CRIMINAL LIABILITY FOR CYBERCRIMES IN THE BRICS COUNTRIES

LILIYA IVANOVA,

University of Tyumen (Tyumen, Russia)

https://doi.org/10.21684/2412-2343-2023-10-1-59-87

One of the areas of cooperation among the BRICS countries is tackling the misuse of information and communication technologies for criminal activities. Each year, the number of cybercrimes continues to grow. Furthermore, the criminal regulation of cybercrimes in each country differs. This article aims to identify the features of criminal liability for cybercrimes in the BRICS countries and offer potential solutions for developing joint legislation initiatives. The primary focus of this discussion is on cybercrime provisions that can be found in the legal acts of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa. The main finding of this research is that the criminal law of each country contains different corpus delicti for dealing with crimes committed in cyberspace. There are also differing conceptions of what constitutes cybercrime. The author proposes the enactment of a common document for the BRICS countries that would contain a shared understanding of cybercrimes as well as the various types of cybercrimes. It is possible to divide cybercrimes into two categories: special cybercrimes committed in the field of computer information and general criminal cybercrimes executed using information technology to commit any other common criminal offences. The results of this research can be used to study the problems of criminal responsibility for cybercrimes in the BRICS countries as well as analyze the ways in which the rules under consideration are actually applied in practice.

Keywords: cybercrime; digital space; Brazil; Russia; India; China; South Africa; BRICS.

Recommended citation: Liliya Ivanova, *Criminal Liability for Cybercrimes in the BRICS Countries*, 10(1) BRICS Law Journal 59–87 (2023).

Table of Contents

Introduction

The international association of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa has firmly entered the international political arena. The Declaration issued following the XI Summit of the BRICS member states, which took place in Brazil on 14 November 2019,[1] reaffirms the countries' commitment to tackling the misuse of information and communications technologies (ICTs) for criminal and terrorist activities The states recognize the progress made by each of the BRICS countries in promoting cooperation through the Working Group on Security in the Use of Information and Communication Technologies, which recently approved its revised Terms of Reference, and through the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs. The Declaration following the XIV Summit of the BRICS member states, which was held in Beijing on 23 June 2022,[2] underscores the importance of establishing legal frameworks of cooperation among the BRICS countries on ensuring security in the use of ICTs.

Over the past decade, BRICS countries have seen a steady increase in crimes committed using computer and telecommunications technologies. The ubiquity of information and communication networks is the primary reason for this increase. Information and telecommunications networks have become indispensable tools in resolving not only corporate issues (through electronic document management systems, business correspondence via the Internet and so on) but also household issues (such as paying for goods online, obtaining public services through a particular website, etc.). New data are added to the information space on a daily basis. At the same time, the widespread dissemination of the latest technologies is fraught

---

[1] Declaration of the 11th BRICS Summit of 2019 (Sept. 10, 2022), available at https://eng.brics-russia2020.ru/images/00/68/006895.pdf.

[2] XIV BRICS Summit Beijing Declaration of 2022 (Sept. 10, 2022), available at http://brics2022.mfa.gov.cn/eng/hywj/ODS/202207/t20220705_10715631.html.

with threats of encroachment on personal security and property as well as the protection of society as a whole and the State, thus implying a risk of harm to the most important social relations.

When a crime is committed over the Internet, it is referred to as a cybercrime.[3] Cybercrimes are numerous and varied.[4] They include cyber theft, fraud, hacking, cyber pornography, violation of privacy, sale of illegal products, online gambling, intellectual property crimes, e-mail spoofing, cyber defamation, cyberstalking, cyber terrorism and others. This author understands cybercrime as a crime where a computer (including different devices) or network is used as a tool or means to commit a crime or as a target for criminals. Computers may serve as both the instruments and the targets of an offence.[5]

Meanwhile, the term "cybercrime" needs to be discussed. As noted in United Nations documents, there are two main definitions. The first is a more narrow definition: "computer crimes". The second is a broader definition and includes all computer-related crimes. Reports of cybercrime largely depend upon the context in which the term is used. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crimes and computer content-related acts, do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term.[6]

At the same time, every country has its own specific legislation. Furthermore, the criminal regulation of cybercrimes also differs. To develop a unified mechanism for implementing liability, it is first necessary to analyze the specifics of the legislative limitations of criminal liability for cybercrimes in each of the BRICS countries. Of course, the main feature that distinguishes cybercrimes from other illegal acts is the use of computer technologies and the Internet when committing a crime. Despite the commonality of interests in countering such actions, approaches to criminalizing violations in the digital space within a particular state differ significantly, both in form and content. It would appear that gaining an understanding of the peculiarities of each country in the criminal law regulations of liability for cybercrimes will help identify general directions and prospects for cooperation in this area.

---

[3] Mir M. Azad et al., *Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law*, 3(5) Int'l J. New Tech. & Res. 1, 3 (2017).

[4] Babak Akhgar et al. (eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook* 149–64 (2014).

[5] Peter Grabosky, *The Internet, Technology, and Organized Crime*, 2 Asian Criminology 147 (2007).

[6] UNODC, *Comprehensive Study on Cybercrime – Draft* (February 2013) (Sep. 10, 2022), available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Problems of cybersecurity have always attracted the attention of scientists.[7] Studies conducted on the liability for cybercrimes in select BRICS countries[8] confirm the importance of this issue. However, a comprehensive analysis of the legislative regulations of criminal liability for cybercrimes in each of the BRICS countries, in general, has yet to be conducted.

This article aims to identify the features of criminal liability for cybercrimes in the BRICS countries and offer potential solutions for developing joint legislation initiatives. The achievement of the stated aim is pursued through the analysis of statistical reports and legal acts of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa, which establish criminal liability for cybercrimes. To that end, the article is divided into five parts that reveal the peculiarities of criminal responsibility for cybercrimes in each of the separately selected BRICS countries. The final section presents the main findings of the research and the future prospects of the joint legislation's development.

1. Criminal Liability for Cybercrimes in the Federative Republic of Brazil

Cybercrime is a major issue in Brazil, as it is in the other BRICS countries. Cyberattacks frequently target officials and government agencies. For example, in June 2020, the Brazilian hacker group "Anonymous" posted personal data of the President of Brazil online, and in November 2020, the Brazilian Supreme Court was suspended due to a hacker attack that blocked access to the electronic database of trials.[9]

Brazilian criminal law is represented by the Brazilian Penal Code[10] which contains a number of provisions regulating criminal liability for crimes committed in the

---

[7] *See, e.g.*, Zoran Mitrovic & Surendra C. Thakur, *Positioning South Africa in the BRICS Cybersecurity Context: A Strategic Perspective*, in Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch Univ, South Africa 251 (2019); Nir Kshetri, *Cybercrime and Cybersecurity Issues in the BRICS Economies*, 18(4) J. Global Info. Tech. Mgmt. 245 (2015); V.S. Subrahmanian et al., *The Global Cyber-Vulnerability Report* (2015).

[8] *See, e.g.*, Lennon Y. Chang, *Cybercrime in the Greater China Region. Regulatory Responses and Crime Prevention across the Taiwan Strait* (2012); *Коробеев А.И., Дремлюга Р.И., Кучина Я.О.* Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 416–425 [Alexander I. Korobeev et al., *Cybercrimes in the Russian Federation: Criminological and Criminal Law Analysis of the Situation*, 13(3) Russian J. Criminology 416 (2019)]; Saurabh Mittal & Ashu Singh, *A Study of Cyber Crime and Perpetration of Cyber Crime in India*, in Evolving Issues Surrounding Technoethics and Society in the Digital Age 171 (2014); Minakshie Dasgupta, *Cyber Crime in India – A Comparative Study* (2009).

[9] Ana Ferraz, *Tech Roundup: Brazil Joins International Cybercrime Convention*, The Brazilian Report (2020) (Sep. 10, 2022), available at https://brazilian.report/tech/2021/12/17/cybercrime-open-finance-racism/.

[10] Código Penal of 1940 (Portuguese) [Brazilian Penal Code] (Sep. 10, 2022), available at http://www.planalto.gov.br/CCIVIL_03/Decreto-Lei/Del2848.htm#art334.

digital sphere or using computer technology. There is no specific chapter devoted to cybercrimes in the criminal legislation of Brazil. Various cybercrime provisions can be found throughout the Code. In the last few years, the legislator has added a few new *corpus delicti* to criminal law, though their numbers are relatively small.

Article 154-A, which was added to the Code on 30 November 2012,[11] establishes criminal liability for hacking a computer device that results in unauthorized access and infection of IT systems with malware. The first of the named actions is the invasion of a third party's computing device, whether or not it is connected to a computer network, through an undue violation of the security mechanism to obtain, tamper with or destroy data or information without the express or tacit authorization of the device owner. The second of the named actions is the installation of vulnerabilities to obtain an illicit advantage. The penalty for such actions is detention, which can range from three months to one year, and a fine. The same penalty applies for producing, offering, distributing, selling or sending a computer program or device that can allow illegal access to another device, whether or not that device is connected to a computer network. All of the above described actions involve the undue violation of a security mechanism with the intent to obtain, tamper with or destroy data. The provisions for such offenses can be found in Section IV, "Crimes against the Inviolability of Secrets" and Chapter VI, "Crimes against Individual Freedom."

The Act of 30 November 2012 came into force 120 days after its official publication, and as of 2013, the Brazilian Penal Code also prohibits interruption or disturbance of a telematic or information service of a public utility. Previously, the law protected only telegraph or telephone services. Today, according to Provision 266 (Chapter II "Crimes against the Security of Media and Transport and Other Public Services"), the interruption or disturbance of telegraph, radiotelegraph or telephone services, as well as telematics services or public utility information services, shall be punishable by imprisonment ranging from one to three years, as well as a fine. Therefore, any denial-of-service attacks are now punishable under the Brazilian Penal Code.

The Act of 24 September 2018 established criminal liability for the disclosure of a rape scene or a rape scene involving a vulnerable person, a sex scene or pornography.[12] The offering, transmitting or publishing a photograph, video or audio file depicting an incident of rape, a rape of a vulnerable person, or any other material dealing with a sex scene, nudity or pornography is thus punishable by up to five years of imprisonment. The legislator indicated various ways of committing crimes. These methods include the above mentioned actions carried out through mass media, a computer or a telematics system.

---

[11] Lei nº 12.737, de 30 de novembro de 2012 (Portuguese) [Act of 30 November 2012] (Sep. 10, 2022), available at http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm#art2.

[12] Lei nº 13.718, de 24 de setembro de 2018 (Portuguese) [Act of 24 September 2018] (Sep. 10, 2022), available at http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Lei/L13718.htm#art1.

In addition, some amendments were made to the Penal Code in order to modify the criminal liability for the crime of inciting suicide and to include the conduct of inducing or instigating self-mutilation, as well as aiding it. As a result, on 26 December 2019, a law was passed that amended Article 122, which prohibits inducing, instigating or assisting suicide or self-mutilation.[13] The new regulation provides that the penalty is doubled if the offence is committed through a computer network, social network or real-time transmission. It is interesting to note that in the Russian Federation, the legislator changed the circumstances under which someone is criminally responsible for inciting, convincing, or aiding suicide in 2017. Since 2012, groups promoting suicide on the social network have discussed the suicides of children and adolescents whose account pages contained suicidal content found by law enforcement officers after their deaths. Similar cases can be found all over the world. The additions to both Criminal Codes are a corresponding response by the legislators to new forms of mental influence on minors that have appeared with the development of information technology.

Any criminal offence perpetrated in a cybernetic context may be punished in the same way as it would be if committed outside of such a context. In this sense, the crime of extortion committed in the context of a ransomware cyberattack is a widespread violation.[14]

Sometimes articles do not specifically mention information and telecommunications networks as a method of committing a crime, but this may be implied in the text of the law since the article names the public commission of a crime. For example, publicly inciting the practice of crime (Art. 286), expressing public justification for a criminal fact or being a perpetrator of a crime (Art. 287) may all be considered crimes committed through the Internet when a person posts some information on a social network or a public messenger app. Crimes against religious feeling and crimes against respect for the dead may be treated the same way. Article 208 prohibits publicly mocking a person for their religious belief or event, as well as publicly vilifying a religious action or object of religious devotion. In the event that such acts are committed using information technology, they should be classified as cybercrimes.

It is important to remember the particularities of Brazilian criminal law. The Penal Code is not the only source of criminal penalties. Brazil has specific rules, regulating the different spheres of life and establishing criminal penalties for offences. For example, the Industrial Property Law (9,779/96)[15] contains provisions on crimes relating to unfair competition. Publication, by any means, of a false affirmation to

---

[13] Lei nº 13.968, de 26 de dezembro de 2019 (Portuguese) [Act of 26 December 2019] (Sep. 10, 2022), available at https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13968.htm.

[14] Fabio F. Kujawski et al., *Cybersecurity Laws and Regulations Brazil*, ICLG (Sep. 10, 2022), available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/brazil.

[15] Industrial Property Law of 1996 (Sep. 10, 2022), available at https://www.jpo.go.jp/e/system/laws/gaikoku/document/index/brazil-e_industrial_property_law.pdf.

the detriment of a competitor with the intent to obtain an advantage is one of the actions that falls under the category of unfair competition. This action is punishable by imprisonment for up to three months to one year or by a fine. The use of the words "any means of publication" includes the use of information technology. Therefore, unfair competition in this part can also be attributed to cybercrime.

There is also special legislation in place to regulate the digital space. The new General Data Protection Law[16] regulates "processing of personal data, including by digital means, by a natural person or a legal entity of public or private law, to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person" (Art. 1). With the exception of specific data (such as health, banking and airline passenger records), Brazil has never had a comprehensive set of rules for dealing with the storage, access and processing of personal data.[17] The majority of the provisions of the above-named law came into force in 2021,[18] and it includes administrative penalties for other offences related to those specified.

At the same time, according to Article 52, the provisions of this article do not replace the application of administrative, civil or criminal sanctions defined in Law 8,078, of 11 September 1990, and in specific legislation. In addition to establishing liability for criminal offenses, the Act[19] provides for the protection of consumers as well as other measures. Some offences may be committed using information and communication technologies and in such cases, they constitute cybercrimes.

Such crimes (without prejudice to the provisions of the Penal Code) may include making a false or misleading statement or omitting relevant information about the nature, characteristic, quality, quantity, safety, performance, durability, price or guarantee of products or services; producing or promoting advertising that can induce the consumers to behave in a way that is harmful or dangerous to their health or safety; and preventing or hindering the consumers' access to the information contained in registrations, databases and records. Although the use of information and telecommunications networks is not typically regarded as a method of committing a crime, the mention of Law No. 8,078 in the General Data Protection Law may indicate that the legislator recognizes the possibility of these actions being perpetrated in cyberspace.

---

16 Lei nº 13.709, de 14 de agosto de 2018 (Portuguese) [Act of 14 August 2018] (Sep. 10, 2022), available at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art65ii.

17 Fabiano Deffenti, *Brazil's Data Protection Law in Force*, LawsofBrazil, 18 September 2020 (Sep. 10, 2022), available at http://lawsofbrazil.com/2020/08/31/brazils-data-protection-law/.

18 *See* Lei nº 14.010, de 10 de junho de 2020 (Portuguese) [Act of 10 June 2020] (Sep. 10, 2022), available at http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm#art20; Lei nº 14.058, de 17 de setembro de 2020 (Portuguese) [Act of 17 September 2020] (Sep. 10, 2022), available at http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14058.htm.

19 Lei nº 8,078, de 11 de setembro de 1990 (Portuguese) [Act of 11 September 1990] (Sep. 10, 2022), available at http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

2. Criminal Liability for Cybercrimes in the Russian Federation

In the Russian Federation, the legal basis for combating cybercrimes first appeared with the adoption of the Criminal Code of the Russian Federation,[20] which came into force on 1 January 1997. A new chapter, Chapter 28, entitled "Crimes in the Sphere of Computer Information" appeared in the Code. However, cybercrimes are not limited to crimes committed using a computer. The use of any electronic, information, or telecommunications networks is established as a constructive or qualifying sign of *corpus delicti* in various articles of the Criminal Code of the Russian Federation.

Official statistics show a steady increase in the number of crimes committed using information technologies. For example, in 2021, the number of reported crimes committed through information and telecommunications technologies or in the field of computer information was 517,722, which is 1.4% higher than the data for the same period in 2020. In 2020, cybercrimes grew by 73.4%. In 2019, the number of crimes committed using computer and telecommunications technologies was 68.5% higher than in the same period the previous year. And in 2018, 174,674 such crimes were registered, that is, 92.8% more than in 2017, during which only 90,587 such crimes were reported.[21] It is important to note that statistics from the Ministry of Internal Affairs of Russia only began to reflect crimes committed using computer and telecommunications technologies since 2017. Prior to 2017, reports reflected only data on crimes committed in the field of computer information. At the same time, the list of crimes that can be committed with the use of information technologies under the Criminal Code of the Russian Federation has significantly expanded since 2016. The use of information technology is a possibility in the commission of various types of crimes, including those committed against property and the safety of individuals, society and the State.

Such a term as "cybercrime," which is so widespread in the world of scientific literature and the media, does not occur and is not disclosed in modern Russian legislation. However, as mentioned, scientists like the term "cybercrime." In addition to this term, Russian scientists also use such categories as: "crimes in the field of information technology," "information crimes," "network computer crimes" and "Internet crimes." However, this author believes that the term "cybercrime" or some other similar term should be included in the Russian Criminal Code for a common understanding of crime in cyberspace.

---

[20] Уголовный кодекс Российской Федерации от 13 июня 1996 г. // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954 [Criminal Code of the Russian Federation on 13 June 1996, Legislation Bulletin of the Russian Federation, 1996, No. 25, Art. 2954].

[21] Министерство внутренних дел Российской Федерации. Статистика и аналитика 2016–2021 [The Ministry of Internal Affairs of the Russian Federation, *Statistics and Analytics 2016–2021*] (Sep. 10, 2022), available at https://мвд.рф/Deljatelnost/statistics.

Russian law enforcement officials also have different understandings of the term "cybercrime." Of the 108 interviewed investigators and operatives of the Tyumen region, 35.3% of respondents understood cybercrimes as crimes committed using information or computer technologies. The same number of respondents understood cybercrimes as crimes committed in the field of information technology and computer communications. Additionally, 23.5% of respondents understand cybercrimes as crimes committed via the Internet or on the Internet. And 5.5% of respondents view cybercrimes more narrowly as crimes committed in the field of computer information, for which responsibility is provided for by Chapter 28 of the Criminal Code of the Russian Federation. Despite the apparent differences in the respondents' answers, all of the definitions include information technologies that are stated as either a place or a means of the commission of a crime.

The content of the category of cybercrimes must comply with the current criminal legislation. As previously noted, the Criminal Code of the Russian Federation contains Chapter 28 "Crimes in the Field of Computer Information," which includes only four articles, from 272 to 274.1 of the Criminal Code of the Russian Federation, and addresses the following areas:

- illegal access to computer information (Art. 272);
- creation, use and dissemination of harmful computer programs (Art. 273);
- violation of the rules for the operation of the facilities for the storage, processing and transmittance of computer information and of information-telecommunication networks (Art. 274);
- impact of illegal activity on the critical information infrastructure of the Russian Federation (Art. 274.1).

Criminal liability for an unlawful impact on the critical information infrastructure of the Russian Federation has been included in criminal legislation since July 2017, following the adoption of the Federal Act concerning the security-critical information infrastructure of the Russian Federation.

In July 2022, Chapter 28 was supplemented with a new article, Article 274.2, which establishes responsibility for violating the rules for 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 the public communication network on the territory of the Russian Federation.

In addition to crimes committed in the field of computer information, several articles of the Criminal Code of the Russian Federation contain a constructive or qualifying sign of the commission of an act "using electronic or information-telecommunication networks, including the Internet." According to Article 2 of the Federal Law "On Information, Information Technologies and Information Protection,"[22]

---

[22] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3448 [Federal Law No. 149-FL of 27 July 2006. On Information, Information Technologies and Information Protection, Legislation Bulletin of the Russian Federation, 2006, No. 31 (part 1), Art. 3448].

an information and telecommunications network is a technological system designed for the transmission of information through communication lines, access to which is provided through computer technology.

A constructive indication of the use of high technologies during the commission of a crime is contained only in Article 137 "Invasion of Personal Privacy"; Article 159.6 "Computer Fraud"; Article 171.2 "Illegal Organization and Conduct of Gambling"; Article 185.3 "Market Manipulation"; and Article 282 "Incitement of Hatred or Enmity" as well as "Abasement of Human Dignity."

The commission of an act using electronic or information and telecommunications networks as an indication that the act poses a greater threat to the public and entails a more severe punishment is mentioned in only fourteen articles of the Criminal Code of the Russian Federation. Here is a list of the acts and the articles:

- Incitement to suicide (Art. 110).
- Persuading or assisting in suicide (Art. 110.1).
- Organization of activities aimed at inducement to commit suicide (Art. 110.2).
- Involvement of a minor in the commission of acts that endanger the life of a minor (Art. 151.2).
- Public calls to commit terrorist activities, public justification of terrorism or propaganda of terrorism (Art. 205.2).
- Sale of narcotic drugs, psychotropic substances or their analogues (part 2 of Art. 228.1).
- Circulation of counterfeit, substandard and unregistered medicaments, medical devices and counterfeit dietary supplements (Art. 238.1).
- Illegal production and distribution of pornographic materials or objects (Art. 242).
- Production and distribution of materials or objects with pornographic pictures of minors (Art. 242.1).
- Using a minor to produce pornographic materials or objects (Art. 242.2).
- Cruelty to animals (Art. 245).
- Illegal procurement and circulation of especially valuable wild animals and aquatic biological resources belonging to species included in the Red Book of the Russian Federation and (or) protected by international treaties to which the Russian Federation is a signatory state (Art. 258.1).
- Public calls for extremist activities (Art. 280).
- Public calls for the commission of actions aimed at violating the territorial integrity of the Russian Federation (Art. 280.1) and others.

It is important to take note of the fact that the legislator mentions information and communication technologies along with the commission of a crime in a public speech, in a publicly performed work or in the mass media. Thus, the publicity of the commission of the act is essential for the listed offences. Meanwhile, the speech and the performance can be broadcast via the Internet, and the mass media used

in these kinds of situations may also be online sources. Publicity manifests itself in an orientation towards an endless circle of people. The same category of publicity is evaluative, and it applies to other crimes as well where a similar qualifying feature appears. There are explanations from the Supreme Court of the Russian Federation; however, the Court does not describe publicity from a quantitative point of view. It appears that publicity is dependent on the informational orientation as well as the potential to reach a large number of people regardless of the actual number of people who have familiarized themselves with it.

If, for example, the guilty person is in a private correspondence with a potential victim through the Internet, then in this case there is no sign of publicity. In this regard, some researchers note that it is unnecessary to establish the use of information and telecommunications networks as a qualifying feature.[23] However, the use of information technology significantly facilitates crime. One illustration of this is the ease with which it is possible, even without a background in psychology, to identify issues and personality imbalances in a potential victim due to the Internet's quick means of searching among those who upload not only personal data but also their personal stories to the network. Additionally, it makes it easier to establish contact with the victim. At the same time, criminals can gain confidence by creating and using a virtual legend about themselves (such as fake profiles, fake photos, etc.) while keeping their real identity unknown. Therefore, the use of information telecommunications networks is rightly recognized by the legislator as a factor that increases the degree of public danger from the deed.

The Criminal Code of the Russian Federation contains several more provisions that, in this author's opinion, can be attributed to cybercrimes. Among such provisions, item "g" part 3 of Article 158 of the Criminal Code of the Russian Federation contains a particularly qualified structure: theft from a bank account, as well as electronic money. Additionally, Article 159.3 of the Criminal Code of the Russian Federation establishes liability for fraud using electronic means of payment and Article 187 of the Criminal Code of the Russian Federation establishes liability for the illegal circulation of electronic means, electronic storage media, technical devices and computer programs intended for the unlawful implementation of the receipt, issue and transfer of funds. The attribution of these structures to cybercrimes is possible due to the subject of the crime, which is either non-cash funds or electronic means or electronic media, that is, everything that appeared because of the development of information technologies and their introduction into the banking sector.

An interesting case recently reached the Supreme Court of the Russian Federation. On 13 May 2019, a person named Kaktan found a contactless bank card. On the same day and the next, Kaktan used the card to make purchases for goods in various

---

[23] *Устинова Т.Д.* Склонение к самоубийству или содействие самоубийству: критический анализ // Lex Russica. 2020. № 3. С. 151–158 [Tatyana D. Ustinova, *Encouragement to Commit Suicide or Assisting with Suicide: Critical Analysis*, 3 Lex Russica 151 (2020)].

shops and cafes, stealing money until the owner of the card blocked it. Kaktan was convicted for attempted theft of non-cash funds. The Supreme Court reclassified the actions of the convict as fraud. The Court pointed out that the current laws did not impose on trade employees the obligation to identify cardholders through the use of documents proving their. Therefore, the qualification of fraud was incorrect.[24]

An analysis of the above-named legal norms reveals certain flaws in the legislative technique. For example, the legislator may formulate the above qualifying feature in different ways: in some cases, information-telecommunications networks are referenced along with electronic ones, while in others they are not. At other times, information and telecommunications networks are referred to as being part of the mass media, whereas at other times they are considered independent of each other.

In the same way that it is the case in Brazil, some articles do not specifically mention information and telecommunications networks as a method of committing crimes, yet such networks may actually exist. For example, public dissemination of knowingly false information about circumstances that pose a threat to the life and security of citizens does take place on the Internet, as practice shows.

Moreover, the crimes listed above are not the only ones that can be committed using advanced technologies. For example, alcoholic beverages and alcohol-containing food products can be sold illegally on the Internet. However, this criterion as a qualifying feature is not reflected in any of the relevant articles of the Criminal Code of the Russian Federation.

3. Criminal Liability for Cybercrimes in the Republic of India

In Asia, India ranks among the two top countries for the highest number of Internet users per country, making it one of the fastest-growing countries in the region.[25] This widespread use of information and telecommunications technologies entails high risks of cyber threats.

In 1981, Lan Murphy (also known as "Captain Zap") became the first person to be found guilty of a cybercrime. He had hacked an American telephone company in order to manipulate its internal clock, so that users could still make free calls at peak times.[26]

---

[24] Определение Верховного Суда Российской Федерации от 29 сентября 2020 г. по делу № 12-УДП 20-5-К6 [Ruling of the Supreme Court of the Russian Federation of 29 September 2020, case No. 12-UDP20-5-K6] (Sep. 10, 2022), available at https://www.vsrf.ru/stor_pdf.php?id=1917106.

[25] Nidhi Arya, *Cyber Crime Scenario in India and Judicial Response*, 3(4) Int'l J. Trend Sci. Res. & Dev. 1108 (2019) (Sep. 10, 2022), available at https://www.ijtsrd.com/papers/ijtsrd24025.pdf.

[26] Nidhi Narnolia, *Cyber Crime in India: An Overview*, Legal Service India E-Journal (2019) (Sep. 10, 2022), available at https://legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html

According to official statistics,[27] the number of reported cybercrimes grows every year. A statistical report showed there were 12,317 reported cybercrimes in 2016. Almost twice as many, 21,796 cybercrimes, were reported in 2017. And in 2018, 27,248 cybercrimes were reported. The number of reported cybercrimes has doubled in two years. During the year 2018, 55.2% of cybercrime cases registered were for the motive of fraud (15,051 out of 27,248 cases), followed by sexual exploitation at 7.5% (2,030 cases) and causing disrepute at 4.4% (1,212 cases). In 2021, statistics showed 52,974 cases of cybercrime.

In order to prevent cyberattacks and punish the guilty, the Indian legislator has established criminal punishments for cyber offences. The criminal legislation that relates to cybercrimes is made up of the Penal Code as well as other various Acts.

The Indian Penal Code, 1860[28] does not contain a separate section dedicated to cybercrimes. A special law regulates relationships in cyberspace. This law is the Information Technology Act (IT Act),[29] which was enacted in the year 2000 but was substantially amended in the year 2008. Meanwhile, since the primary objective of this Act is to create an enabling environment for the commercial use of IT, specific crimes committed using computers have not been included. The relevant sections of the Indian Penal Code contain several offences relating to cyberspace.[30] Special laws also apply. According to the statistics, these offences constitute violations under both Special and Local Laws (SLL). Thus, there are three broad groups of cybercrimes in India. The first group of crimes is governed by the Information Technology Act, the second group is governed by the Indian Penal Code and the third group of crimes is governed by the Special and Local Laws.

The Information Technology Act is the primary legislation in India dealing with cyber offences, and it is based on the United Nations Model Law on Electronic Commerce which was adopted by the United Nations Commission on International Trade Law.[31] Chapter XI of the Information Technology Act establishes penalties for offences in cyberspace. The crime list (Arts. 65–74) is very extensive and detailed, and it includes the following offenses:

- Tampering with computer-source documents.
- Computer-related offences such as sending offensive messages through communication services, etc.; dishonestly receiving stolen computer resources or

---

27 National Crime Records Bureau, *Crime in India* (2021) (Sep. 10, 2022), available at https://ncrb.gov.in/en/crime-india.

28 The Indian Penal Code of 1860 (Sep. 10, 2022), available at https://www.indiacode.nic.in/handle/123456789/2263?locale=en.

29 The Information Technology Act of 2000 (Sep. 10, 2022), available at https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf.

30 Mittal & Singh 2014.

31 Sujata Pawar & Yogesh Kolekar, *Essentials of Information Technology Law* (2015).

communication devices; identity thefts; cheating by personation using computer resources; violation of privacy.

• Cyber terrorism.

• Publication or transmission of an obscene or sexually explicit act in electronic form that includes publishing or transmitting obscene material in electronic form; publishing or transmitting material containing sexually explicit actions, etc., in electronic form; publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form and contravening the preservation and retention of information by intermediaries.

• Failing to comply with Controller directives.

• Contravention of the powers of the Central Government that include interception, monitoring or decryption of information through any computer resource; blocking public access to any information through any computer resource and contravention of the power to authorize monitoring and collecting traffic data or information through any computer resource for cybersecurity.

• Unauthorized access to or an attempt to access a protected computer system.

• Misrepresentation.

• Breach of confidentiality and privacy.

• Disclosure of information in breach of a lawful contract.

• Publishing an electronic signature certificate that is false in certain particulars and published for a fraudulent purpose.

Cyber terrorism is recognized as the most socially dangerous crime because it is the only cybercrime punishable by imprisonment, which may extend to life imprisonment. This crime is particularly interesting because there is no generally accepted understanding of the actions that constitute cyber terrorism in the world: whether it is a distinct phenomenon or simply a form of information warfare conducted by terrorists.[32]

Moreover, there is no related *corpus delicti* in the legislation of many countries.

Section 66 describes cyber terrorism extensively and includes two kinds of criminal actions.

The first one includes offences committed with the intent to threaten the unity, integrity, security or sovereignty of India or to instill fear in the people or any groups of the people. Examples of this category include: denying or causing the denial of access to any person authorized to access a computer resource; attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or introducing or causing the introduction of any computer contaminant. And through the means of such conduct, it causes or is likely to cause death or injuries to persons or damage to or destruction of property, disrupts or knows that it is likely to cause harm or disruption of supplies or services essential to the life of the community, or adversely affects the critical information infrastructure.

---

[32] Martti Lehto & Pekka Neittaanmäki (eds.), *Cyber Security: Analytics, Technology and Automation* 78 (2015).

The second one includes offences that are committed knowingly or intentionally and involve the penetration of or access to a computer resource without authorization or access that exceeds authorized access. They include gaining access to information, data or computer databases that are restricted for reasons related to the security of the State or foreign relations; or gaining access to any restricted information, data or a computer database, with reasons to believe that such information, data or computer databases so obtained may cause harm to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality; or concern the contempt of Court, defamation or incitement to an offence; or be to the advantage of any foreign nation, group of people or otherwise.

There are some problems in formulating certain *corpus delicti* under the IT Act. For example, the provision on child pornography talks only of sexualized representations of actual children and omits fantasy play-acting by adults and such. Thus, from a direct reading of the provision, it is unclear whether drawings depicting children will also be deemed an offence under the provision.[33]

Moreover, some crimes are not definable. For example, Provision 66D provides punishment for cheating by personation using a computer resource but does not disclose what the cheating by personation is. As will be shown below, the Indian Penal Code (IPC) contains cheating by personation too. According to section 416 of the IPC, "a person is said to 'cheat by personation' if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is." It would appear that the only difference between crimes under the IT Act and those under the IPC is the use of computer resources. Furthermore, the punishments are similar. It is therefore unclear why duplication of the *corpus delicti* is necessary. It should be noted that cheating inducing delivery of property entails punishment under the IPC even if the crime was committed using a computer resource because the penalty under section 420 of the IPC is stricter than the penalty under section 66D of the IT Act.

As noted above, the Indian Penal Code contains several crimes that can constitute cybercrimes. In some sections of the Code, the description of crimes allows cybercrimes to be attributed to them. For example, describing a way of committing a crime as "by words, either spoken or written, or by signs, or by visible representation, or otherwise" indicates an extensive list of ways to commit a crime, which can include means of information technology. This feature is characteristic of sedition (sec. 124A) and promoting enmity between different groups on grounds of religion, race, place of birth, residence, language and so on, as well as of acts prejudicial to the maintenance of harmony (sec. 153A).

---

[33] Jitender K. Malik & Sanjaya Choudhury, *Privacy and Surveillance: The Law Relating to Cyber Crimes in India*, 9(12) J. Engineering, Computing & Architecture 83 (2019).

In the case of defamation (sec. 499), the way of committing a crime is described slightly differently: "by words either spoken or intended to be read, or by signs or by visible representations."

Cyberstalking (sec. 354D) includes such activities as monitoring a woman's usage of the Internet, e-mail or any other form of electronic communication.

Electronic records can be found as an object of infringement in such crimes as forgery, forgery for cheating, forgery to harm the reputation and using a forged document or electronic record as genuine (sec. 463–471).

Using a telecommunications device or any other electronic mode, including the Internet, is specified in section 509B, which establishes criminal liability for sexual harassment by electronic means. Fake news on social media may be punishable under section 505, which shows liability for statements conducing to public mischief.

It is worth noting that the text of the law does not always necessarily indicate the use of information technology in the commission of a crime. However, in statistics, if a crime takes place online, it is reflected as a "cybercrime." For example, abetment of suicide (sec. 306) may take place online, in which case it is considered cybercrime. However, the Code does not explicitly mention the online abetment of suicide. Regardless of the way in which a suicide is abetted (online or offline), the punishment for such a criminal act is imprisonment of any kind for a term that may extend to ten years, as well as a fine.

Let us suppose a crime is related to the use of information and telecommunications networks, but there is no mention of these technologies in the section. In that case, accountability belongs under this section, but the statistics will reflect such situations as cybercrimes. Examples of such crimes are data theft (sec. 379–381); fraud which includes offences involving credit cards and debit cards, ATMs, online banking fraud, one-time password (OTP) fraud and so forth. (sec. 420, 465 and 468–471); cheating and dishonestly inducing delivery of property (sec. 420); counterfeiting which includes offences involving currency (sec. 489A–489E) and stamps (sec. 255); and cyber blackmailing and threatening (sec. 506, 503 and 384).

The last group of cybercrimes includes offences prohibited by the Gambling Act,[34] Lotteries Act,[35] Copy Right Act,[36] Trade Marks Act[37] and others.

The Gambling Act provides for the punishment of public gambling as well as the keeping of common gaming-houses in the United Provinces, East Punjab, Delhi and

---

[34] The Public Gambling Act of 1867 (Sep. 10, 2022), available at https://www.indiacode.nic.in/handle/123456789/2269?view_type=browse&sam_handle=123456789/1362.

[35] The Lotteries (Regulation) Act of 1998 (Sep. 10, 2022), available at https://www.indiacode.nic.in/handle/123456789/1994?view_type=browse&sam_handle=123456789/1362.

[36] The Copyright Act of 1957 (Sep. 10, 2022), available at https://www.indiacode.nic.in/handle/123456789/1367?view_type=browse&sam_handle=123456789/1362.

[37] The Trade Marks Act of 1999 (Sep. 10, 2022), available at https://www.indiacode.nic.in/handle/123456789/1993?locale=en.

the Central Provinces. This Act prescribes penalties for owning, keeping or having charge of a gaming-house as well as the penalties for being found in a gaming-house. Online gambling is also punishable.

The Lotteries Act prohibits organizing, conducting or promoting any lottery. A state government may organize, realize or promote a lottery, subject to the specific conditions named in section 4 of the Act. Therefore, operating online lotteries may be punishable with rigorous imprisonment for a term which may extend to two years, with a fine or with both.

The Copy Right Act provides criminal responsibility for such offences as an infringement of copyright or other rights conferred by this Act; deliberate use of an infringing copy of a computer program; possession of plates to make infringing copies; violation of the protection of Rights Management Information; disposal of infringing documents or plates to make infringing copies; and making false entries in the register, etc., for producing or tendering false statements to deceive or influence any authority or officer.

Interestingly, punishment for an infringement of copyright is assigned regardless of mercenary motive. Where the violation does not concern any gain in the course of trade or business, the Court may only, for adequate and special reasons to be mentioned in the judgment, reduce a sentence of imprisonment or impose a fine in a smaller amount.

The Trade Marks Act provides penalties for such offences as applying false trademarks, trade descriptions, etc.; selling goods or providing services to which a false trademark or false trade description has been applied; falsely representing a trademark as registered; improperly describing a place of business as being affiliated with the Trade Marks Office; and falsifying entries in the register.

The scope of Special and local laws is not limited to the named acts. There are different laws in India. And if the offence takes place in the cybersphere, it is considered a cybercrime.

It is possible to incur criminal liability under both the Indian Penal Code and a Special Law. For example, scholars, Jitender K. Malik and Dr. Sanjaya Choudhury considered the following case:[38] The Mumbai Police registered the following first case of cyber terrorism since the amendment to the Information Technology Act. One day, emails containing a threat were sent to both the Bombay Stock Exchange (BSE) and the National Stock Exchange (NSE). The Internet Protocol (IP) address of the sender was traced to Patna, in Bihar. The Internet Service Provider (ISP) was identified as "Sify," and the e-mail address had been created only four minutes before the e-mail was sent. The sender had provided two mobile numbers in the personal details column while creating the new email identity. Both the numbers belonged to a photo frame manufacturer in Patna. The police, thus, registered cases of forgery

[38] Malik & Choudhury 2019, at 88.

for cheating, criminal intimidation cases under the Indian Penal Code and cyber terrorism under section 66-F of the Information Technology Act.

4. Criminal Liability for Cybercrimes in the People's Republic of China

In China, cybercrimes are consistently an area of focus since they are widely recognized as a threat to national security. According to the Supreme People's Procuratorate of the People's Republic of China, in recent years, prosecuting authorities have fully performed their functions and resolutely curbed the spread of cybercrimes. The number of cybercrime cases handled has increased significantly year by year, with an average annual increase of more than 34%. During the new crown pneumonia (Covid-19) epidemic, prosecution authorities have consistently maintained a strong focus on cybercrimes. According to statistics, as of 7 April 2020, prosecution authorities across the country had reviewed and approved the arrest of 3,275 people in 2,718 criminal cases involving the epidemic as well as 1,862 public prosecutions of 2,281 people, of which 1,588 were arrested for fraud.[39]

In China, the system for regulating cybercrime is a multi-dimensional and comprehensive mechanism designed to protect the computers as well as the data that is stored on the computers.[40]

The Criminal Law of the People's Republic of China (hereinafter Criminal Law)[41] was adopted by the Second Session of the Fifth National People's Congress on 1 July 1979 and amended by the Fifth Session of the Eighth National People's Congress on 14 March 1997. The revised edition of the Code came into force on 1 October 1997. There was no specific criminal provision regarding computer crime before 1997. The first reported crime was theft, which involved transferring a bank's funds into a designated account. It took place in 1986 and was the first documented cybercrime in China.[42]

The section titled "Crimes of Disturbing Public Order" of the Criminal Law of the People's Republic of China combines all of the relevant cybercrime regulations into a single document. In addition to this, there are other crimes listed in the chapter that

---

[39] 最高检召开党组会研究打击网络犯罪举措 成立惩治网络犯罪维护网络安全研究指导组 [The Supreme People's Procuratorate held a party committee meeting to study measures to combat cybercrime and established a research steering group to punish cybercrime and maintain cybersecurity] (Sep. 10, 2022), available at https://www.spp.gov.cn/spp/tt/202004/t20200407_458139.shtml.

[40] Hong Lu et al., *A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States*, 5 Asian Criminology 127 (2010).

[41] 中华人民共和国刑法 [Criminal Law of the People's Republic of China of 1979] (Sep. 10, 2022), available at http://www.chnlawyer.net/law/subs/xingfa.html.

[42] Qianyun Wang, A *Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe* 42 (2017).

are not computer related. It should be noted that China took the first significant step toward criminalizing cybercrimes in February 2009 by including computer crimes in its Criminal Law.[43] However, initially, there were only a few articles in the Criminal Law relating to cybercrimes, namely, Articles 285, 286 and 287. Of course, it was impossible to foresee all of the different types of cyber offences. The development of information technology as well as the proliferation of criminal violations in cyberspace has led to the addition of new *corpus delicti* in legislation. The amendments of 2009 were not the last of the amendments in the sphere of cybercrime regulations. Amendments were also made in the years that followed. For instance, Amendment IX added three new Articles, 286A, 287A and 287B, in 2015.

Currently, the Criminal Law contains the following computer-related crimes.

Article 285 provides punishment for illegal intrusion into a computer information system, for unlawfully obtaining computer information system data and unlawful control of computer information system, as well as for providing intrusion into or unlawful control of computer information system programs and tools. It is important to note that the gravity of the circumstances and the damaging consequences can result in an increase in the punishment to as much as seven years of imprisonment. As with provisions, certain categories are unclear. For example, it is unclear which circumstances may be considered "serious" or "especially serious."

Article 286 provides punishment for destroying computer information systems and network service malfeasance. It includes the intentional production and dissemination of computer viruses and other destructive programs. Criminal liability is incurred if there are serious consequences. Therefore, the absence of serious consequences excludes criminal responsibility. Meanwhile, the term "serious consequences" is an estimated category that may entail difficulties in understanding and implementing in practice. This provision went into effect on 1 November 2019.

Article 286-1 provides punishment for refusal to fulfil the obligations of information network security management. Network service providers are obliged to comply with laws and administrative regulations. If any one of the conditions is not met, there shall be criminal liability for breaking the law and refusing to make corrections despite receiving an order from the regulatory authorities to take corrective measures. The first is the extensive and large-scale dissemination of illegal information. According to the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate,[44] the following circumstances constitute a large-scale dissemination

---

[43] Nir Kshetri, *Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations*, 13(1) Electronic Com. Res. 20 (2013).

[44] 最高人民法院 最高人民检察院 关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释 [Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Networks and Helping Information Network Criminal Activities of 2019] (Sep. 10, 2022), available at https://www.spp.gov.cn/spp/xwfbh/wsfbh/201910/t20191025_436138.shtml.

of information. Firstly, the dissemination of more than 200 illegal video files or more than 2,000 illegal pieces of information other than illegal video files; secondly, the dissemination of criminal information, the total quantity of which meets the relevant quantitative standards according to the corresponding ratio, thirdly, the distribution of illegal information to more than 2,000 user accounts; fourthly, the use of a communication group with a cumulative number of group member accounts of more than 3,000 or a social network with a cumulative number of followers of more than 30,000 to spread the illegal information; and fifthly, more than 50,000 views on the illegal information that has been posted. Additionally, there may be other circumstances that result in the massive dissemination of illegal data.

The other circumstances defining criminal liability are the leakage of user information that results in severe consequences or the existence of serious events that led to the destruction of evidence in criminal cases, among other serious circumstances.

According to the Interpretation, the phrase "other serious circumstances" in Article 286-1 includes the following: (a) failing to keep a log of the vast majority of users or failing to carry out the obligation of authenticating identity information; (b) refusing to make corrections despite repeated requests within two years; (c) causing information network services to be mainly used for illegal crimes; (d) allowing information network services and network facilities to be used to carry out cyberattacks, and as a consequence, seriously affecting production and life; (e) causing information network services to be used to commit crimes endangering national security, terrorist activity crimes, organized crimes of the underworld, corruption and bribery crimes, or other significant crimes; (f) causing damage to the information network of state organs or providing public services in the fields of communications, energy, transportation, water conservancy, finance, education and medical treatment, in a way that seriously affects production and life; as well as other severe violations of information network security management obligations. The last phrase indicates a non-exhaustive list of the circumstances entailing responsibility under criminal law. The main feature of such cases is the seriousness of the consequences.

If the acts constitute other crimes at the same time, then the offender should be convicted and punished under the provisions of the more severe punishment.

Article 287-1 provides punishment for the illegal use of information networks. Unlawful use of information networks is the use of systems to commit one of the following acts under "serious circumstances." Such criminal acts include the creation of websites and communication groups to commit fraud, instruction in criminal methods, the production or sale of prohibited items, controlled items and other illegal and unlawful activities; the publication of information related to the production or sale of drugs, weapons, obscene materials and other prohibited or regulated articles or other illicit and criminal information; or the publication of information to commit fraud and other illegal and unlawful activities. As in previous provisions, if the acts also constitute other crimes at the same time, the offender should be convicted and punished under the provisions of the more severe punishment.

Article 287-2 provides punishment for the assistance of cybercrime if the circumstances are severe. For instance, if unlawful use of networks is detected, technical support or advertising promotion are punishable under the Criminal Law. Technical support includes Internet access, server hosting, network storage, communication transmission among other services. If the acts also consist of other crimes committed at the same time, the liability falls under a stricter article.

According to the above-mentioned interpretation, the term "serious circumstances" as stipulated in Article 287-2 of the Criminal Law, includes supporting three or more entities; the payment settlement amount is more than 200,000 yuan; providing funds of more than 50,000 yuan through advertising; the illegal income is more than 10,000 yuan; those who have received administrative punishments within the past two years for illegally using information networks, assisting information cybercrime activities, or threatening the safety of computer information systems and assisting information cybercrime activities; the crime committed by the supported entities causes serious consequences; among other severe circumstances.

The mention of the possibility of punishing a person according to a norm with a more severe punishment in Articles 286-1, 287-1 and 287-2 indicates that the standards on computer-related crimes provided in these articles only apply if there are no signs of another more serious crime. When compared to other *corpus delicti* provided in the different sections, the above named provisions do not appear to be special rules. The extent to which certain specific provisions of the Criminal Law are applicable to a given case is directly dependant on the gravity of the offence.

Cybercrimes are not limited to the reviewed articles. Some categories are covered in other chapters. For example, Article 253-1 applies to cases involving personal information infringements acts. According to Article 253-1, "whoever sells or provides a citizen's personal information to others in violation of relevant state provisions or steals or otherwise illegally obtains a citizen's personal information will be sentenced to imprisonment of not more than three years or criminal detention, a fine, or both when the circumstances are serious. If the circumstances are 'especially serious,' the offence is punishable by three to seven years of imprisonment and a fine." Although there is no mention of the Internet or other networks in the provisions of this article, it may still relate to cybercrime if the personal information has been recorded electronically or published through electronic systems.

In May 2017, the Supreme People's Court and the Supreme People's Procuratorate of China released a judicial interpretation on the infringement of personal information in criminal cases. Effective 1 June 2017, the Interpretation defines the scope of personal data under the Criminal Law of the People's Republic of China. It clarifies other issues relevant to the criminal offence of infringement of personal information.[45]

[45] Library of Congress, *China: Judicial Interpretation on Infringement of Personal Information Released* (2017) (Sep. 10, 2022), available at https://www.loc.gov/law/foreign-news/article/china-judicial-interpretation-on-infringement-of-personal-information-released/.

In particular, "citizens' personal information" refers to all kinds of information, recorded electronically or otherwise, that, either alone or together with other information, can identify certain natural persons' identities or reflect certain natural persons' activities. Those who provide citizens' personal information to specific individuals, as well as those who publish citizens' personal information through information networks or other routes, shall be found to have "provided citizens' personal information" as provided for in Criminal Law Article 253-1. The Interpretation describes the situations that should be deemed "serious" and "especially serious circumstances."

The distinction between computer-related crimes and those covered by Article 253-1 is a necessary provision. Where a website or communications group is set up for the illegal criminal activities of unlawful acquisition, sale, or provision of citizens' personal information, and the circumstances are serious, it shall be convicted and punished as the crime of illegal use of information networks following the provisions of Article 287-1 of the Criminal Law; and where it simultaneously constitutes a violation of citizens' personal information, it shall be convicted and sentenced under the crime of violating citizens' personal information.

Where network service providers refuse to perform obligations of information network security management as provided for in the laws and administrative regulations and when they refuse to make corrections even after being ordered to do so by the oversight and regulatory departments, thereby leading to a leak of user citizens' personal information and causing serious consequences, they shall be convicted and punished under Article 286-1 of the Criminal Law for the crime of refusing to perform obligations of information network security management.

As is known, cybercrimes are varied, and sometimes it is difficult to foresee liability for all of the possible crimes that might be committed online or through telecommunications technology. In this situation, the provisions of Article 287 are very important. According to Article 287, anyone who uses computers to commit financial fraud, theft, embezzlement, embezzlement of public funds, theft of state secrets or other crimes shall be convicted and punished by the relevant provisions of this law. Thus, whether or not a crime is actually committed while using a computer, it will nonetheless result in criminal culpability. For example, advocating terrorism or extremism by way of distributing any information within a social network would be punishable under Article 120-3. Inciting ethnic hatred or ethnic discrimination through the Internet, if the circumstances are serious, shall be punishable under Article 249.

5. Criminal Liability for Cybercrimes in the Republic of South Africa

As elsewhere in the world, cybercrime poses a serious threat to South Africa. According to the most recent Accenture report, the attack surface has grown tremendously, and threat actors have targeted South African entities on all fronts

in 2019. For example, in September, Garmin South Africa disclosed that sensitive customer payment data entered into its shopping portal, shop.garmin.co.za, had been stolen. In October 2019, a breach in the network of a major South African city resulted in unauthorized access to its systems.[46] South Africa experienced a cross-industry spike in cyberattacks in 2019, making it the country with the third-highest number of cybercrime victims worldwide.[47]

In the Republic of South Africa, the provisions on criminal liability for cybercrimes are included in various regulations that protect a specific area of the digital sphere. The current legal framework legislation is a hybrid of different pieces of legislation and common law.[48] The laws in the country's statute book do not comprehensively and uniformly criminalize conduct which is internationally regarded as cybercrimes. The rules currently in the statute book are silo-based since various departments have enacted legislation to protect their interests in cyberspace, which has led to varying proscriptions of cybercrimes and penalization of such conduct. The common law is used to prosecute some of the offences, but it needs to grapple with new concepts such as intangible data.[49]

As mentioned, there are a number of provisions in different acts that may relate to offences involving information-telecommunications technology. For example, the Critical Infrastructure Protection Act[50] criminalizes furnishing, disseminating or publishing in any manner whatsoever information relating to the security measures applicable at or in respect of a critical infrastructure other than under Acts of Parliament that provide for the lawful disclosure of information. The Protected Disclosures Amendment Act, 5 of 2017,[51] which amends the Protected Disclosures Act, 2000, makes the disclosure of false information a criminal offence. The mentioned acts may take place through the Internet. Meanwhile, such crimes are not cybercrimes in the sense that the legislator intended simply because another Act uses the term "cybercrime."

---

46 Accenture, *Insight into the Threat Landscape of South Africa* (2020) (Sep. 10, 2022), available at https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf.

47 Bob Koigi, *South Africa Has Third-highest Number of Cybercrime Victims Globally, Report*, Africa Business Communities, 4 June 2020 (Sep. 10, 2022), available at https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/.

48 Cybersecurity Laws and Regulations South Africa (2020) (Sep. 10, 2022), available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa.

49 Memorandum on the Objects of The Cybercrimes and Cybersecurity Bill of 2017 (Sep. 10, 2022), available at https://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.pdf.

50 The Critical Infrastructure Protection Act of 2019 (Sep. 10, 2022), available at https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000.

51 The Protected Disclosures Amendment Act of 2017 (Sep. 10, 2022), available at https://www.gov.za/documents/protected-disclosures-amendment-act-5-2017-english-afrikaans-2-aug-2017-0000.

Thus, in the Republic of South Africa, the Electronic Communications and Transactions Act is the principal Act regulating crimes in the digital sphere.[52] Chapter VIII is devoted to "cybercrimes," which contains this term in the title of this chapter and includes such offences as unauthorized access to, interception of, or interference with data (Art. 86) and computer-related extortion, fraud and forgery (Art. 87). All of the offences that are listed are intentional acts and appear without authority or permission to do so.

The penalties vary depending on the type of cybercrime. Some cybercrimes are punishable with a fine or imprisonment for a period not exceeding twelve months. Such cybercrimes include, firstly, the access or interception of any data that is in violation of the Interception and Monitoring Prohibition Act, 1992; secondly, interference with data in a way that causes such data to be modified, destroyed or otherwise rendered ineffective. And thirdly, engaging in any of the following actions, such as producing, selling, offering to sell, procuring for use, design, adaption for use, distributing, or possessing any device, including a computer program or a component that is designed primarily to overcome security measures for the protection of data, or performing any of those acts concerning a password, an access code or any other similar kind of data with the intent to utilize such item unlawfully.

Consider a scenario in which the utilization of such a device or computer program is intended to unlawfully overcome security measures that are designed to protect such data or access to it. In that case, the punishment increases up to imprisonment for a period not exceeding five years. The same penalty may be imposed for any of the acts named above committed with the intent to interfere with access to an information system in order to deny service, even partially, to legitimate users.

Computer-related extortion, fraud and forgery are punishable with a fine or imprisonment for a period not exceeding five years. Computer-related extortion is the commission of any unlawful action involving a computer device and program or the threat to do so, in order to obtain any illegal proprietary advantage by undertaking to cease or desist from such activity, or by undertaking to restore any damage caused as a result of those actions.

Computer-related fraud and forgery refers to any of the mentioned cyber acts committed to obtain any unlawful advantage by causing the production of forged data with the intent that it be considered or acted upon as if it were authentic.

The mere attempt to commit a cybercrime must be punishable by a fine or imprisonment just as in the case of the actual commission of the offence and the punishment may be carried out in full. Aiding and abetting someone to commit a cybercrime is also punishable. However, as is generally known, not all countries follow this principle. For example, the Criminal Code of the Russian Federation

[52] The Electronic Communications and Transactions Act of 2002 (Sep. 10, 2022), available at https://www.gov.za/documents/electronic-communications-and-transactions-act.

regulates that the penalty for attempting to commit a crime cannot exceed three-quarters of the maximum punishment for that crime. It seems that the degree of danger posed by a cybercrime that has been committed differs from a crime that has been attempted. However, the full penalty appears to be justified in order to counter the spread of cybercrime.

It is important to note that South Africa is currently in the process of rationalizing its legislation concerning cybercrimes. The National Cybersecurity Policy Framework was released at the end of 2015 (SSA, 2015), followed by drafts of the Cybercrimes and Cybersecurity Bill (Department of Justice and Correctional Services, 2017).[53]

The National Cybersecurity Policy Framework for South Africa defines cybercrime as illegal acts, the commission of which involves the use of information and communication technologies.[54] The Cybercrimes and Cybersecurity Bill of 2017 is now known as the Cybercrimes Act of 2019[55] The primary aim of the Act is to deal with cybercrimes and the punishment for committing them. This Act combines all of the prohibited offences in digital space into a unified code of cybercrimes. The provisions of the Bill illustrate a wide range of cybercrimes, including the following: unlawful access; unlawful interception of data; unlawful acts in respect of software or hardware tools; unlawful interference with data or computer programs; unlawful interference with computer data storage medium or computer system; unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data or devices; cyber fraud; cyber forgery and utterance; and cyber extortion.

Malicious communications include, among other things, data messages that incite damage to property or violence or are harmful and the distribution of data messages containing intimate images without consent.

Without a doubt, the development of this Bill is a progressive step forward for the country. The main advantage is the unification of cybercrime provisions into a single act as well as the inclusion of a detailed description of each offence. However, there are some controversial issues.

First, there is no mention of the term "cybercrime" in any of the provisions that are devoted to definitions. It seems illogical because it is a crucial category. Moreover, the term "cybercrime" appears in the title of the Act as well as in the title of Chapter 2. At the same time, Chapter 2 includes two parts. The first section is devoted to cybercrime. The second section describes malicious communications that may also constitute cybercrimes; however the term "cybercrime" is absent from this section. Second, it appears that some cybercrimes are outside the purview of this Act's

---

53 Van N. Brett, *An Analysis of Cyber-Incidents in South Africa*, 20 Afr. J. Info. & Comm. 113, 115 (2017).

54 The National Cybersecurity Policy Framework for South Africa of 2015 (Sep. 10, 2022), available at http://cybercrime.org.za/docs/National_Cybersecurity_Policy_Framework_2012.pdf.

55 The Cybercrimes Bill of 2019 (Sep. 10, 2022), available at https://www.gov.za/sites/default/files/gcis_document/201811/bill06b-2017.pdf.

regulation. For instance, in accordance with Provision 12 of the Act, the common law offence of theft must be interpreted in such a way so as to not exclude the theft of an incorporeal. Perhaps there are some other crimes that may be related to cybercrimes.

Third, it appears complicated to quickly comprehend what penalty corresponds to which offence because the legislator indicates the numbers of the law provisions for the violation of which there will be punishment. Accordingly, in order to determine what crimes are punishable, it is necessary to refer to the corresponding article of the law every time.

Conclusion

In concluding the assessment of the legislative provisions on criminal liability for cybercrimes in the BRICS countries, it is possible to distinguish between the general and state-specific features of each of the countries. In Brazil, the different chapters of the Penal Code and other laws contain a number of cybercrime provisions. There is no single division in the Code for such crimes. Various acts that regulate specific fields of activity and establish penalties for breaking adopted rules contain cybercrime provisions as well. Meanwhile, the term "cybercrime" is absent in Brazilian law. However, the commission of a crime through telecommunications networks is recognized as a circumstance that increases the severity of punishment for such offences. In addition, the law recognizes that any crime may be committed through electronic and telecommunications systems, yet there is no mention of this method in the relevant articles.

In Russia, cybercrime provisions include a particular chapter that establishes penalties for crimes committed in the sphere of computer information. In addition, articles in other sections of the Criminal Code of the Russian Federation may occasionally contain an indication of the commission of a crime using electronic or information and telecommunications networks as a sign of a *corpus delicti*. The term "cybercrime" does not appear anywhere in the Russian legislation either.

In India, cybercrime provisions are contained in the Information Technology Act, the Indian Penal Code and the Special and Local Laws. There is a wide range of cybercrimes in India. Official reports actively use the term "cybercrime." According to statistics, certain offences are classified as cybercrimes if they take place online. However, the law does not specifically indicate information technology as a possible method of committing the crime.

In China, the section titled "Crimes of Disturbing Public Order" of the Criminal Law of the People's Republic of China not only regulates computer-related crimes, but also includes cybercrime standards. Other chapters also contain some general cybercrime provisions. Moreover, Chinese legislation confirms that if the commission of any crime involves the use of a computer, regardless of whether there is any

mention of this in a definite article, criminal liability will follow in any case. The Criminal Law contains numerous unclear *corpus delicti* features, which are interpreted by the Supreme People's Court and the Supreme People's Procuratorate based on the particular circumstances of each case.

In South Africa, both statute law and common law contain cybercrime provisions. The Electronic Communications and Transactions Act may be regarded as the principal act, regulating digital sphere crimes and including the term "cybercrime." Currently, South Africa is in the process of reforming its cybercrime laws. Additionally, the Cybercrimes and Cybersecurity Bill combines all of the cybercrime provisions into a single act and establishes a new *corpus delicti* according to international requirements.

Each of the BRICS countries has specific features in the regulation of liability for cybercrime that appear to be caused by the particularities of their legal systems, the situation with cybercrimes and the attitude of legislators towards cybersecurity problems. At the same time, all of the countries are striving to protect data from unlawful actions while seeking to expand their understanding of cybercrimes and establish criminal liability for them. In these aspects, it would be worthwhile to develop supranational provisions in order to ensure cybercrime protection by legal means.

To effectively counter cybercrime at the interstate BRICS level, it would be desirable to enact a single document containing a common understanding of cybercrimes and the various types of cybercrime that can be uses by all five countries. It appears conceivable to classify cybercrimes into two large groups: special cybercrimes committed in the field of computer information and general criminal cybercrimes that are executed using information technology to commit any common criminal offences (for example, theft, assisted suicide, public dissemination of criminally significant information and so on.). This division will allow countries to find common ground on the issue of criminal responsibility for cybercrime.

Additionally, it would be preferable to introduce in the national legislation of each country a provision that allows for the possibility of recognizing as cybercrime any act committed through the use of information and telecommunications technologies. This provision will make it possible to detect new and emerging forms of committing criminal acts in the digital space or through telecommunications networks.

Finally, analyzing the law enforcement activities of the national judiciary can facilitate a deeper understanding of the problems of criminal liability for cybercrimes in the BRICS countries, which also appears to be a promising area for further research.

Acknowledgements

I wish to thank Valeria Evdash, Director of the Center for Academic Writing "Impulse," University of Tyumen, for her valuable advice during the preparation of this manuscript.

References

Akhgar B. et al. (eds.). *Cyber Crime and Cyber Terrorism Investigator's Handbook* (2014). https://doi.org/10.1016/C2013-0-15338-X

Arya N. *Cyber Crime Scenario in India and Judicial Response*, 3(4) International Journal of Trend in Scientific Research and Development 1108 (2019). https://doi.org/10.31142/ijtsrd24025

Azad M.M. et al. *Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law*, 3(5) International Journal of New Technology and Research 1 (2017).

Brett V.N. *An Analysis of Cyber-Incidents in South Africa*, 20 African Journal of Information and Communication 113 (2017). https://doi.org/10.23962/10539/23573

Chang L.Y. *Cybercrime in the Greater China Region. Regulatory Responses and Crime Prevention across the Taiwan Strait* (2012).

Dasgupta M. *Cyber Crime in India – A Comparative Study* (2009).

Grabosky P. *The Internet, Technology, and Organized Crime*, 2 Asian Criminology 145 (2007). https://doi.org/10.1007/s11417-007-9034-z

Kshetri N. *Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations*, 13(1) Electronic Commerce Research 41 (2013). https://doi.org/10.1007/s10660-013-9105-4

Kshetri N. *Cybercrime and Cybersecurity Issues in the BRICS Economies*, 18(4) Journal of Global Information Technology Management 245 (2015). https://doi.org/10.1080/1097198X.2015.1108093

Lehto M. & Neittaanmäki P. (eds.). *Cyber Security: Analytics, Technology and Automation* (2015). https://doi.org/10.1007/978-3-319-18302-2

Lu H. et al. *A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States*, 5 Asian Criminology 123 (2010). https://doi.org/10.1007/s11417-010-9092-5

Malik J.K. & Choudhury S. *Privacy and Surveillance: The Law Relating to Cyber Crimes in India*, 9(12) Journal of Engineering, Computing and Architecture 83 (2019).

Mitrovic Z. & Thakur S.C. *Positioning South Africa in the BRICS Cybersecurity Context: A Strategic Perspective*, in Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch Univ, South Africa 251 (2019).

Mittal S. & Singh A. *A Study of Cyber Crime and Perpetration of Cyber Crime in India*, in Evolving Issues Surrounding Technoethics and Society in the Digital Age 171 (2014). https://doi.org/10.4018/978-1-4666-6122-6.ch011

Pawar S. & Kolekar Y. *Essentials of Information Technology Law* (2015).

Subrahmanian V.S. et al. *The Global Cyber-Vulnerability Report* (2015).

Wang Q. A *Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe* (2017).

Коробеев А.И., Дремлюга Р.И., Кучина Я.О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации //

Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 416–425 [Korobeev A.I. et al. *Cybercrimes in the Russian Federation: Criminological and Criminal Law Analysis of the Situation*, 13(3) Russian Journal of Criminology 416 (2019)]. https://doi.org/10.17150/2500-4255.2019.13(3)

Устинова Т.Д. Склонение к самоубийству или содействие самоубийству: критический анализ // Lex Russica. 2020. № 3. С. 151–158 [Ustinova T.D. *Encouragement to Commit Suicide or Assisting with Suicide: Critical Analysis*, 3 Lex Russica 151 (2020)].

Information about the author

Liliya Ivanova (Tyumen, Russia) – Associate Professor, Department of Criminal Law, University of Tyumen (6 Volodarskogo St., Tyumen, 625003, Russia; e-mail: l.v.ivanova@utmn.ru).