commission of official crimes (for example, embezzlement), when the damage caused is estimated at more than 100,000 yuan; (b) the commission of crimes included in section 7 of the Criminal Code of China, such as bribery, commercial bribery and official crimes committed using official position; and (c) crimes that violate the constitutional rights of citizens or have a profound impact on the rights of citizens (Art. 263 of the Regulations of the Supreme People's Prosecutor's Office).

Because the implementation of technical and investigative measures involves a wide range of actions that restrict the constitutional rights of citizens, Chinese legislation provides a mechanism for monitoring and authorizing this type of investigative action. As a result, if it is necessary to conduct these activities, the investigator must apply for their production. The investigator submits a report to the responsible head of the public security body, who issues a resolution authorizing the implementation of technical and investigative measures, which is forwarded to the special department that handles these types of investigative actions (Arts. 255–256 of the Order of the Ministry of Public Security). Thus, the types of investigative actions that are named by the Supreme People's Prosecutor's Office are conducted at the approved request of the prosecutor and transferred to the department of technical and investigative measures of the public security bodies for production (Art. 268 of the Regulations of the Supreme People's Prosecutor's Office).

With the advancement of computer technologies, the method of considering criminal cases online is increasingly preferred. Currently, a prototype Internet court with the ability to accept applications online and consider criminal cases based on their merits is being introduced in several regions of China. This technical capability allows a court session to be held even when the suspect is detained in the detention center of the district department of the public security body. Even though the first time a criminal case was considered on its merits in an online court format occurred back in 2008 in Shanghai, there are still many restrictions. For example, in Zhejiang Province, it is stated that only pilot courts (the courts participating in the experiment) are allowed to consider online applications, while in Shanghai, the possibility of submitting applications for consideration online in civil and commercial cases is limited. It should be noted that court sessions for online consideration of

criminal cases are significantly less frequent than civil cases.[26,27] In our opinion, such a preponderance is related to the need for ensuring the interests of entrepreneurship in the PRC and, at the same time, the need for prompt responses to offenses in this area. Nevertheless, there is confidence in the subsequent expansion of the scope of application of online criminal courts.

Modern societal demands and trends in the development of Chinese legislation necessitate a flexible approach to the use of modern information technologies and communications by Chinese law enforcement agencies. For example, since 2015, public security agencies and the People's Prosecutor's Office have been actively implementing the Internet Plus program. In a broad sense, this program refers to the practice of introducing Internet technologies in the development of economic, social and other types of state activities, providing a broad platform for introducing various innovations and reforming the activities of state bodies. This social structure provides opportunities for optimizing and integrating the Internet in the distribution of social resources, thereby introducing the results of innovations in the economic and social spheres.

In the field of Chinese criminal procedure, there are opinions regarding the creation of a single platform for investigating criminal cases that would be based on modern software and designed to automate several procedural actions.[28] It is assumed that even after these reforms, the criminal investigation process will be electronic.

At the same time, the People's Prosecutor's Office also performs several supervisory functions within the framework of the project "Internet and Prosecutor's Office." To combat cybercrime, this platform summarizes information available in the databases of prosecutor's offices, conducts active explanatory work, provides legal and news information, as well as conducts activities to receive and consider complaints and applications from citizens and inform the participants in criminal proceedings, their representatives and defenders about the progress of the investigation of a criminal case.[29]

The Preventive Response Commission makes extensive use of information technology in the preventative efforts of all law enforcement agencies. Public security

---

[26] After consideration of civil cases, thanks to the China information online system, all information is sent to a single Internet platform. In addition, this platform allows you to transmit information about the trial process to the parties, their legal representatives, and defenders by mobile phones, by sending voice messages, as well as emails (Art. 3 of the Regulations of the Supreme People's Court on the consideration of cases by Internet Courts). In addition, since 2019, the Chinese government and the Supreme People's Court have been implementing a 5-year pilot program "Mobile Micro Court," which will expand the geography of online courts to 12 Chinese provinces.

[27] The Impact of the Internet on the Culture of Criminal Justice (Dec. 20, 2022), available at http://www.doc88.com/p1146988046898.html.

[28] *Id.*

[29] The Internet and the Prosecutor's Office – research and results (2016) (Dec. 20, 2022), available at http://newspaper.jcrb.com/html/2016-01/13/content_204512.htm.

agencies that have a wide range of powers to conduct operational-investigative, administrative-jurisdictional, criminal-procedural and other types of activities to combat crimes, using various services, instant messengers, social networks, mobile applications and other convenient interfaces, participate when organizing preventive work with citizens.

2. The Features of the Development of Information Technologies in Criminal Proceedings in India

The concept of evidence is enshrined in the first article of the Indian Evidence Act).[30] According to the first part of this article, oral evidence is "all statements that the court authorizes or requires to be made before it by witnesses about the facts under investigation." The second part of the article is aimed at defining documentary evidence and defines it as "all documents, including electronic records, submitted for verification with a court." Initially, the concept of electronic evidence was given in Article 96 of the Information Technology Act (ITA), Article 65B).[31] According to this definition, "electronic evidence" refers to any evidentiary information that is either stored or transmitted electronically and includes computer evidence, digital audio, digital video, cell phones and digital fax machines.

Additionally, the growth of cyberterrorism was linked to changes in the legislation. Recognizing "cyberterrorism" as a particularly dangerous crime that encroaches on the unity, integrity, security or sovereignty of the nation through unauthorized access or distribution of malicious software, legislators have imposed sanctions in the form of life imprisonment for those convicted of this crime (Art. 69F of the ITA). To combat cybercrime, the ITA has established the Indian Computer Emergency Response Team (CERT-India) and describes its functions, all of which are designed to ensure security in cyberspace. Any service provider, intermediary, data center, legal entity or individual is required to provide the CERT-India with information upon request. In the event of failure to provide information, the service provider, legal entity or individual is liable for imprisonment for up to one year or a fine. Moreover, government agencies are empowered to issue orders to intercept, monitor and decrypt any information generated, transmitted, received or stored on any computer resources. Legal obligations and guarantees related to such actions of the State are also established.

In October 2019, the Government of India announced the launch of the world's largest facial recognition system. It is anticipated that in the future, the police of 29 states of the country and seven union territories will have access to a single

---

[30] Indian Evidence Act, 1872 (Dec. 20, 2022), available at https://www.indiacode.nic.in/handle/123456789/2188?sam_handle=123456789/1362.

[31] The Information Technology Act, 2000 (Act No. 21 of 2000) (Dec. 20, 2022), available at https://wipolex.wipo.int/ru/text/185999.

centralized database, which will facilitate the search for criminals and missing people.[32] The scope of the proposed system is described in a document published by the National Crime Registration Bureau. It is expected that the facial recognition system will be able to match images obtained from a growing network of surveillance cameras with a database that will include photos of criminals, as well as passport photos and other images of average citizens collected by various government systems, including "Aadhaar."

The National Cybersecurity Policy, which was approved by the Government of India in July 2013, is the first Indian doctrinal document that aims to provide a comprehensive and unified vision of the policy priorities of the Indian state, private sector and society at large regarding cybersecurity.[33] CERT-India is an organization that operates to create systems for the early detection of threats, the management of vulnerabilities and the response to threats. Additionally, the National Critical Information Infrastructure Protection Center (NCIIPC) was created in order to protect the nation's critical infrastructure.[34]

The mission of the NCIIPC is to take the necessary measures to help protect critical information infrastructure from unauthorized access, exposure, use, disclosure, destruction, disruption of functionality and interaction as well as to increase the information security of all stakeholders.

Furthermore, the Digital India program which provides for the creation of an e-government infrastructure, electronic document management and all other digital services for providing services to the population in electronic form, has been in operation since 2006.

As a result, there is a system of regulatory legal acts in India, regulating various areas of information technology, including the turnover of content, the use of social networks and instant messengers, personal data, electronic signatures, Internet cafe activities etc. Strategic documents on cybersecurity and protection against cyber threats have been adopted. India also has a history of massive restrictions on Internet access. Close attention should be paid to the new mechanisms for regulating content on the Internet proposed by the Government of India in October 2019. In order to implement these mechanisms, changes have been proposed to the information technology rules concerning rules for intermediaries. The main purpose of these changes is to increase the level of responsibility that intermediaries have for the content that is posted while still ensuring its transparency.

---

[32] Julie Zaugg, *India is trying to build the world's biggest facial recognition system*, CNN, 18 October 2019 (Dec. 20, 2022), available at https://edition.cnn.com/2019/10/17/tech/india-facial-recognition-in-tl-hnk/index.html.

[33] Sankalp Gurjar, *India's Cybersecurity: A Look at Approach and Readiness*, Indian Council of World Affairs, 15 July 2021 (Aug. 13, 2022) (Dec. 20, 2022), available at https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=6172&lid=4236.

[34] NIC-CERT, Government of India (Dec. 20, 2022), available at https://nic-cert.nic.in/.

Active reform of the Indian criminal justice system in terms of introducing electronic document management began in 2005, when the Electronic Committee for the Introduction of Information and Communication Technologies in the Judicial System was established.[35] The E-Committee is the governing body charged with overseeing the e-Courts project developed under the "National Policy and Action Plan for the Introduction of Information and Communication Technologies (ICT) in the Indian Judicial System-2005." E-Courts is a pan-Indian project that is overseen and funded by the Ministry of Justice, the Ministry of Law, and the Ministry of Justice of the Government of India. Its vision is to transform the country's judicial system by using ICTs in the courts.

In May 2005, the e-Committee submitted a report on the strategic plan for the implementation of information and communication technologies in the Indian judicial system. The e-Committee developed this national policy as well as the action plan for its implementation based on input received from ICT decision-makers regarding organizations, service providers, R & D experts and leading manufacturers with expertise in various areas relevant to managing change in the Indian judicial system. The timeframe for implementation was five years from the date of the law's entry into force.[36]

Three stages of implementation of the planned goals were identified in the strategic plan for the introduction of information and communication technologies. During the first phase of the e-Courts project, the majority of courts have developed computational tools for providing court services as well as software for collecting case information, and many district courts have launched their websites.

In the second phase, which has been ongoing since 2014, the main goals provided for in the action plan for this stage have been implemented[37] with the announcement that each court and each judicial official has been provided with unique identification numbers (UIDs) and an information system for case management (Case Information Software, CIS) has been developed and implemented[38] for automation and record keeping, minimization of manual work, scanning and digitization of case reports, automation of court archives, computerization of court libraries, and video conferences for all courts with all law enforcement agencies and correctional institutions.

According to its functional purpose, the Case Information System software in version 3.0 provides a digital form for the long-awaited electronic document flow

---

35 The E-Committee, Supreme Court of India (Dec. 20, 2022), available at https://ecommitteesci.gov.in/.

36 National Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary (Dec. 20, 2022), available at https://main.sci.gov.in/pdf/ecommittee/action-plan-ecourt.pdf.

37 Policy and Action Plan Document Phase II (Dec. 20, 2022), available at https://cdnbbsr.s3waas.gov.in/s388ef51f0bf911e452e8dbb1d807a81ab/uploads/2020/05/2020053169.pdf.

38 Case Management through CIS 3.0 (Dec. 20, 2022), available at https://cdnbbsr.s3waas.gov.in/s388ef51f0bf911e452e8dbb1d807a81ab/uploads/2020/08/2020082670.pdf.

in court cases; electronic payment and electronic processing; a registration counter for the parties to the case; and the ability to track one's case 24 hours a day, 7 days a week.

In 2021, a draft of the third phase of e-Courts was prepared, which states that the infrastructure for the judicial system would be digitized and that there would be provisions made for the digitalization of paper processes. In the third phase, an "ecosystem approach" that supports scale, speed and sustainability was put into operation. Moreover, it is important to note that in October 2016, the Government of the Russian Federation and the Government of the Republic of India signed an agreement on cooperation in the field of security in the use of information and communication technologies.[39]

3. The Features of the Development of Information Technologies in Criminal Proceedings in South Africa

The government of South Africa has developed an adversarial system of criminal justice that was borrowed from England, even though the jury trial was abolished in 1969. The source of criminal procedure law in South Africa is the Criminal Procedure Act (1955 and 1977).[40] According to the Act, criminal proceedings can be divided into three stages or phases: namely, pre-trial, trial and post-trial.

South African evidentiary law consists of general and statutory law.[41] Currently, the South African Evidence Regulation Survey has been moved to the constitutional level. Article 35(5) of the Constitution of South Africa states that evidence obtained in violation of the Bill of Rights should be excluded if the admission of such evidence makes the trial unfair or otherwise prejudices the administration of justice. Therefore, these constitutional provisions apply to the admissibility of electronic evidence.

According to Article 210 of the South African Code of Criminal Procedure, the concept of evidence is revealed through its relevance:

> No evidence about any fact, question or thing can be accepted if it is not relevant or insignificant and which cannot serve as proof or refutation of any point or fact considered in criminal proceedings.[42]

---

[39] Agreement between the Government of the Russian Federation and the Government of the Republic of India "On Cooperation in the Field of Security in the Use of Information and Communication Technologies," Electronic Fund of Legal and Regulatory Technical Documents (Dec. 20, 2022), available at https://docs.cntd.ru/document/420384231.

[40] Criminal Procedure Act 51, 1977 (Dec. 20, 2022), available at http://www.mangaung.co.za/wp-content/uploads/2014/11/Criminal-Procedure-Act.pdf.

[41] Raymond Steenkamp Fonseca & Jo-Ansie van Wyk, *Cybersecurity in South Africa: Status, Governance, and Prospects*, 4 Routledge Companion to Global Cyber-Security Strategy 591 (2021).

[42] Criminal Procedure Act 51, 1977 (Dec. 20, 2022), available at http://www.mangaung.co.za/wp-content/uploads/2014/11/Criminal-Procedure-Act.pdf.

The Code of Criminal Procedure does not explicitly contain the "electronic" attribute when defining the concept of "proof." Articles 236 and 236A specify that the concept of "document" includes a record or decrypted computer printout created using any mechanical or electronic device, as well as any device with which information is recorded or stored.

The legislative solution to most issues concerning electronic evidence was established in the Law on Electronic Communications and Transactions No. 25 of 2002 year.[43] Article 15 of the third chapter of the Law proclaims the admissibility and evidentiary value of messages and data as electronic evidence, defining them as "generated, created, sent, received, or stored with electronic means." The first part of Article 15 stipulates that messages (data) should not be rejected as evidence in the process of proof in any judicial proceeding solely because they are electronic messages (data) or because they are not in their original form.

The second point requires further explanation. In the Anglo-Saxon system of evidentiary law, the rule of the best evidence applies, according to which in any evidentiary information, the primary source (original form) containing data about the fact is of primary importance. Therefore, this law establishes that the electronic presentation of electronic information will not be considered a violation of the "best evidence rule" because it no longer exists in its original form.[44] It is argued that data obtained electronically will not be subject to special requirements and that the usual standards of admissibility and evidentiary requirements will apply.

One of the debatable questions is whether a data message is a document or an object (real evidence). The resolution of this issue in South Africa, as a representative of the Anglo-Saxon legal system, is of fundamental importance because it depends on whether they are acceptable or unacceptable as real evidence under the "hearsay" doctrine. According to this doctrine, evidence created or perceived by a person must be presented in court by that person. Therefore, the evidence is examined in court as tangible objects by the parties themselves or by knowledgeable people who have been invited to the hearing. As a result, messages (data) can be admissible as real evidence if they are generated by a computer, and their evidentiary value depends on the operation of the computer. However, communications (data) are considered documents if their evidentiary value depends on the individual. Due to the fact that some data messages may have the characteristics of both real and documentary evidence, it can be difficult to distinguish whether a data message is real evidence or documentary evidence.

---

[43] The South African legislator uses the terms "data message" or "data" taken from the 1996 UN Model Law, Electronic Communications and Transactions Act, 2002 (Dec. 20, 2022), available at https//www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

[44] Beverley Townsend, *The Lawful Sharing of Health Research Data in South Africa and Beyond*, 1(31) Info. & Comm. Tech. L. 17 (2022).

To regulate the interception of certain communications, control certain signals and radio frequency spectra, and establish procedures for issuing orders authorizing the interception of communications and the provision of information to law enforcement agencies, South Africa has adopted a law called the Regulation of Interception of Communications and the Provision of Communication-related Information Act.[45] This law provides for the creation of centers for listening, intercepting messages and other issues of interaction with Internet service providers.

Furthermore, Chapter 9 of the Act provides for the use of information received from information and telecommunications networks as evidence in criminal proceedings. Article 47 of this chapter stipulates that information regarding the commission of a criminal offense obtained through any wiretapping, or the provision of any real-time information or archival information related to communications by this law or any other similar law in another country, may be admissible as evidence in criminal or civil proceedings.

The legal basis for allowing the use of intercepted information as evidence in criminal or civil proceedings is the written permission of the National Director or any member of the Prosecutor's Office who is authorized to do so in writing by the National Director. In accordance with the established procedure, the judge and regional magistrate review the application and issue an order authorizing the receipt of data from information and telecommunications networks.

4. The Features of the Development of Information Technologies in Criminal Proceedings in Brazil

The use of information technology in criminal proceedings in Brazil is the responsibility of the police, which consists of three branches: the Brazilian Federal Police, the Federal Traffic Police and the National Forces.[46] The powers of the Brazilian Federal Police are enshrined in the Brazilian Constitution, which highlights the importance of its legal status and the legal protections afforded under the law in the context of an acute confrontation in the fight against crime. The first paragraph of Article 144 of the Constitution establishes the powers of the Federal Police to investigate criminal offenses in various fields, including cybercrime.

The second section of the Brazilian Code of Criminal Procedure provides an explanation of the nature of police investigations.[47] As stipulated in that section, the police must go to the scene of the crime and ensure that the condition and safety of

---

45 The Law on Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002 (Dec. 20, 2022), available at https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13.

46 Polícia Federal (Dec. 20, 2022), available at https://www.gov.br/pf/pt-br.

47 The Criminal Procedure Code of Brazil, Law No. 3689 of 3 October 1941 (Dec. 20, 2022), available at https://wipolex.wipo.int/ru/text/503944.

the situation at the crime scene do not change before the arrival of criminologists. Furthermore, the police must also seize items related to the case after the crime scene has been examined and evidence taken by forensic experts, collect all evidence that serves to clarify the facts and circumstances of the case, and take statements from the injured party and from the accused in order to identify and classify the people and things involved in the crime. Additionally, the police must conduct interviews, appoint and conduct forensic examinations, and fingerprint and attach the biographical data of the accused to the protocol.

In Brazil, the use of information technologies in criminal proceedings includes eavesdropping on telephone conversations of any nature for the purpose of criminal investigations, as set out in the Law of 1996 on the interception of computer data.[48] According to Article 3 of this law, permission to eavesdrop on telephone conversations is granted by a judge at the request of a police body or a representative of the Ministry of Public Security. A request for wiretapping should contain an explanation that its implementation is necessary for the investigation of a criminal offense, indicating the means to be used. The judge typically rules on the request within a maximum of twenty-four hours.

In accordance with section 4 of the Code of Criminal Procedure, a competent police authority may request, on the basis of a court order, that companies providing telecommunications or telemetric services immediately provide the appropriate technical means, signal user information and other data necessary to determine the location of the victim or suspects.

If necessary, for the prevention and suppression of crimes related to trafficking in persons, the representative of the Ministry of Public Security or the Chief of Police, with the approval of the court, may require companies providing telecommunications or telematics services to immediately provide appropriate technical means or technical information in the form of radio signals that make it possible to determine the location of the victim or the person suspected of committing a crime. A radio signal refers to the location of a coverage station, its division into sectors and the intensity of radio frequencies.

The most profound changes in the Brazilian criminal procedure legislation in the field of information technology application occurred in 2019 with the adoption of Law No. 13964 of 24 December 2019,[49] which was designed to improve criminal rights and criminal procedure. Articles 8A and 10A of this law establish the right of the police to receive electromagnetic, optical or acoustic signals from the information technology environment with the sanction of a judge at the request of the police or the Prosecutor's Office.

---

[48] Acts against the Confidentiality, Integrity and Availability of Computer, Data and Systems, Interception of Computer Data (Dec. 20, 2022), available at http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm.

[49] Law No. 13964 of 24 December 2019 (Dec. 20, 2022), available at https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm.

An entire section of the 2019 Law is devoted to the implementation of operational search activities, the confidential cooperation of citizens with police agencies and the recording of information using information technologies. It is required by paragraph 13 to record negotiations and acts of cooperation using magnetic, digital or similar equipment, including audiovisual equipment, designed to obtain more reliable information, with a copy of the recorded material as a guarantee.

At the conclusion of the activities related to the operation, a detailed report, together with all electronic actions performed during the operation, must be recorded, recorded, stored and submitted to the competent judge (sec. 5). Registered electronic actions should be collected in separate protocols and attached to the criminal process along with the police investigation, which will ensure that the identities of the undercover police agent and those involved in the investigation are preserved.

Conclusion

This study of the legislation and practices of the BRICS countries shows that the introduction of Internet technologies into the process of criminal investigations is one of the most important areas for improving the effectiveness of the work done by preliminary investigation bodies and courts. In the context of the transformation of society and the technologization of crime, state policy in the BRICS countries is aimed at digitizing criminal procedure activities for the purpose of collecting evidence, as well as implementing the state concept of administering justice through the Internet. The state policy of these countries on the use of information technologies is implemented through the legislative consolidation of the ability to collect electronic data as part of the process of gathering evidence, record that data in electronic form and submit the criminal case materials to the court in electronic form.

Through the creation of Internet platforms, efforts are being made to automate the process of investigating criminal cases and to develop unified systems for collecting, storing, processing and exchanging evidence in electronic form. In the example of the BRICS countries, we observe constant modernization of the processes of implementation of both criminal procedure and all law enforcement activities, which allows us to recognize the prospects for practical application and, to a certain extent, the need to borrow the latest Internet technologies used in these countries in the criminal process of other countries.

In terms of technology, China is the closest to the new information technology regime in the data society. China can change the way that information technology and information analysis support crime investigation, moving away from documents and towards using data, while also simplifying the procedural form of criminal proceedings, which establishes the written nature of the proceedings in the case. The most interesting aspect of this development is the movement of China towards

the practical use of Internet platforms and cloud storage facilities designed for the exchange of data and procedural documents between investigative bodies and the court. In our opinion, these funds significantly reduce bureaucratic obstacles and unnecessary document flow, which allows investigators and prosecutors to focus directly on the investigation of criminal cases.

The electronic form of criminal case materials ensures the implementation of the applicant's right to prompt access to information and serves as an additional guarantee for the protection of the constitutional rights of the individual involved in criminal proceedings.

However, this is not spelled out in the laws of all countries, and the practice is followed ambiguously. At the same time, it is important to distinguish electronic data from audiovisual data. Another issue that is problematic for all of the countries is the use of data that is still publicly available on the Internet as evidence in instances when its source cannot be removed. In many cases, it is necessary to find a reasonable balance between electronic evidence and traditional types of evidence. At the same time, the participation of the court in obtaining permission for the seizure of technical devices is noted (for example, according to Art. 99 of the Criminal Procedure Code of Japan). This takes into account the interests of the owner or custodians of the seized items. A forensic computer-technical examination may be ordered and performed with respect to seized technical devices, program code or information in digital form.

Information technologies are being used in a wide range of criminal activities, in particular, cybercrime, and thus, the importance of using information technologies in criminal proceedings will only continue to increase. At the same time, there will be a growing need for closer cooperation between the law enforcement agencies of the BRICS countries and the law enforcement agencies of other countries.

References

Akcali Gur B. *Cybersecurity, European Digital Sovereignty and the 5G Rollout Crisis*, 46 Computer Law & Security Review (Article 105736) (2022). https://doi.org/10.1016/j.clsr.2022.105736

Begishev I.R. *Limits of Criminal Law Regulation of Robotics*, 12(3) Vestnik of Saint Petersburg University. Law 522 (2021). https://doi.org/10.21638/spbu14.2021.303

Bokovnya A.Yu. et al. *Analysis of Russian Judicial Practice in Cases of Information Security*, 13(12) International Journal of Engineering Research and Technology (Article 4602) (2020).

Chen X. & Gao X. *Analysing the EU's Collective Securitisation Moves Towards China*, 2(20) Asia Europe Journal 195 (2022). https://doi.org/10.1007/s10308-021-00640-4

Chen Yu. *Legal Rules for the Use of Electronic Search and Arrest Data*, 36(5) Modern Law 111 (2014).

Dai Sh. & Liu J. *Guidelines for the Study of Electronic Evidence* (2014).

Fan Ch. & Li S. *On the Rules of Using Electronic Evidence in Criminal Proceedings in China* (2016).

Fonseca R.S. & van Wyk J.-A. *Cybersecurity in South Africa: Status, Governance, and Prospects*, 4 Routledge Companion to Global Cyber-Security Strategy 591 (2021). https://doi.org/10.4324/9780429399718-50

Gorian E. *Genesis of Data Security Mechanism in China: The Next Step to Data Nationalism*, 8(2) China and WTO Review 255 (2022). https://doi.org/10.14330/cwr.2022.8.2.02

Shutova A.A. et al. *Legal Measures for Crimes in the Field of Cryptocurrency Billing*, 7(25) Utopia y Praxis Latinoamericana 270 (2020).

Townsend B. *The Lawful Sharing of Health Research Data in South Africa and Beyond*, 1(31) Information and Communications Technology Law 17 (2022). https://doi.org/10.1080/13600834.2021.1918905

Yuan I. *Problems of Considering Evidence under the New CPC of the People's Republic of China*, 3 Socio-Political Sciences 137 (2017).

Information about the authors

Anna Dmitrieva (Chelyabinsk, Russia) – Head, Department of Criminal and Penitentiary Law, Criminology, South Ural State University (National Research University) (87 Lenina Ave., Chelyabinsk, 454080, Russia; e-mail: dmitrievaaa@susu.ru).

Shadi Alshdaifat (Sharjah, UAE) – Associate Professor of Public International Law, College of Law, University of Sharjah (e-mail: salshdaifat@sharjah.ac.ae).

Pavel Pastukhov (Perm, Russia) – Professor of Criminal Procedure and Criminalistics, Perm State University; Professor of Public Law, Faculty of Extra Budgetary Education, Perm Institute of the Federal Penal Service of Russia (1 Bukireva St., Perm, 614990, Russia; e-mail: pps64@mail.ru).