BRICS Law Journal

Volume X (2023) Issue 1

The journal's founder is

University of Tyumen
UTMN

ISSN 2412-2343 (Online)

ISSN 2409-9058 (Print)

Key title: BRICS law journal (Print)
Abbreviated key title: BRICS law j. (Print)
Variant title: BRICS LJ

Contacts: bricslaw@gmail.com

"BRICS Law Journal" is registered
by the Federal Service for supervision
of legislation in mass communications
and cultural heritage protection (Russia).
Reg. No. FS77-69105 of March 14, 2017.

BRICS LAW JOURNAL (BRICS LJ)

An independent, professional peer-reviewed academic legal journal.

Aims and Scope

The *BRICS Law Journal* is the first peer-reviewed academic legal journal on BRICS cooperation. It is a platform for relevant comparative research and legal development not only in and between the BRICS countries themselves but also between those countries and others. The journal is an open forum for legal scholars and practitioners to reflect on issues that are relevant to the BRICS and internationally significant. Prospective authors who are involved in relevant legal research, legal writing and legal development are, therefore, the main source of potential contributions.

The *BRICS Law Journal* is published in English and appears four times per year. All articles are subject to professional editing by native English speaking legal scholars. The BRICS LJ is indexed by Scopus.

Notes for Contributors

Manuscripts must be the result of original research, not published elsewhere. Articles should be prepared and submitted in English. The BRICS LJ doesn't accept translations of original articles prepared not in English. The BRICS LJ welcomes qualified scholars, but also accepts serious works of Ph.D. students and practicing lawyers.

Manuscripts should be submitted electronically via the website *www.bricslawjournal.com*. Articles will be subjected to a process of peer review. Contributors will be notified of the results of the initial review process within a period of two months.

Citations must conform to the *Bluebook: A Uniform System of Citation*.

TABLE OF CONTENTS

GUEST EDITORS' NOTE ON LAW AND DIGITAL TECHNOLOGIES: THE WAY FORWARD

ELIZAVETA GROMOVA,

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

DANIEL BRANTES FERREIRA,

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

https://doi.org/10.21684/2412-2343-2023-10-1-5-6

Recommended citation: Elizaveta Gromova & Daniel Brantes Ferreira, *Guest Editors' Note on Law and Digital Technologies: The Way Forward*, 10(1) BRICS Law Journal 5–6 (2023).

This Special Issue of the BRICS Law Journal is devoted to one of the most intriguing, promising and highly relevant research areas – the synergy of law and digital technologies. At present, digital technologies have been capturing all spheres of our life. Its potential is significant, and opportunities for application are genuinely limitless. Its emergence is also connected with risks and threats that can be minimized by designing proper regulations. At the same time, the design of such regulation represents a massive challenge to the law and lawmakers and requires in-depth research. Therefore, discussing state-of-the-art issues and defining future steps in regulating digital technologies worldwide is crucial.

That was the idea of creating the Research Group "Law, Digital Technologies & ADR." The Group was launched in 2021 with the primary aim – of creating an international virtual hub for research and cross-cultural collaboration in the sphere of Law and Digital Technologies from the global and comparative perspective. The Group united young and experienced researchers from 7 countries (Brazil, USA, Russia, Italy, India, Portugal and Uganda) and was co-hosted by South Ural State University, Ambra University, and Universidade Candido Mendes.[1]

---

[1] Research Group "Law, Digital Technologies & ADR" (official website) (Jan. 12, 2023), available at https://adrdt.ambra.education/.

The Conference "Law and Digital Technologies: The Way Forward" was held to provide the participants of the Research Group with the opportunity to present the results of their research. This Conference also gave a unique chance for researchers to discuss law and digital technologies and do international networking.[2] The Conference had more than 120 participants from Russia, Brazil, India, the USA, Italy, Spain, the United Kingdom, Slovenia, Poland, Romania, etc.

BRICS Law Journal was the partnering Journal of the Research Group and the Conference, and this is how the Special Issue "Law and Digital Technologies: The Way Forward" was born. This Special Issue is a collection of the best papers of the Conference participants and experts on highly relevant topics in the sphere of law and digital technologies convergence. Here the readers will find solutions to the cutting-edge legal issues of using digital technologies in criminal law and procedure, labor relations, privacy and personal data protection. The special issue is international with the contributions of authors from Russia, Brazil, United Arab Emirates, India, China, and Italy.

We genuinely hope readers will find this Special Issue valuable and informative. The papers gathered here may be regarded as the natural step forward for lawmaking and future research in law and digital technologies.

We want to thank all authors, Research Group and Conference participants for their papers. And, of course, our unique and enormous gratitude to professor Elena Gladun, the Editor-in-Chief of the BRICS Law Journal, for her constant support of our projects and the significant contribution she is making to develop legal research and collaboration!

[2] Conference "Law and Digital Technologies: The Way Forward" (official webpage) (Jan. 12, 2023), available at https://adrdt.ambra.education/conference/.

ARTICLES

THE LEVEL OF CYBERSECURITY OF THE BRICS MEMBER COUNTRIES IN INTERNATIONAL RATINGS: PROSPECTS FOR COOPERATION

OKSANA OVCHINNIKOVA,

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

NITEESH KUMAR UPADHYAY,

Symbiosis Law School, Noida Campus (Symbiosis International Deemed University, Pune, India)

https://doi.org/10.21684/2412-2343-2023-10-1-7-34

Creating a legal framework for cybersecurity is a key factor in the digitalization of an economy. The interaction between the BRICS member countries has undergone a digital transformation, which has improved their ability to work together economically and strengthened the growing influence of these countries in the international arena. The purpose of the present study is to determine the potential of the BRICS member nations to form a joint cybersecurity strategy. The authors put forward a hypothesis that the formation of an effective cybersecurity system is possible only with a sufficient level of development of information and communication technologies and a high degree of digitalization of interstate governance. The scientific novelty of this research lies in its complex approach to the scientific and theoretical analysis of the problems of ensuring cybersecurity in the BRICS member countries, on the basis of which it identifies the common areas for cooperation. The research methodology is based on establishing a correlation between the indicators of e-government development and the criteria for state cybersecurity, followed by a comparative analysis. As a quantitative indicator, the authors use the data of the E-Government Development Index for the BRICS member countries from 2010 to 2018. Additionally, the level of maturity of each country's national cybersecurity system is reflected in the rating of the International Telecommunication Union (ITU). Based on the ITU rating, we assess the cybersecurity efficiency of the BRICS member countries versus other countries. The findings of the research lead the authors to the conclusion that state control over cyberspace and the availability of a national strategy are prerequisites for achieving a high level of cybersecurity.

Keywords: national security; cybersecurity; cyberthreats; cyberattack; information infrastructure; cyber terrorism; BRICS.

Recommended citation: Oksana Ovchinnikova & Niteesh Kumar Upadhyay, *The Level of Cybersecurity of the BRICS Member Countries in International Ratings: Prospects for Cooperation*, 10(1) BRICS Law Journal 7–34 (2023).

Table of Contents

Introduction

Cybersecurity is a critical area of global regulatory interest.[1] States seek to preserve their access to and safeguard their dependence on cyberspace, which frequently entails a departure from set norms.[2] Since 2002, the United Nations has adopted several resolutions aimed at the creation of a global cybersecurity culture.[3] However, there are still no international law institutions in place to ensure the appropriate control. This has led to competition between the states for priority in this area. The national digital economic infrastructures of the BRICS member countries have a leading position in global e-commerce. China dominates with a turnover of $2.09 trillion, while India is the fastest growing market.[4] An increase in the share of digital transactions between the BRICS member countries will allow them to significantly increase sales turnover and neutralize the disadvantages of their fragmented geographical location. Unifying

---

1 Dimitra Markopoulou et al., *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, 35(6) Computer L. & Security Rev. 1 (2019).

2 Pallavi Khanna, *State Sovereignty and Self-Defence in Cyberspace*, 5(4) BRICS L.J. 139 (2018).

3 UN, *Creation of a Global Culture of Cybersecurity: Resolution/adopted by the General Assembly*, United Nations Digital Library System, 31 January 2003 (Feb. 2, 2023), available at https://digitallibrary.un.org/record/482184?ln=en.

4 Global Ecommerce 2020, *Ecommerce Decelerates amid Global Retail Contraction but Remains a Bright Spot*, Report by Ethan Cramer-Flood, 22 June 2020 (Feb. 2, 2023), available at https://www.emarketer.com/content/global-ecommerce-2020#page-report.

the BRICS member countries would result in an increase in the power of the overall international system. By 2020, the total GDP of the BRICS member countries amounted to 25% of the global GDP ($21 trillion), and their share in the international commodity turnover amounted to almost 20% ($6.7 trillion). Mutual exports of the countries of 'the five' grew by 45% (from 2015 to 2019).

The focus on the digitalization of economic interaction, despite its potential advantages, is linked with certain risks. An increase in the number of operations in cyberspace inevitably leads to an increase in security threats and incidents. Cases of unauthorized penetration into the digital infrastructure of governments and businesses cannot be prevented through technological methods. They elicit a major public response in the mass media and on the Internet. The transnational nature of cyberattacks leads to the appearance of tensions between states, which in turn give rise to the need to ensure security in cyberspace by legal means.

The national policy of a state can be defined and institutionalized in cyberspace through the adoption of a cybersecurity strategy. The components of an effective cybersecurity strategy are not universal. They are determined by the extent to which the information and communications technology (ICT) of a state has developed, as well as by the peculiarities of its international and domestic policies and its management practices.[5] Cybersecurity strategy also largely depends on the proportion of the population using ICT tools in their day-to-day life.

Researchers have been actively exploring the cybersecurity strategies of developed countries, which ensure the exchange of positive experience and advanced development. Cybersecurity is defined as a means not only of protecting and defending society and its essential information infrastructures but also a way of prosecuting national and international policies through the means of information technology means.[6] According to numerous industry experts, a state's ability to prevent fundamental cyberthreats and develop a national cyber protection policy directly depends on the development level of the infrastructure meeting the requirements of international cybersecurity indices.[7] A number of countries also have their own response teams for potential cyberattacks, for example in India The purpose of the computer emergency response team is to protect and prevent any kind of cyberattacks on Indian computer system, computer network and computer resources.[8] There is an interrelation between the legal framework and the formation of cyberattack response authorities:

---

5 Guide to Developing a National Cybersecurity Strategy (2018) (Feb. 2, 2023), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

6 Tim Stevens, *Global Cybersecurity: New Directions in Theory and Methods*, 6(2) Pols. & Governance 1 (2018).

7 Olga Vakulyk et al., *Cybersecurity as a Component of the National Security of the State*, 9(3) J. Security & Sustainability Issues 775 (2020).

8 The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (2013) (Feb. 2, 2023), available at https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf.

Cybersecurity breaches cannot be contained within the borders of a single country. Cyberattacks are launched in cyberspace, the actual boundaries of which cannot be determined.[9] When it comes to cybersecurity, the issue of jurisdiction raises serious concerns and calls for improved international cooperation in the development of a legal, technical and judicial system.

All of the BRICS member countries are considered developing countries.

> However, the BRICS association is gradually going beyond the scope of only economic cooperation and acquiring the features of institutionalization of supranational education. The logic of the stages of the unification of the BRICS member nations demonstrates rapprochement in various areas of interstate cooperation.[10]

Nevertheless, some scholars believe that in forming cybersecurity strategies, states strive to increase cyber training both in defense and offense, viewing these strategies as a new opportunity to develop their military potential.[11] To this end, the strengthening of cooperation between the BRICS member countries is limited by various types of government control that foster mutual distrust and asymmetry of power within the group.[12] In the context of BRICS, stronger countries are often characterized by aggressive behavior in cyberspace, which can lead to the loss of digital sovereignty by less developed countries.[13]

The key problem is that the contrary viewpoints are not supported by specific data. We are of the opinion that in order to determine the potential for cybersecurity cooperation between the BRICS member countries, it is necessary to:

- Analyze the problems of introducing ICT in each of the countries.
- Carry out a comparative analysis of national cybersecurity strategies.
- Highlight promising areas for cooperation.

Studying these data will allow us to determine the possible level of cooperation and assess the prospects for the formation of a joint strategy.

The BRICS member countries can continue to strengthen their positions in the global economy through the formation of a single digital market. Digital transformation requires an integrated approach. New technologies should not be introduced without control. States should guide the use of technologies and respond flexibly to ongoing

---

[9] Hans de Bruijn & Marijn Janssen, *Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies*, 34(1) Gov't Info. Q. 1 (2017).

[10] Evgenii Nikitin & Mensah C. Marius, *Unified Digital Law Enforcement Environment – Necessity and Prospects for Creation in the "BRICS Countries"*, 7(2) BRICS L.J. 66 (2020).

[11] Ali Burak & Daricili Barış, *Analysis of the Cyber Security Strategies of People's Republic of China*, 14(28) Güvenlik Stratejileri Dergisi (J. Security Strategies) 1 (2018).

[12] Rodrigo Fracalossi de Moraes, *Whither Security Cooperation in the BRICS? Between the Protection of Norms and Domestic Politics Dynamics*, Global Policy (June 2020) (Feb. 2, 2023), available at https://ssrn.com/abstract=3632389.

[13] Brett Van Niekerk, *South Africa and the Cyber Security Dilemma*, 18(2) J. Info. Warfare 96 (2019).

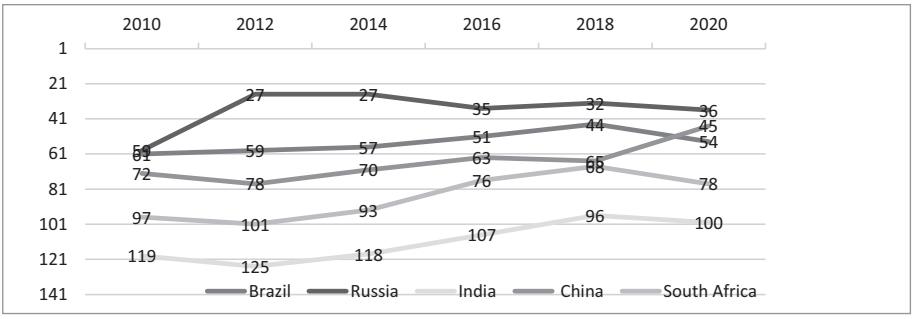
changes. It is impossible to ensure the national cybersecurity of each country without international cooperation. Successful models from other countries should serve as a point of growth to upgrade national cybersecurity strategies.[14] The adoption of a joint cybersecurity strategy among BRICS member countries could significantly increase the influence of this bloc in the international community.

1. E-Government as a Basis for the Formation of a National Cybersecurity System

An integrated approach must be used to assure national cybersecurity. States should guide the use of technologies and respond flexibly to ongoing challenges. The development of e-government and online provision of public services reflects the level of integration of public management of economic digitalization and serves as the basis for the formation of a national cybersecurity system. Only a developed e-government can ensure adequate interaction of cybersecurity subjects at all levels in order to prevent and suppress cyberattacks.[15]

Analysis of the data from the United Nations E-Government Development Index showed that the BRICS member countries are making efforts to introduce ICT. Having examined the data from 2010 to 2020, we see that the indicators of the e-development level do not have positive dynamics in all the countries. This indicates existing problems to be studied in detail (Figure 1).[16]

Figure 1: **E-Government Development Index of the BRICS member countries**



Source: Author, based on UN open data

[14] ITU, *ITU National Cybersecurity Strategy Guide*, International Telecommunication Union (September 2011) (Feb. 2, 2023), available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf.

[15] FCC, *Cyber Security Planning Guide*, Federal Communications Commission (October 2012) (Feb. 2, 2023), available at https://transition.fcc.gov/cyber/cyberplanner.pdf.

[16] Brig V. Anand, *A Perspective on BRICS Development Strategies: Prospects and Issue*, Vivekananda International Foundation, 11 September 2017 (Feb. 2, 2023), available at https://www.vifindia.org/article/2017/september/11/a-perspective-on-brics-development-strategies-prospects-and-issues.

Let us consider the effectiveness of the development of e-government in each of the BRICS member countries. The main aspects for our analysis are the condition of online services, telecommunication technologies and human capital.

1.1. E-Government in the Russian Federation

Russia is the leader in digitalization among the BRICS member states and is ranked 36th on the 2020 United Nations E-Government Survey. Public policy in Russia has consistently emphasized digitalization; however, further development is hampered by the insufficiently high level of information and communication infrastructure, which is rated at 0.7723 in the same UN Survey.[17] This gap is explained by the large size of the country's territory and the harsh climatic conditions in thirty percent of the regions.

Solutions to bridge this gap are included in the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030.[18] Its objectives include the development of the information and communication infrastructure and the creation of a new technological basis for the development of the economy and social sphere. The main priority of the Strategy is to improve the living standards of the population through the widespread use of national ICT.

The Digital Economy national project is being implemented from 2018 to 2024 to achieve the objectives of the Strategy. Its task is to create a stable and secure information and telecommunications infrastructure that allows for the high-speed transmission, processing and storage of large amounts of data available to all organizations and households.[19] Officials plan to develop and launch the Federal Spatial Data Web Portal – a state information system; connect public and local self-government authorities to the Internet; introduce interdepartmental electronic document management using electronic signatures in the activities of federal and regional executive authorities; create a platform to exchange information between the state, citizens as well as profit and non-profit organizations (Digital Profile infrastructure); develop and launch a protected digital environment for audiovisual interaction between governmental authorities, organizations and citizens at the federal, regional, and municipal levels; and launch an Electronic Passport for RF citizens.[20]

---

[17] 2020 United Nations E-Government Survey (July 2020) (Feb. 2, 2023), available at https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf.

[18] Decree of the President of the Russian Federation, 9 May 2017 (Feb. 2, 2023), available at http://www.kremlin.ru/acts/bank/41919.

[19] 'Digital Economy' National Project, 18 September 2020 (Feb. 2, 2023), available at http://static.government.ru/media/files/3b1AsVA1v3VziZip5VzAY8RTcLEbdCct.pdf.

[20] Digital Public Administration Factsheet, 20 September 2020 (Feb. 2, 2023), available at https://joinup.ec.europa.eu/sites/default/files/inline-.files/Digital_Public_Administration_Factsheets_Sweden_vFINAL.pdf.

1.2. E-Government in China

China is ranked 45th in the 2020 UN Rating. From 2010 to 2018, the country smoothly climbed from 93rd to 68th place. However, in 2020, China made a sharp leap, rising twenty positions at once. At the same time, China came close to the ideal model in terms of the quality of its online services. The index for this indicator was 0.9059.[21]

The active introduction of e-government and the digitalization of government control are driven by economic needs. The largest transnational companies have begun to actively enter the Chinese market. However, investments can only be attracted with the availability of digital tools for prompt cooperation with regulatory agencies and the compliance of the e-government development level with global standards.

The barrier to attracting international capital was the excessive bureaucratization of China's government control system. Each day, government agencies issue a large number of regulations, which are constantly updated and amended. Furthermore, the Golden Bridge Project was launched to ensure their timely distribution. This project aims to create a fundamental infrastructure for national information systems and provide assistance to administrative authorities. The creation of government websites allows individuals and organizations to gain prompt access via the Internet to relevant information and services online.

The development of e-government in China has ensured annual market growth rates of 12% to 17% (10 years before 2017) and opened up the market with a total value of 272.2 billion yuan (about 38 billion dollars).[22]

In May 2019, a national public services platform was launched, which is linked to 46 departments of the State Council and 32 local self-government authorities. This platform improved the general capabilities of the government services on the Internet. As of December 2019, the platform had 339 million registered users, which means that one out of three Internet users in China signed up on the platform.[23] The capabilities of the online service have improved. Administrative approval procedures have been simplified. Many permits can be granted online. Herewith, the number of citizens using e-government services is only 23.4% of the population, which is caused by the digital divide between different segments of the population. There is inequality both in the provision of access to ICT and in its use.

However, China is still considered an emerging economy with tight government control. The state not only encourages the development of ICT but also directs its

---

21 Masoud Shayganmehr & Gholam A. Montazer, *A Novel Model for Assessing E-Government Websites Using Hybrid Fuzzy Decision-Making Methods*, 1468 Int'l J. Computational Intelligence Systems (2021) (Feb. 2, 2023), available at https://www.atlantis-press.com/journals/ijcis/125956171/view.

22 Lin Rubi, *China's E-Government Drive Creates $38bn Market*, Nikkei Asia, 8 October 2019 (Feb. 2, 2023), available at https://asia.nikkei.com/Business/Business-trends/China-s-e-government-drive-creates-38bn-market.

23 Ji Jing, *China Has Made Remarkable Progress in Delivering E-Government Services*, Beijing Review, 20 July 2020 (Feb. 2, 2023), available at http://www.bjreview.com/Nation/202007/t20200720_800214813.html.

efforts towards establishing state control over the Internet space on its territory, which keeps the rest of the world from not knowing what is going on in China, as we have seen during the COVID-19 pandemic situation.

> The "Great Firewall" prevents Internet users in China from visiting many foreign websites for one reason or the other and blocking them completely.[24]

Internet access capabilities differ significantly among the different departments in China. Metropolitan areas and large cities have a developed network and robust websites for local government authorities. Thus, the 2020 UN rating cites the unified system of public services in Shanghai as an example of successful e-government.[25] Over 29.21 million individuals and over 2.08 million legal entities are registered on the municipal e-government portal. The portal not only allows users to handle a wide range of routine matters, such as registering a business and paying utility bills, but also provides information on the various types of emergencies and the emergency services that are available to deal with them.

The level of access to information and communications technologies in Shenzhen, Hangzhou and Guangzhou in Eastern China is nearly three times the national average.[26] However, in Longnan in the Gansu province, Bijie and Tongren in the Guizhou province, Ganji in the Sichuan province and Hetian in the Xinjiang province, network access is only half the national average.[27]

Another reason for the gap is the large proportion of elderly people (18.1% of the total[28]). Furthermore, 17.95% of the population is below the age of fifteen years, and as a result, they are unable to use digital services due to age limitations.[29]

---

[24] Sonali Chandel et al., *The Golden Shield Project of China*: *A Decade Later an In-depth Study of the Great Firewall*, in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 111 (2019).

[25] Jing, *supra* note 23.

[26] Chuanglin Fang et al., *The Sustainable Development of Innovative Cities in China: Comprehensive Assessment and Future Configuration*, 24 J. Geographical Sci. (2014) (Feb. 2, 2023), available at https://www.researchgate.net/publication/267340319_The_sustainable_development_of_innovative_cities_in_China_Comprehensive_assessment_and_future_configuration.

[27] Zhouying Song et al., *China's Prefectural Digital Divide: Spatial Analysis and Multivariate Determinants of ICT Diffusion*, 52 Int'l J. Info. Mgmt. (Article 102072) (2020).

[28] Huang Lanlan et al., *Narrowing 'Digital Divide': China Steps up Efforts to Better Serve the Elderly in Digital Age*, Global Times, 2 December 2020 (Feb. 2, 2023), available at https://www.globaltimes.cn/content/1208770.shtml.

[29] C. Textor, *Population Distribution in China in 2020, by Broad Age Group*, Statista, 19 May 2021 (Feb. 2, 2023), available at https://www.statista.com/statistics/251524/population-distribution-by-age-group-in-china/.

1.3. E-Government in Brazil

Over the past two years, Brazil has moved down in the UN rating significantly (from 44th to 54th). However, the quality and level of the online services provided are very high. A peculiar feature of Brazil is the constant feedback between government service providers and consumers. One of the distinguishing features of Brazil that makes it stand apart from the other BRICS countries is the way in which its citizens actively contribute to the creation of new digital projects and in the improvement of those that already exist. The resolution of digital issues at a consumer level is a unique practice that has the potential to be of long-term benefit in any country's digital policy.[30]

The National Debureaucratization Council coordinates the Effective Brazil (Brasil Eficiente) program, which aggregates the measures of all federal public service institutions, including ministries and the presidency. The goal of the program is to modernize relations between the government and society and make life easier for citizens and organizations that use public services. The program aims to optimize public services, simplify the procedure for obtaining services, and reduce costs.[31] For example, Decree No. 9094, dated 17 July 2017, states that federal government authorities should not request documents or information from citizens who are already registered in federal government databases.

The first version of the Brazilian Digital Government Strategy was implemented in 2016–2018. Several digital identity projects have been recently completed, for example, Brazilian driver's licenses, Brazilian voting IDs (Título Eleitoral), worker's IDs (Carteira de Trabalho) and the electronic version of the National ID Card and Registry (enacted by Law no. 13,444/2017). The delivery of digital services has also been largely improved with the implementation of a services portal that aggregates information (or e-services) from the majority (or all) of Brazilian federal entities.[32]

In May 2018, an updated version of the Strategy was presented. The document sets five strategic goals: (a) promoting the availability of open government data; (b) promoting transparency through ICTs; (c) expanding and innovating in the provision of digital services; (d) exchange and integration of data, processes, systems, services and infrastructure and (e) improving social participation in the life cycle of public policies and services.[33]

---

30 UNCTAD, *Digital Economy Report 2019*, United Nations, 4 September 2019 (Feb. 2, 2023), available at https://unctad.org/system/files/official-document/der2019_en.pdf.

31 The Effective Brazil Program, Brazilian Government Portal, 16 December 2017 (Feb. 2, 2023), available at http://www.brasileficiente.gov.br/.

32 Digital Government Review of Brazil, *Towards the Digital Transformation of the Public Sector*, OECD Digital Government Studies, 28 November 2018 (Feb. 2, 2023), available at https://doi.org/10.1787/9789264307636-en.

33 Brazilian Digital Government Strategy, 21 May 2018 (Feb. 2, 2023), available at https://www.governodigital.gov.br/EGD.

An important result of the Strategy was the creation of the National Digital Transformation System and the Interdepartmental Committee for Digital Transformation (CIT Digital), which became the main controlling bodies in the implementation of the digital policy.[34]

1.4. E-Government in South Africa

The Republic of South Africa (RSA) also dropped in the UN rating, moving from 68th to 78th place. At the same time, the provision of public online services and the digital literacy of the population are both at decent levels, with an index of 0.7471 and 0.7371, respectively. However, the telecommunications infrastructure index is low at 0.5832. The main reason for the slowed development is the insufficient coverage of the country's territory with fixed (wired) broadband lines, with only 1.92 per 100 people connected to the Internet.[35]

We should take note of the objective reasons impeding the development of ICT in South Africa. The main reason is the geographical remoteness of the African continent, which entails high costs for the construction and operation of the necessary digital infrastructure.

For this reason, the development of ICT in the RSA is centered in densely populated districts and metropolitan areas. The provided services are shaped according to the Western model and focused on the needs of the educated city dweller. A large-scale survey of government online services was conducted by research scholars, Shawren Singh and Bob Travica. They found that all government websites in South Africa, which is a country with eleven official languages, only provide information in English.[36]

The development level of e-government in the RSA can only increase if Western models are adapted to the peculiar features of the local population. Furthermore, the technological complexity and high cost of projects for the development of information and communication infrastructure in Africa predetermine the need to attract investments and specialists from more developed countries. This area holds a lot of potential for the development of cooperation among the BRICS countries.

1.5. E-Government in India

India is significantly behind other BRICS member countries in terms of its position in the UN rating, occupying the 100th place at present. However, a contradictory

---

[34] OECD, *Policies for Digital Transformation: Recommendations for a Whole-of-Government Approach*, OECD iLibrary, 11 March 2019 (Feb. 2, 2023), available at https://www.oecd-ilibrary.org/sites/95ac155a-en/index.html?itemId=/content/component/95ac155a-en.

[35] UN Study E-Government 2020 (Feb. 2, 2023), available at https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf.

[36] Tendani Mawela et al., *E-Government Implementation: A Reflection on South African Municipalities*, 29(1) South African Computer J. 147 (2017).

picture comes up when analyzing individual indicators. The level of providing online government service in India is 0.8529. According to this indicator, India is inferior only to China and Brazil among the BRICS member countries. The high quality of providing public services is ensured by the government's constant efforts to implement digital initiatives.[37]

The Digital India Program was launched in 2014 to ensure a high quality of public services. The goal of this program is to transform India into a digital society and a knowledge economy. The program is implemented in three main areas: the creation of a digital infrastructure useful for citizens, e-government and on-demand services and digital empowerment of citizens.[38]

However, the majority of citizens do not have access to the highly efficient government services available online. According to projections made by the UN for its 2020 rating, India's information and communication infrastructure development index was estimated to be 0.3515 and the level of the population's computer literacy was estimated at 0.5848. The 2017–2018 National Sample Survey showed that only 23.8% of Indian households had Internet access. In rural households (66% of the population), access to the Internet is at 14.9%, whereas in urban households access is at 42%[39] The measures taken by the Indian government to establish control over the Internet space also reduce the availability of e-government services. In this particular scenario, the issue that arises is not simply the restriction of the consumable content but rather the complete prohibition of access to the global network. In 2019, there were 121 Internet outages in India. For instance, in August 2019, the government in the states of Jammu and Kashmir completely blocked Internet access for 175 days to prevent riots,[40] and therefore it was impossible to receive e-government services, especially at a time of riots and other internal disturbances. India's multiculturalism is another problem. E-government websites mainly post information in English. Even though the majority of the population does speak English, in a country with twenty-two officially constitutionally recognized languages, finding content in the local language is a challenge.[41]

---

37 PIB Delhi, *High Performance Computing (HPC) and Information Communication Technologies (ICT) discussed at BRICS Working Group Meeting*, Ministry of Science and Technology, 30 May 2021 (Feb. 2, 2023), available at https://www.pib.gov.in/PressReleasePage.aspx?PRID=1722819.

38 Vision of Digital India, 18 November 2014 (Feb. 2, 2023), available at https://digitalindia.gov.in/content/vision-and-vision-areas.

39 Digital Daan, Digital Empowerment Foundation (Feb. 2, 2023), available at https://www.digitaldaan.in/.

40 Berhan Taye, *Internet Shutdowns in 2019: A Global Overview*, Access Now, 22 February 2019 (Feb. 2, 2023), available at https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

41 UN, *E-Government Development Index*, Digital Russia, 28 August 2018 (Feb. 2, 2023), available at https://d-russia.ru/wp-content/uploads/2018/08/E-Government-Survey-2018_FINAL-for-web.pdf.

Nevertheless, India is actively trying to eliminate the digital divide. The country has the largest national identification system, Aadhaar, with biometric and demographic data of over a billion users. The poorest segments of the population, who had never previously possessed an identity card, were digitally identified through this system. As a result of this system, they are able to gain access to social benefits and Internet banking. There are over 1 billion bank accounts and mobile telephones connected to Aadhaar, and the database has recorded over $12 billion in financial transactions.[42]

Government initiatives within the framework of the Digital India Program focus on connecting rural communities to the network; lowering prices of Internet-connected phones and data transfer calling plans; promoting e-wallets and creating free Wi-Fi hotspots among others endeavors.[43]

2. Strategic Cybersecurity Activities

The most authoritative measurement of a state's cybersecurity level is the Global Cybersecurity Index, which is calculated by the International Telecommunication Union (ITU). The study compares the achievements of the participating countries in these areas.

According to the Global Cybersecurity Index (2018), only Russia and China have a high level of cybersecurity among the BRICS member countries; the remaining three countries have an average level. The countries of the bloc have a significant spread in the ratings, occupying from 26th to 70th places out of 194 (Table 1).

Table 1: **The Global Cybersecurity Index 2018 of the BRICS member countries**

Country	Level	Rating
Russia	high	26
China	high	27
India	high	47
South Africa	medium	56
Brazil	medium	70

Source: Author based on ITU open data (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)

[42] Noor A. Samion & Azlinah Mohamed, *Innovation of National Digital Identity: A Review*, 9(1.2 Special Issue) Int'l J. Advanced Trends in Computer Sci. and Engineering 151 (2020).

[43] Sharada P. Mohanty et al., *On the Design of a Youth-Led, Issue-Based, Crowdsourced Global Monitoring Framework for the SDGs*, 11(23) Sustainability (Article 68399) (2019).

The foundation for ensuring cybersecurity at the national level is a program document determining the state's policy in this area. Currently, all BRICS member countries have adopted such a document. However, we can see significant differences in the terminology and main directions of implementation (Table 2).

Table 2: **Cybersecurity strategies of the BRICS member countries**

Country	Year	Document title
Russia	2010 (2016)	Information Security Doctrine of the Russian Federation
India	2013	National Cybersecurity Policy
South Africa	2015	The National Cybersecurity Policy Framework
China	2017	Cybersecurity Law of the People's Republic of China
Brazil	2020	Brazilian National Cybersecurity Strategy E-Cyber

Source: Author, based on open data

Let us compare the goals and objectives of the national strategies of the BRICS member countries, the response procedure to cyberattacks and measures to counter cybercrimes. Russia uses the term "information security" instead of the concept of cybersecurity. Information security involves protecting information networks and maintaining the sovereignty, territorial integrity, defense, and security of the state.

In terms of cybersecurity, Russia is significantly ahead of other EAEU member states. It ranks 26th in the rating and belongs to the group of countries with a high level of cybersecurity. Its readiness to repel cyberattacks is 86.3%.[44]

The Doctrine of Information Security of the Russian Federation was first adopted in 2000. The updated document has been in effect since 2016. The subject of regulation is not only the security of the hardware and software complex but also the content of information transmitted using the global network.

Criminal liability for computer information crimes has been stipulated in the Russian legislation since 1996. Law enforcement practices are constantly monitored and criminal justice standards governing liability for crimes involving information and communication technologies are being improved. In the first quarter of 2021, criminal liability for libelous actions committed using information and telecommunication networks was introduced, and criminal liability for incitement to narcotics committed through telecommunication networks was toughened.

[44] ITU, *Global Cybersecurity Index (GCI)*, ITU Publications (2018) (Feb. 2, 2023), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

International cooperation in the field of information security is determined by a separate regulatory instrument – the Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security until 2020.[45]

China is also committed to the decisive role of the state in ensuring cybersecurity. The main regulatory document is the Cybersecurity Law of the People's Republic of China, which entered into force on 1 June 2017. The law aims to ensure cybersecurity; protect the sovereignty and national security of cyberspace and social and public interests; protect the legal rights and interests of citizens, legal entities and other organizations; and contribute to the healthy development of informatization of the economy and society.[46]

According to the law, the state undertakes to contribute to widespread Internet access, increase the level of network services, and guarantee the legal, well-ordered and free distribution of network information.

Network users are responsible for upholding the Constitution and laws, keeping the peace and respecting public morality. A multi-layered cybersecurity protection system has been established according to this law:

1. Developed and implemented national standards for network products and services. These standards include the Basic Level of Information Security Technologies for Classified Cybersecurity Protection (GB/T 22239–2019), Guidelines for Classified Cybersecurity Protection (GB/T 25058–2019) and Guidelines for the Classification of Classified Cybersecurity Protection (GB/T 22240–2020).[47]

2. The Cybersecurity Verification Measures were adopted and are to be implemented by network operators. These measures should prevent unauthorized access to the Internet and ensure user identification and preliminary verification of posted content. If the information poses a threat to the national security of the state, the operator should block it and report it to the appropriate public authorities.[48] Additionally, the posted content is constantly monitored by network operators and authorized state bodies to exclude state security and public moral risks.[49]

3. Outlined requirements for the protection of the critical information infrastructure. The main ones include storage of information on the territory of mainland

---

[45] Information Security Doctrine of the Russian Federation, 29 December 2008 (Feb. 2, 2023), available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.

[46] Cybersecurity Law of the People's Republic of China, 29 June 2018 (Feb. 2, 2023), available at https://www.chinafile.com/ngo/laws-regulations/cybersecurity-law-of-peoples-republic-of-china.

[47] Susan Xuanfeng Ning & Han Wu, *China: Cybersecurity Laws and Regulations*, ICLG, 2 November 2020 (Feb. 2, 2023), available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china.

[48] NCES, Security Management, National Center for Education Statistics, 2 November 2020 (Feb. 2, 2023), available at https://nces.ed.gov/pubs98/safetech/chapter4.asp.

[49] Cybersecurity Verification Measures, 20 April 2020 (Feb. 2, 2023), available at http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.

China, annual inspections of the condition of networks by service providers and selective testing of networks by government agencies.

China also adopted the International Strategy of Cooperation on Cyberspace on 1 March 2017. It emphasizes the need for international cooperation to ensure cybersecurity. In addition to the development of a global Internet governance system, it proposes creating a system of international behavioral rules and norms for states regarding cyberspace. It takes note of China's aspiration to participate in bilateral and multilateral agreements in this field and promote practical cybersecurity cooperation among the BRICS members.[50]

India adopted their National Cyber Security Policy in 2013. The document is a framework and defines a development strategy in this area. The main goals are as follows:

1. To create a safe cyber ecosystem in the country, form adequate trust and confidence in IT systems and transactions in cyberspace, and thereby enable the wider implementation of IT in all sectors of the economy.

2. To develop effective partnership relations between the public and private sectors based on joint participation in cyberspace security assurance.

3. To create a cybersecurity and privacy culture that provides for the users' responsible behavior and actions through effective communication and promotion strategies.

The large number of cyberattacks coming from other states as well as the discovery of vulnerabilities in the existing system led to adjustments to the digital policy. The development of a new National Cybersecurity Strategy for 2020–2025 was announced at the end of 2019.[51] However, it has not been published yet. The steps that have already been taken show that there is an emphasis on ensuring digital sovereignty and strengthening state control over cyberspace. In accordance with the Law on Personal Data of 2019, their storage is localized on the territory of India. Furthermore, the Defense Cyber Agency of India's tripartite Armed Forces Command was formed, whose task is to counter cyberthreats.[52]

Nevertheless, public-private partnerships continue to play a significant role in cybersecurity. The Indian modern digital policy implements the principle of joint but differentiated responsibility with a gradual increase in the role of the state in cybersecurity assurance.[53]

---

50 Tian Shaohul, *International Strategy of Cooperation on Cyberspace*, News.cn, 1 March 2017 (Feb. 2, 2023), available at http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_3.htm.

51 David Chinn et al., *Perspectives on Transforming Cybersecurity*, McKinsey & Company (March 2019) (Feb. 2, 2023), available at https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx.

52 *India to Have Defence Cyber Agency in May; Rear Admiral Mohit to Be its First Chief*, India Today: News, 30 April 2019 (Feb. 2, 2023), available at https://www.indiatoday.in/india/story/india-defence-cyber-agency-may-rear-admiral-mohit-1513381-2019-04-30.

53 *India's Trillion-Dollar Digital Opportunity*, Ministry of Electronics and Information Technology, 28 April 2019 (Feb. 2, 2023), available at https://www.digitalindia.gov.in/ebook/MeitY_TrillionDollarDigitalEconomy.pdf.

The Republic of South Africa adopted the National Cybersecurity Policy Framework (NCPF) on 4 December 2015. The goals include:

1. To promote a cybersecurity culture and to require compliance with the minimum security standards.

2. To strengthen the acquisition of intelligence information as well as investigations, prosecutions and lawsuits related to the prevention and suppression of cybercrimes, cyberwars, cyberterrorism and other malicious cyber acts.

3. To establish partnerships between the state, private and public sectors for the purpose of implementation of national and international action plans.

4. To ensure the protection of the National Critical Information Infrastructure (NCII).

5. To improve the legal framework that regulates cyberspace.

6. To maximize human potential.

A peculiar feature of the NCPF is its emphasis on the participation of the private sector, government, academic world and the general public in ensuring cybersecurity.

The lack of legal regulation in the field of cybersecurity in South Africa is a serious issue. However, since the adoption of the NCPF, significant progress has been made: the Critical Infrastructure Protection Act was passed and a draft Law on Cybercrimes and Cybersecurity was elaborated. The latter defines the concept of cybercrimes and introduces criminal liability for Internet crimes.[54]

Another problem is the lack of cybersecurity skills. To solve this problem, the Department of Communications and Postal Services established a Cybersecurity Center, which organizes civic education in this field with the participation of the public and private sectors.[55]

South Africa considers national cybersecurity a multifaceted concept implemented with the participation of many interested parties. The main efforts are focused on training and generating human potential, civic education and awareness, research and development of systems and cybercrime control.[56]

Brazil began shaping its legal cybersecurity framework in 2018 with the adoption of the National Information Security Policy.[57] The National Cybersecurity Strategy (E-Cyber) was adopted on 5 February 2020. It became the first module in the legal support of information security and defines the following strategic goals:

---

54 Cybersecurity Bill, 12 July 2017 (Feb. 2, 2023), available at https://pmg.org.za/bill/684/.

55 *Deputy Minister Pinky Kekana: CEO Forum for Cybersecurity*, South African Government, 26 March 2019 (Feb. 2, 2023), available at https://www.gov.za/speeches/deputy-minister-pinky-kekana-ceo-forum-cybersecurity-26-mar-2019-0000.

56 Noluxolo Kortjan, *A Cyber Security Awareness and Education Framework for South Africa* (November 2013) (Feb. 2, 2023), available at https://core.ac.uk/download/pdf/145053774.pdf.

57 Decree of the President of the Republic of Brazil, 28 December 2018 (Feb. 2, 2023), available at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm.

- to make Brazil more prosperous and secure in the digital environment;
- to increase Brazil's resilience to cyberthreats;
- to increase the cybersecurity effectiveness of Brazil in the international arena.

The Strategy was based on the principle of organizing joint activities of the public sector, the private sector, the academic world and society. There are eight types of Computer System Information Response Teams (CSIRTs) outlined to counter cyberattacks:

- National Responsibility Center;
- International Coordination Centers;
- CSIRT for critical infrastructures (energy, finance, telecom);
- CSIRT of providers;
- Corporate CSIRT;
- Academic CSIRT;
- CSIRT of the state authority;
- Military CSIRT.

The main responsibility to protect the critical infrastructure is assigned to companies operating in this area. They should create cybersecurity management structures that include the establishment of guidelines, manuals, classifications and procedures for handling incidents, as well as security rules applicable to all employees, contractors and suppliers.[58]

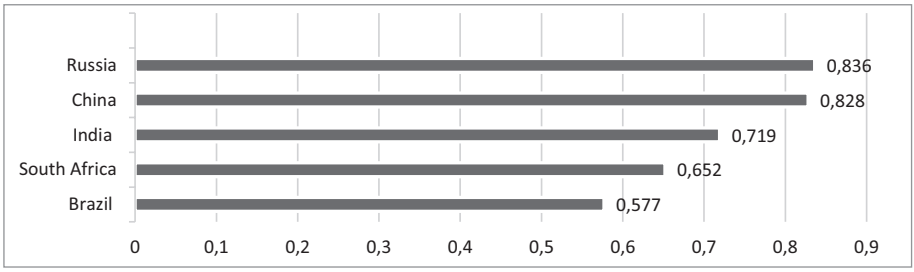
In general, E-Cyber is rather declarative; it defines the main lines of cybersecurity assurance but does not provide for specific measures for their implementation.

All of the BRICS member countries make targeted efforts to implement the key lines of cybersecurity. However, their national strategies set different priorities. Russia and China consider cybersecurity to be one of the components of state sovereignty, imposing strict state control over its provision. India, Brazil and South Africa, on the contrary, are making efforts to increase global information exchange and organize public-private partnerships in cybersecurity.

This difference in the approaches hinders closer interaction. However, an analysis of the results of the Global Cybersecurity Index (2018) shows that the countries with state control governing cyberspace have a higher cyber protection level. While Russia is ready to repel cyberattacks and counter cybercrimes by 83.8%, this indicator in Brazil is only 57.7% (Fig. 3).

[58] Decree of the President of the Republic of Brazil No. 10.222 'On Approval of the National Cybersecurity Strategy,' 5 February 2020 (Feb. 2, 2023), available at https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

Figure 3: **The level of cybersecurity of the BRICS member countries**



Source: Author, based on ITU open data (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)

We believe that the digitalization of the economy and public administration, which has grown significantly during the pandemic, has increased the dependence of the states on the condition of cybersecurity. Repeated cyberattacks have the potential to seriously damage national economies. The existence of different cyberattack regulatory models in the private sector complicates the formulation and implementation of universally acceptable rules and standards necessary to ensure cyber defense. This predetermines the need for a state-oriented approach to effective containment in cyberspace and provides grounds for a further rapprochement of the BRICS member countries.

3. Cybersecurity Cooperation of the BRICS Member Countries

The joint strategic goal of the BRICS member countries to strengthen cybersecurity cooperation was officially formulated in 2013. The eThekwini Declaration which was signed in Durban, South Africa on 27 March 2013 states:

> We believe it's important to contribute to and participate in a peaceful, secure, and open cyberspace and we emphasize that security in the use of information and communication technologies through universally accepted norms, standards and practices is of paramount importance.[59]

The areas of cooperation were specified at a meeting of the National Security Advisors held at the same summit: first, preventing cyberspace from turning

[59] *eThekwini Declaration v. BRICS Summit*, Durban, South Africa, 27 March 2013 (Feb. 2, 2023), available at http://www.nkibrics.ru/system/asset_docs/data/53da/485c/676c/761f/8d73/0000/original/V_BRICS_SUMMIT_-_ETHEKWINI_DECLARATON_MARCH_27__2013_DURBAN__SOUTH_AFRICA.docx?1406814300.

into a platform for recruiting terrorists and spreading radical ideologies; second, punishing not just the attackers, but also the organizers of cyber terrorism and cybercrimes and third, developing international cooperation through multilateral mechanisms within the UN framework. The joint strategic goal of reforming global cyberspace governance laid a solid strategic foundation for BRICS cybersecurity cooperation. The major challenges these countries face require further development of their agenda in order to help developing countries gain greater authority in the governance system.[60]

However, cooperation has been limited to the coordination of special positions. The 2020 Summit did not result in the adoption of a program document on the cybersecurity interaction of the BRICS member countries. The member countries proposed that they continue working on concluding an appropriate five-way agreement.[61] This is because the differences in the types of regimes lead to the appearance of mistrust between the countries and the imbalance of power inside the bloc raises concerns in the form of potential unequal agreements.[62]

During the period of cooperation within the BRICS framework, Russia entered into bilateral agreements on information security with all of the member countries.

The Agreement between the Government of the Russian Federation and the Government of the Federal Republic of Brazil on cooperation in the field of international information and communication security, signed on 14 May 2010 in Moscow, was the first document of its kind.

The main areas of cooperation enshrined in this document do not contain specific bilateral measures but serve as frameworks and declarations. They contain the following items:

1. Determination, approval and implementation of the necessary joint measures required to ensure international information and communication security.

2. Creation of a joint structure for the prevention, detection, elimination and response to information security threats.

3. Examination, research and assessments in the field of information and communication security, including cooperation between the parties in the areas of technology and science.

4. Development of interaction within the framework of Internet governance forums on information and communication security issues.

---

60 Gao Wanglai, *BRICS Cybersecurity Cooperation: Achievements and Deepening Paths China International Studies*, PressReader.com, 20 January 2018 (Feb. 2, 2023), available at https://www.pressreader.com/china/china-international-studies-english/20180120/281513636564569.

61 *BRICS National Security Advisors discuss topical issues of security cooperation*, Official website of the Russian BRICS Chairmanship in 2020, 18 September 2020 (Feb. 2, 2023), available at https://eng.brics-russia2020.ru/news/20200918/582132/BRICS-National-Security-Advisors-discuss-topical-issues-of-security-cooperation.html.

62 Moraes, *supra* note 12.

5. Ensuring the information and communication security of national critically important infrastructures.

6. Development and implementation of an approved policy for the use of electronic digital signatures and information protection during international information exchange.

7. Exchange of information on legislation pertaining to information and communication security issues in the Russian Federation and the legislation of the Federal Republic of Brazil.

8. Development and improvement of the international legal framework as well as the practical mechanisms of cooperation between the parties in strengthening international information and communication security.

9. Cooperation on the international information and communication security problems within the framework of existing international organizations and forums.

10. Knowledge exchange, specialist education and organization of task meetings, conferences, seminars and other forums of the authorized representatives and experts in information and communication security of the parties involved in the agreement.[63]

The agreement notes that the essential principle of cooperation is non-interference in the internal affairs of another state. The agreement is, thus far, only declarative. Bilateral events are not held, but the countries continue to cooperate in this area within BRICS.

On 8 May 2015, the Government of the Russian Federation and the Government of the People's Republic of China signed an agreement on international information security cooperation.[64] Over the five years since the conclusion of the previous bilateral agreement, the digitalization of economic and social life has reached a new level. This led to the globalization of cyberspace and the appearance of new types of information threats.

Between 27 November 2013 to 15 December 2014, hackers stole personal information (phone numbers, email and postal addresses, credit and debit card numbers and PINs) from 110 million customers of Target Corporation, the third largest retail chain in the United States. As a result, American financial institutions suffered losses of over $200 million. In its 2015 Cyber Security Intelligence Index, IBM reported that nearly two-thirds of cyberattacks focused on three industries: finance and insurance, information and communications, and production.[65]

---

63 Agreement between the Government of the Russian Federation and the Government of the Federative Republic of Brazil on International Information and Communication Security, 14 May 2010 (Feb. 2, 2023), available at http://docs.cntd.ru/document/902366519.

64 Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on international information security cooperation, 8 May 2015 (Feb. 2, 2023), available at http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1.

65 *42 Cyber Attack Statistics by Year: A Look at the Last Decade*, Sectigo Store, 8 December 2016 (Feb. 2, 2023), available at https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/.

During this period, the actions of cybercriminals moved from the national to the international level and affected the activities of not only economic organizations but also state institutions. On 3 June 2013, hackers from the group Anonymous disrupted the websites of the Turkish President, the Prime Minister and several government agencies. Thus, criminals supported anti-government demonstrations in the country.[66]

In response to the new challenges, the agreement formulates relevant types of cyberthreats, such as the use of ICT to interfere in the internal affairs of states; disrupt public order; incite interethnic, interracial and interfaith hostility; promote racist and xenophobic ideas and theories that generate hatred and discrimination; incite violence and instability and destabilize the internal political and socio-economic situation; violate state governance; and cause economic and other damage.[67] The general provisions of this agreement include such terms as computer attack, unlawful use of information resources, and unauthorized interference with information resources.[68]

The main areas of cooperation in this agreement are more clearly elaborated. The number of areas of cooperation has grown from ten to sixteen. The content has become more specific. The agreements reached are implemented with a high degree of precision.

The establishment of cooperation in the scientific and research areas was a promising area of development. The agreement formulates specific measures: promotion of scientific research in international information security; joint research projects; joint training of specialists; and student, graduate student and lecturer exchange programs between specialized higher educational institutions.

By September 2013, thirteen Russian-Chinese educational associations and 124 general educational programs were established.[69] Moreover, the implementation of a joint project of Moscow State University and the Beijing Polytechnic Institute to found the Russian-Chinese University in Shenzhen was a significant achievement. Students at this university are given lectures in three languages, and graduates of the Russian-Chinese University will be able to receive diplomas from both the

---

66 Major Hacker Attacks in 2001–2016: Timeline, TASS, 18 December 2016 (Feb. 2, 2023), available at https://tass.ru/info/1408961.

67 ITU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, International Telecommunication Union, 23 September 2012 (Feb. 2, 2023), available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

68 UN, *Information and Communication Technology Policy and Legal Issues for Central Asia*, United Nations Economic Commission for Europe, 18 December 2020 (Feb. 2, 2023), available at https://unece.org/DAM/ceci/publications/ict.pdf.

69 European Commission, *Education and Training Monitor*, European Commission, 14 March 2019 (Feb. 2, 2023), available at https://ec.europa.eu/education/sites/default/files/document-library-docs/volume-1-2019-education-and-training-monitor.pdf.

Russian and the Chinese universities. The number of students that participated in the exchange program exceeded 90 thousand students.[70]

In June 2019, Russian President Vladimir Putin and Chinese President Xi Jinping signed the Joint Statement between the People's Republic of China and the Russian Federation on the Development of the Comprehensive Partnership and Strategic Cooperative Relations Entering a New Era in Moscow. This statement declared 2020–2021 as the Year of Russian-Chinese Scientific, Technical and Innovative Cooperation. The parties reached an agreement on a plan of action to expand the mutually beneficial cooperation between research centers, educational organizations and innovation clusters of the partnering states and to promote the growing effectiveness of joint scientific, technical and research projects. They signed a Road Map of the Russian-Chinese cooperation in the fields of science, technology and innovation for the period 2020–2025, which provides for the realization of over 1,000 joint activities.[71]

Another promising area of development was the deepening of cooperation and coordination of the activities between Russia and China on ensuring international information security within the framework of international organizations and forums. The need to deepen cooperation within the BRICS was noted separately.[72] At the 2015 Ufa Summit, the BRICS leaders decided to create a task force on cooperation in the ICT sphere. In November 2016, the Communications Ministers of the BRICS member countries agreed on a common goal of creating a digital partnership. In January 2017, the China Council for the BRICS Think Tank Cooperation (CCBTC) was established. In May, the CCBTC convened a Cyber Economy and Cybersecurity Symposium attended by relevant experts from the BRICS member countries and presented written proposals for the BRICS Summit in Xiamen to be held in September of that same year.[73]

Also of note, the bloc outlined cooperation between the competent law enforcement authorities of Russia and China to investigate cases related to the use of ICT for terrorist and criminal purposes as well as in the field of computer incident response.[74]

Following the signing of the agreement, both sides acknowledged the need to develop cooperation in this area. However, they did not agree on specific measures,

---

[70] *The student exchange volume between Russia and China has exceeded 90 thousand people*, RIA Novosti, 16 September 2019 (Feb. 2, 2023), available at https://ria.ru/20190916/1558731168.html.

[71] *Russia and China opened the Years of Scientific, Technical and Innovative Cooperation*, Russian Government, 12 September 2021 (Feb. 2, 2023), available at http://government.ru/news/40273/.

[72] VII BRICS Summit: 2015 Ufa Declaration, 7 September 2015 (Feb. 2, 2023), available at http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html.

[73] Wanglai, *supra* note 60.

[74] UNODC, *The Use of Internet for Terrorist Purposes* (2012) (Feb. 2, 2023), available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

likely due to the close relationship between the activities of the competent authorities and the security of the state. The joint use of information on the existing and potential risks and information security threats can lead to the vulnerability of the state's critical infrastructure and damage national cybersecurity.

Notably, the text of the agreement contains provisions designed to minimize the risks of cooperation. The agreement provides that each party has an equal right to protect the information resources of its state from unlawful use and unauthorized interference, including from computer attacks on them, and shall not take similar actions in relation to the other Party.

On 15 October 2016, the Government of the Russian Federation and the Government of the Republic of India signed a cooperation agreement on the use of ICT.[75] The following threats were highlighted for the first time in this agreement:

• The harmful use of ICTs aimed at undermining the sovereignty, violating territorial integrity and threatening international peace, human rights, freedom of expression, security and strategic stability.

• Malicious attacks on the critical information infrastructure, which can undermine the safe and stable functioning of global and national information and communication networks, including actions capable of causing economic damage.

• Dissemination of information through the use of ICTs with the intent to disrupt public order, community and social harmony as well as to undermine government control.

Human rights, community and social harmony are protected priorities. This is consistent with the main directions of the Cybersecurity Strategy of India, which considers enterprises and organizations of the private sector and civil society institutions to be the main subject of security regulations in this area. The Indian Information Technology Act aims to prevent all forms of hacking, hijacking and hacktivism.

As a result, one of the highlighted areas of cooperation is an increase in transparency, accountability and inclusiveness in the management of the global Internet network and maintaining its security and stable operation.

On 15–16 February 2018, security advisers held bilateral consultations to realize the agreement. The parties emphasized the need to prevent the use of cyber technologies for criminal and terrorist purposes, also pointing out the need to develop rules for the behavior of the states in this area with the UN in a coordinating role. The parties confirmed their intention to expand practical cooperation on security issues in the use of ICTs, including exchanging data on new challenges in this area and information containing technical and confidential data and capacity building, including through the exchange of ICTs to counter their use for criminal

[75] 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, 15 October 2016 (Feb. 2, 2023), available at http://docs.cntd.ru/document/420384231.

and terrorist purposes.[76] However, the insufficient consistency of the positions led to a lack of specific results. Despite this, the countries continue to hold political dialogues on cybersecurity to further expand cooperation.

On 4 September 2017, the Government of the Russian Federation and the Government of the Republic of South Africa signed an agreement on international information security cooperation.[77] The language used to describe cyber threats and areas of cooperation is similar to the agreements with other BRICS member countries. The insufficient level of infrastructure development and provision of access to ICT in South Africa made cooperation in cybersecurity research and joint research projects a top priority. Cooperation in this area is realized in a public-private partnership.

In January 2018, representatives of the business community of South Africa visited RTI JSC to implement the Safe City project. The project involves the establishment of municipal centers for monitoring and managing the urban environment as well as upgrading the relevant infrastructure in South Africa. System integration solutions and technologies developed by a Russian company will serve as the project's software foundation.

In October 2020, the largest research project on the development of digital infrastructure in South Africa was launched. Researchers from the BRICS member countries will carry out joint research to develop an intercontinental quantum communication channel. The channel will be 10,000 kilometres long and will connect the universities participating in the project in South Africa and China. Russian specialists are developing new optical fiber technologies; China will provide quantum satellite communications; India will model fiber-optic communications and South Africa will be the lead executor of the project.[78]

This study will lay the foundation for the development of IT communications in all member countries since quantum communications provide an unprecedented level of information security. We firmly believe that the fact that Russia has bilateral cybersecurity agreements with all of the BRICS member countries is an essential achievement that can serve as a launching pad for entering into multilateral agreements.

---

[76] *Russia and India agreed to expand cybersecurity cooperation*, RIA Novosti, 16 February 2018 (Feb. 2, 2023), available at https://ria.ru/20180216/1514801963.html.

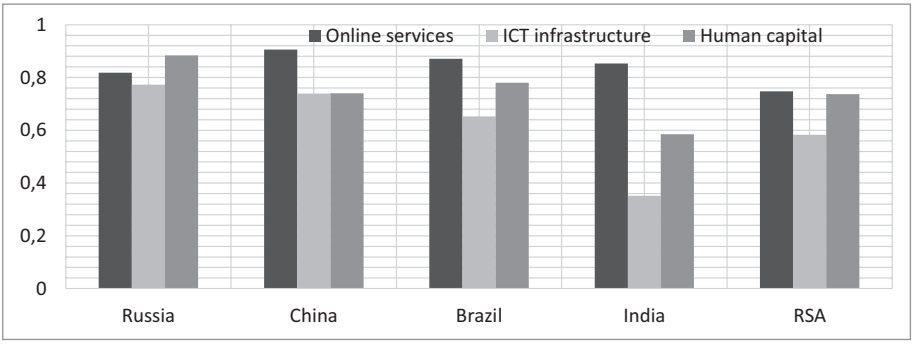
[77] Agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on international information security cooperation, Garant, 4 September 2017 (Feb. 2, 2023), available at https://base.garant.ru/71764786/.

[78] STI overview: Five-Year Anniversary of Cooperation in Science, Technology and Innovation under the Memorandum of Understanding, BRICS, 14 March 2020 (Feb. 2, 2023), available at https://brics-russia2020.ru/images/113/91/1139196.pdf.

Conclusion

Thus, despite significant differences in the development of e-government, each of the BRICS member countries has high achievements in one or several indicators (Fig. 2).

Figure 2: **The standing of the BRICS member countries as measured by the main indicators of the E-Government Index**



Source: UN Study E-Government 2020

The most significant progress has been made in the provision of digital public services, ranked at 0.74–0.90. All countries have common platforms and cloud information storage, leading to the need to protect the data contained in them, and therefore, to have a formal national cybersecurity strategy.

Brazil, India and South Africa are experiencing difficulties in the development of the information and communication infrastructure, which is currently rated at 0.35–0.65. The construction of fiber-optic networks could become a promising area of economic cooperation within the BRICS.[79]

The Russian Federation is the leader in terms of the level of human capital development, with a rating of 0.88. The remaining member countries need to make efforts to eliminate the digital divide between certain territories and segments of the population. International educational and research programs, which are an integral part of cybersecurity cooperation, can be helpful in this regard.

A detailed study of the e-governments of these countries leads us to the conclusion that all of the countries have made significant achievements in the provision of online public services (from 0.9 to 0.74). According to this indicator, the BRICS member

[79] Stacia Lee, *International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable*, University of Washington (January 2016) (Feb. 2, 2023), available at https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/.

countries are in the top twenty nations worldwide. The government systems of the countries studied are highly integrated with digital platforms and cloud storage systems, which makes them vulnerable to cyberthreats. These observations allow us to conclude that all of the BRICS member countries are highly interested in the formation of a common, well-regulated state cybersecurity system.

However, after a thorough study of the Global Cybersecurity Index (2018), we found that countries with government regulation have a higher cybersecurity level (Russia, China). This level directly depends on the degree of responsibility assumed by the state. Countries with insufficiently centralized cyber defense systems are lower in the rating (Brazil, South Africa, India) and are often affected by cyberattacks. As a result, India was forced to apply government regulation of cyberspace, which increased its effectiveness. We therefore come to this conclusion that there are objective grounds for strengthening state control over cybersecurity and hope that the positions of the BRICS member countries can be brought closer together.

According to our study of the bilateral agreements on cybersecurity cooperation of the BRICS member countries, we concluded that there are common areas for cooperation. These areas include:

• Educational projects that enhance human potential.

• Joint applied research.

• Joint actions to close the digital divide and develop broadband access networks in all countries of the bloc.

• Unification of legislation of the member countries on the criminalization of unlawful acts in cyberspace.

We believe that in order to move to a strategic level of interaction and coordinate the actions of the BRICS member countries in the international arena, a mixed intergovernmental committee for cybersecurity cooperation should be created. This committee will serve as an executive body for the preparation and execution of the following events,

• Exchange of information and best practices in combating cybercrime.

• Development of an integrated digital platform of the BRICS member countries to exchange data on cyber incidents in the financial sector, best practices and regulatory experience in information security.

• Regular publication of the Compendium of Best Practices on the Supervision and Control of Information Security Risks as well as its publication on a digital platform.

• Implementation of bachelor's and master's cybersecurity programmes within the BRICS Institute.

In addition, the current state of world affairs requires that the BRICS countries consolidate their position in the field of cybersecurity. The first step could be to hold a video meeting among representatives of the Group of Five Countries in charge of security issues to adopt a joint memorandum.

References

Bruijn H. & Janssen M. *Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies*, 34(1) Government Information Quarterly 1 (2017). https://doi.org/10.1016/j.giq.2017.02.007

Burak A. & Barış D. *Analysis of the Cyber Security Strategies of People's Republic of China*, 14(28) Güvenlik Stratejileri Dergisi (Journal of Security Strategies) 1 (2018). https://doi.org/10.17752/guvenlikstrtj.495748

Chandel S. et al. *The Golden Shield Project of China*: *A Decade Later an In-depth Study of the Great Firewall*, in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 111 (2019). https://doi.org/10.1109/CyberC.2019.00027

Khanna P. *State Sovereignty and Self-Defence in Cyberspace*, 5(4) BRICS Law Journal 139 (2018). https://doi.org/10.21684/2412-2343-2018-5-4-139-154

Kortjan N. *A Conceptual Framework for Cyber Security Awareness and Education in South Africa*, 52(1) South African Computer Journal 29 (2014). https://doi.org/10.18489/sacj.v52i0.201

Markopoulou D. et al. *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, 35(6) Computer Law and Security Review 1 (2019). https://doi.org/10.1016/j.clsr.2019.06.007

Mawela T. et al. *E-Government Implementation: A Reflection on South African Municipalities*, 29(1) South African Computer Journal 147 (2017). https://dx.doi.org/10.18489/sacj.v29i1.444

Mohanty S.P. et al. *On the Design of a Youth-Led, Issue-Based*, *Crowdsourced Global Monitoring Framework for the SDGs*, 11(23) Sustainability (Article 68399) (2019). https://doi.org/10.3390/su11236839

Niekerk B.V. *South Africa and the Cyber Security Dilemma*, 18(2) Journal of Information Warfare 96 (2019). https://doi.org/ 10.23962/10539/23573

Nikitin E. & Marius M. *Unified Digital Law Enforcement Environment – Necessity and Prospects for Creation in the "BRICS Countries"*, 7(2) BRICS Law Journal 66 (2020). https://doi.org/10.21684/2412-2343-2020-7-2-66-93

Samion N.A. & Mohamed A. *Innovation of National Digital Identity: A Review*, 9(1.2 Special Issue) International Journal of Advanced Trends in Computer Science and Engineering 151 (2020). https://doi.org/10.30534/IJATCSE/2020/2391.22020

Song Z. et al. *China's Prefectural Digital Divide: Spatial Analysis and Multivariate Determinants of ICT Diffusion*, 52 International Journal of Information Management (Article 102072) (2020). https://doi.org/10.1016/j.ijinfomgt.2020.102072

Stevens T. *Global Cybersecurity: New Directions in Theory and Methods*, 6(2) Politics and Governance 1 (2018). https://doi.org/10.17645/pag.v6i2.1569

Vakulyk O. et al. *Cybersecurity as a Component of the National Security of the State*, 9(3) Journal of Security and Sustainability Issues 775 (2020). https://doi.org/10.9770/JSSI.2020.9.3(4)

Yuan L. et al. *Evaluating the Readiness of Government Portal Websites in China to Adopt Contemporary Public Administration Principles*, 29(3) Government Information Quarterly 403 (2012). https://doi.org/10.1016/j.giq.2011.12.009

Information about the authors

Oksana Ovchinnikova (Chelyabinsk, Russia) – Associate Professor, Department of Judicial and Law Enforcement Activities, Institute of Law, South Ural State University (National Research University) (47a Elektrostalskaya St., Chelyabinsk, 454038, Russia; e-mail: ovchinnikova-ov@yandex.ru).

Niteesh Kumar Upadhyay (Nodia, India) – Associate Professor, Symbiosis Law School, Noida Campus, Symbiosis International (Deemed University) Pune (Block A, 47/48, Sector-62, Noida, 201301, India; e-mail: niteesh_marshal@yahoo.co.in).

FEATURES OF THE APPLICATION OF DIGITAL TECHNOLOGY IN CRIMINAL PROCEEDINGS OF THE BRICS COUNTRIES

GALINA RUSMAN,

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

EUGENIO D'ORIO,

Bio Forensics Research Center (Ischia, Italy)

ELIZAVETA POPOVA,

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

PAVLOS KIPOURAS,

School of Forensic Graphology (Naples, Italy)

https://doi.org/10.21684/2412-2343-2023-10-1-35-58

The current pace of technological development creates new opportunities for improvements in various spheres of human activity, including the sphere of criminal proceedings. In the BRICS countries, the achievements of modern technological developments, in particular the use of digital technology in criminal proceedings, have their own unique characteristics. This article describes the current state of criminal proceedings in the BRICS member countries. The authors analyze practices in criminal proceedings with the aim of identifying best practices, advantages and disadvantages of using digital technology in the criminal justice sector, as well as outlining prospects for the development of this technology in the BRICS countries. The authors come to the conclusion that the use of digital technology in criminal proceedings should contribute to increased access to justice, procedural economy and effective investigation, and as a result, a fair verdict in criminal cases in all of the BRICS member states.

Keywords: criminal proceedings; digital technologies; BRICS countries; artificial intelligence; electronic evidence; 3D technologies.

Recommended citation: Galina Rusman et al., *Features of the Application of Digital Technology in Criminal Proceedings of the BRICS Countries*, 10(1) BRICS Law Journal 35–58 (2023).

Table of Contents

Introduction

In the modern world, one of the key roles is played by advanced technologies that are able to adapt to the realities of the world and respond to the challenges they present. The current state of development in digital technology creates new opportunities for improvements in various spheres of human activity. This is also confirmed by the fact that the use of technical means and scientific achievements in criminal proceedings is becoming more widespread every year.

The COVID-19 pandemic contributed to the accelerated introduction of new technologies into the judicial system, including within the sphere of criminal procedure. The urgent need for digital technologies was manifested in the decision to ensure the right of citizens to personal participation and respect for their procedural rights as participants in the court session. Digital technologies such as artificial intelligence, videoconferencing, electronic courts and 3D technologies are particularly important in this context.

In order to fully realize the right of citizens to access justice, criminal proceedings must respond in a timely manner to changes taking place in the modern world's political, economic and legal environments, including taking into account such processes as epidemics. In this regard, legal scientists are increasingly turning to the use of digital technologies in their research in criminal proceedings. Moreover, particular attention is paid to the prospects of their application in the BRICS countries.

The use of digital technical means, in particular videoconferencing, artificial intelligence and 3D technologies, opens up new prospects for the further improvement of criminal procedural activities, significantly increasing the chances of an effective investigation of crimes and, as a result, the imposition of a fair sentence.

At the same time, the need to optimize criminal proceedings through the use of such technologies, while ensuring the constitutional right of citizens to access to justice and the integrity of criminal procedural evidence, requires the adoption

of appropriate legal regulation. Paramount importance is given to the features of the admissibility of evidence obtained as a result of the use of such digital technical means. This is especially important since the main trend in the use of digital technology in the criminal proceedings of the BRICS countries is the introduction of electronic evidence; however, the regulatory framework for these types of evidence has not yet been fully formed.

Digital technologies are characterized by a high degree of novelty, due to which they are becoming increasingly important in the development of criminal proceedings and having a significant impact on the resolution of criminal procedural tasks. It should be noted that modern technologies play a significant role in the digitalization of criminal proceedings. Therefore, the use of these technologies during the preliminary investigation of a crime or a court hearing should contribute to improving the efficiency of the justice system, as well as the quality of the evidence base and the level of access that citizens have to justice.

1. Electronic Justice and Features of the Use of Electronic Evidence

Due to the widespread use of digital technologies in criminal proceedings, the possibility of performing procedural actions in digital form, also known as electronic justice, is becoming increasingly in demand. In response to the challenges of the modern world, a growing number of countries, including Brazil, Russia, India, China and South Africa, are adopting laws aimed at combating the rise in cybercrime and working with evidence in electronic form.

To date, the main forms of electronic justice currently in use, including in the BRICS countries, include remote judicial proceedings using real-time video and audio transmission technology (videoconferencing), electronic evidence and electronic services, such as informing the parties or exchanging relevant court materials with the parties, as well as information databases of national judicial systems.[1]

In Russia, in order to implement the strategy of electronic justice, the state automated system "Justice" and the "My Arbitrator" systems are in operation.

In India, a deep learning chatbot is being developed that could have the capability to engage in interactive dialogue and also offer suggestions on future courses of action. In addition, such a development would aid in the analysis of various laws, including the criminal procedure legislation of India in its different states.[2]

---

[1] *Luo Y.* Practice of E-Justice in China // Государство и право во времени и пространстве: сборник тезисов докладов Республиканской научно-практической конференции с международным участием студентов, магистрантов, аспирантов, 3 декабря 2021 г. / под ред. Д.В. Петроченкова [Ye Luo, *Practice of E-Justice in China*, in Dmitry V. Petrochenkov (ed.), The State and Law in Time and Space: A Collection of Abstracts of Reports of the Republican Scientific and Practical Conference with International Participation of Students, Undergraduates, Postgraduates, 3 December 2021] 350–51 (2022).

[2] Adv. V.K. Singhal, *An Advanced Deep Learning Based Approach for Judicial Decision Support Process*, 13(2) Int'l J. Electronics Engineering 18 (2021).

In China, the active process of digitalization in the courts began in 2016. Thus, the Shanghai Court initiated the development of an intelligent criminal case processing system in order to clarify the guidelines on the basic standards of evidence at different stages of the trial and to assist court personnel in collecting and reviewing evidence in accordance with the law in a comprehensive and standardized manner.[3] As a direct consequence of the implementation of the "smart courts" system, it is now possible to submit documents, present evidence, hold court sessions, make decisions, as well as conduct proceedings under review of a court decision online.

By 2019, China had developed a court system that offered its citizens access to online services for the entire judicial process. The advantages of such systems of electronic justice, carried out with the help of "smart courts," have emerged as a timely and effective solution to the problems that have arisen due to the COVID-19 pandemic. As a result, "smart courts" are aimed at solving one of the tasks of the Criminal Procedure Law of the People's Republic of China, namely, to "accurately" and "timely" establish the facts.[4]

Furthermore, "smart courts" in China should make full use of information and communication technologies, including the Internet, cloud computing, big data and artificial intelligence, in order to modernize the judicial system and judicial capacity.[5]

The widespread development of digital technologies has led to the fact that there is a pressing need to improve criminal justice and criminology, which has forced legislators and scientists to immediately begin working to address this urgent need.

Indian researchers B. Mishra, S. Chatterjee and S. Mishra believe that

> in general the Indian government is trying to adhere with the fast paced technological developments by following the process of adjusting with the current scenario by following three major steps of making adjustment with the already prevalent National Laws, identification of gaps in the existing legislations and drafting of new legislation to comply with the existing legal loopholes.[6]

In order to implement the planned goals, India has implemented legislative, institutional and procedural changes to effectively respond to cybercrime. Thus, in

---

[3] Jia Yu & Jun Xia, *E-Justice Evaluation Factors: The Case of Smart Court of China*, 37(4) Info. Dev. 658 (2021).

[4] Changqing Shi et al., *The Smart Court – A New Pathway to Justice in China?*, 12(1) Int'l J. for Ct. Admin. 3 (2021).

[5] Mimi Zou, *'Smart Courts' in China and the Future of Personal Injury Litigation*, J. Personal Injury L. (June 2020) (Jan. 3, 2023), available at https://ssrn.com/abstract=3552895.

[6] Banipriya Mishra et al., *Traditional Judicial Systems Need Ammunition for Future*, 24(2) J. Legal, Ethical & Reg. Issues 1, 3 (2021).

order to respond to cybercrime, amendments were adopted to the Indian Penal Code of 1860 as well as the Information Technology Act of 2000, which form the basis of legislation relating to cybercrime. In addition, the Evidence Act of 1872 has been amended to make electronic evidence relevant and acceptable in Indian courts.[7]

South African companies are also actively exposed to cyberattacks. However, despite this, South African legislation currently does not regulate in detail the general standards of information security in companies. If the organizations responsible for the processing of information, as well as the security and confidentiality of the personal information processed by them, do not take these measures, then they are in violation of the Cybercrime Act of 2020.[8]

With the improvement of modern information technologies in the criminal process, the need for the regulation of their application is also increasing. In today's world, it is extremely difficult to avoid leaving a digital fingerprint.

It is impossible to ignore the fact that, as a result of the inherent nature of digital criminology, which provides means for collecting, examining, analyzing and presenting evidence as well as using it in trial, it is becoming one of the most developed areas in the field of criminal procedure. Digital forensics has developed so rapidly over the past decades thanks to the outstanding progress of information technology. These advancements have made it possible to find non-standard solutions to the challenges of cloud forensics, network forensics and mobile device expertise.

Additionally, with the global digitalization of society, information about people, information processes and events is frequently contained in discrete form on electronic media. As a result, there is an urgent need to optimize the collection of evidence in electronic form by converting it into an analog, readable form.

Brazilian researchers E. Oliveira, Jr., T.J. Silva, A.F. Zorzo and C.V. Neu are of the opinion that the process of experimentation in the field of digital forensics should be improved. It is proposed that special attention be paid to its procedural fixation and the ability to exchange data in order to ensure their repeatability. The issue of conducting an experiment in the field of digital forensics is especially important, since its absence puts the reliability and potential of the evolution of science at risk, and consequently, the level of reliability and evidentiary value of electronic evidence in court.[9]

N.P. Mailis notes that the study of digital footprints in Russia receives considerable attention. Different approaches have been developed not only for terminology but

---

[7] Urvashi S. Mishra, *Application of Cyber Forensics in Crime Investigation*, Research Paper (2018) (Jan. 3, 2023), available at http://ijrar.com/upload_issue/ijrar_issue_1227.pdf.

[8] Nathan-Ross Adams, *South African Company Law in the Fourth Industrial Revolution: Does Artificial Intelligence Create a Need for Legal Reform?*, LLM dissertation, University of the Western Cape (2021) (Jan. 3, 2023), available at http://dx.doi.org/10.2139/ssrn.4052285.

[9] Ednei Oliveira, Jr. et al., *Digital Forensics Experimentation: Analysis and Recommendations*, 34(1) Forensic Sc. Rev. 21, 40 (2022).

also for the processes of detecting and removing such traces, understanding their nature and determining which category of traces they should be assigned to.[10]

In the Russian scientific literature, it is customary to understand a digital footprint as:

> criminalistically significant computer information about events or actions, reflected in the material environment, in the process of its origin, processing, storage and transmission. Digital traces are characterized by a high speed of transformation, are easily destroyed and modified, can be represented by an almost infinite number of copies, are easily distributed in computer networks and are available at any point where there is a connection to the Internet.[11]

Furthermore, E.R. Rossinskaya and T.A. Saakov note that digital data can be processed by a computer, but cannot always be presented in the form of electrical signals. Thus, the quick response (QR) code, which incorporates standardized coding modes, can be recorded not on an electronic data carrier, but on paper, wood or polymer material. And although the QR code cannot produce any electrical signals, the digital information encoded in it can still be processed by an electronic device.[12]

However, such a controversial issue as the use of digital evidence in courts still remains unresolved. For example, in India, there is a lack of interaction between research institutes, forensic laboratories, investigative bodies and prosecutor's offices. It is emphasized that "law enforcement agencies lack adequate training in collection and use of evidence using cyber forensics."[13]

There is an ongoing debate among the scientific community and the BRICS countries on whether electronic evidence presented in criminal proceedings is admissible as evidence in a criminal case or not. However, the criminal legal system does not always keep up with the pace of technological development, especially in terms of the use of digital technical means.

---

[10] *Майлис Н.П.* Роль инновационных технологий в развитии цифровой трасологии // Теория и практика судебной экспертизы. 2022. Т. 17. № 2. С. 19 [Nadezhda P. Mailis, *The Role of Innovative Technologies in the Development of Digital Traceology*, 17(2) Theory & Pract. Forensic Sci. 18, 19 (2022)].

[11] *Россинская Е.Р.* Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета им. О.Е. Кутафина. 2019. № 5(57). С. 35 [Elena R. Rossinskaya, *Problems the Use of Special Knowledge for the Judicial Investigation of Computer Crimes in the Conditions of Digitalization*, 5(57) Courier of Kutafin Moscow State Law University (MSAL) 31, 35 (2019)].

[12] *Россинская Е.Р., Сааков Т.А.* Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3(15). С. 111 [Elena R. Rossinskaya & Tigran A. Saakov, *The Problems of Collecting Digital Footprints of Crimes in Social Networks and Messengers*, 3(15) Criminology: Yesterday, Today, Tomorrow 106, 111 (2020)].

[13] Mishra, *supra* note 7.

In terms of electronic evidence, one of the features of the Code of Criminal Procedure of the Russian Federation is that the emphasis is shifted to the information carrier, since the legislator uses the term "electronic information carrier." However, scientists note that the very concept of electronic evidence has a broader meaning than simply "electronic media." This is explained by the fact that the primary aspect of electronic evidence is the information itself, while the medium on which it is contained is of secondary importance.[14]

It is worth noting that investigators, in accordance with paragraph 6, Part 2 of Article 74 of the Russian Code of Criminal Procedure, are permitted to attach emails, messages, screenshots, subscriber connections, video recordings and other information recorded on special media as additional documents to the materials of criminal cases. At the same time, the question of the admissibility of such electronic documents as evidence is of central significance.[15]

Article 474.1 of the Code of Criminal Procedure of the Russian Federation establishes the procedure for the use of electronic documents in criminal proceedings. Participants in criminal proceedings can now submit various procedural documents as well as documents attached to them to the court in electronic form through the official website of the court using an electronic digital signature. Scientists believe that the very provision of this article implies the permissibility of submitting written evidence to the court in the form of an electronic document signed with an electronic signature.[16]

Thus, since the path to electronic document flow in criminal proceedings in Russia has already been opened, the reasonable continuation of the development of criminal procedural legislation should be the formation of an electronic criminal case during the pre-trial stages.

P.K. Shrivastava draws attention to the fact that in India it is necessary to take added special precautions for the identification, collection, preservation and examination of electronic evidence as it can be easily altered, damaged or destroyed as a result of improper handling or inspection.

The author emphasizes that:

> the electronic evidence should essentially satisfy the following conditions:

---

[14] *Ким Д.В. и др.* Современные направления развития криминалистических методик и технологий в уголовном судопроизводстве [Dmitry V. Kim et al., *Modern Trends in the Development of Forensic Techniques and Technologies in Criminal Proceedings*] 138 (2020).

[15] *Палиева О.Н., Семенцова И.А.* Использование искусственного интеллекта и информационных технологий в ходе расследования уголовных дел // Вестник Московского университета им. С.Ю. Витте. Серия 2: Юридические науки. 2021. № 2(28). С. 38 [Oksana N. Palieva et al., *The Use of Artificial Intelligence and Information Technology during the Investigation of Criminal Cases*, 2(28) Moscow U. Bull. named after S.Yu. Witte Series 2 Legal Sci. 38 (2021)].

[16] Kim et al. 2020, at 142.

1. It should be produced by a computer which has been used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

2. The information derived in the electronic record, was regularly fed into the computer in the ordinary course of activities;

3. The computer was operating properly;

4. The duplicate copy must be a reproduction of the original electronic record.[17]

According to the Indian Evidence Act of 1872, if a document is required to prove a fact, only the original document must be presented in court and not a copy, photograph or any other type of reproduction. Since any reproduction of a press release or document has a lower level of reliability than the original source, which opens up the possibility for fraud or falsification, the original must always be consulted.

Initially, electronic documents, if printed, were treated as secondary evidence in accordance with the strict provisions of the Indian Evidence Act. However, this attitude changed after the adoption of amendments to the Evidence Act in the year 2000:

> Section 65B provides that shall be considered documents, thereby making it primary evidence, if the pc which produced the record had been regularly in use, the knowledge fed into the computer was a part of the regular use of the PC and the PC had been operating properly. It further provides that each one computer output shall be considered as being produced by the pc itself, whether it had been produced directly or indirectly, whether with human intervention or without.[18]

Thus, the information contained in an electronic record is considered to be the original or source of documents, even if it is printed on paper, stored, recorded or copied on computer-generated media, if special conditions are met.[19]

In China, electronic data were not recognized at the legislative level as an independent type of evidence until 2012, despite their appearance in judicial practice. An amendment to the Criminal Procedure Law of the People's Republic of China in 2012 established that electronic data is recognized as an independent type of evidence, that is neither material evidence nor documentary evidence:

---

[17] P.K. Shrivastava, *Electronic Evidence in Crime Investigation-Darknet & Policing*, The Indian Police J. 43, 45 (2021).

[18] Nilima Prakash & Roshni Duhan, *Computer Forensic Investigation Process and Judicial Response to the Digital Evidence in India in Light of Rule of Best Evidence*, 8(5) Int'l J. Mgmt. & Soc. Sci. 1, 7 (2020).

[19] *Id.* at 9.

> Article 48 of the Criminal Procedure Law of the People's Republic of China (2012 Amendment) provides that electronic data shall be the eighth category of evidence, separating electronic data from physical evidence, documentary evidence, and audio-visual materials.[20]

After the adoption of this amendment, the Chinese scientific community turned its attention to the prospects for improving the relevant Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases (hereinafter, the Rules) for the use of electronic data, including their collection, storage and authentication. As a result, the application of these Rules in relation to electronic data is not possible without a specialist and the technical means used by the specialist.

Up until 2014, it was generally accepted that the collection of electronic data should be carried out by a minimum of two investigators with the relevant expertise. However, in 2016, this specified requirement for the mandatory availability of relevant specialized knowledge was abolished. Nevertheless, according to Article 6 of the Rules, adopted in 2019, the collection of electronic data must be carried out by two or more investigators, and if necessary, a specialist, "professional technician," may be involved at the direction of the investigators.[21]

At the same time, in accordance with the Rules established in China in 2019, investigators have the right to select the most appropriate method of seizure in order to complete the procedural action effectively and reasonably.[22] One should agree with the researchers who argue that

> practical needs and procedural issues are supposed to be taken into consideration before specific technologies are applied in the custody process of electronic data.[23]

In South Africa, even at the draft law stage, the Cybercrimes Act of 2020 provided for a set of procedures specifically designed for the seizure and storage of electronic evidence, as well as technical assistance from electronic service providers, financial institutions and individuals to the investigator in their search and seizure.[24]

In addition to increasing access to justice, electronic justice should also contribute to increasing the level of professionalism of investigators and judges, transparency of

---

[20] Fan Yang & Jiao Feng, *Rules of Electronic Data in Criminal Cases in China*, 64 Int'l J. L. Crime & Just. 3 (2021).

[21] *Id.* at 5.

[22] *Id.*

[23] *Id.* at 6.

[24] Eveshnie Reddy, *Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill*, 41(2) Statute L. Rev. 226 (2020).

the criminal process, as well as increasing the level of efficiency, economy and public confidence in the judicial system as a whole. That is why it is extremely important to review the current rules governing the use of electronic data in criminal proceedings to ensure that they meet the modern requirements imposed by the legal systems of each of the BRICS member countries as well as society as a whole.

2. Videoconferencing Technologies and Criminal Proceedings

Another priority area for the use of digital technology in criminal proceedings is the introduction of videoconferencing, the large-scale adoption of which is directly related to the onset of the COVID-19 pandemic in 2020. During this period, there was a pressing need to create conditions that would allow for remote work. Courts around the world were forced to respond quickly to the problems associated with the need to ensure social distancing in the context of the pandemic. The rapid transition from traditional to online procedures helped citizens gain access to the justice system even during the period of the established restrictions.

In Brazil, the problem of participation in court sessions via videoconference is still not fully resolved. In 2020, virtual hearings were held in the first instance in criminal cases and were regulated by Resolution 329 of the National Council of Justice. In addition, the application process has already been fully digitized in all Brazilian courts, with this being mandatory in higher courts.

Nonetheless, researchers continue to wonder whether the use of videoconferencing will not worsen the problems already existing in Brazil, namely the lack of universal education, a lack of resources, access to lawyers, etc. In this way, several virtual hearings were appealed, as detrimental to the right to a fair trial, on the grounds that

> Article 3(1) of Resolution 329 establishes that virtual hearings will not take place if any of the parties involved declare a "technical or instrumental impossibility" of participation.[25]

In this regard, the Brazilian Bar Association petitioned the National Council of Justice, demanding that virtual hearings be held only on a voluntary basis, subject to the consent of all parties.

The practice of using individual programs and messengers as an audiovisual contact during court sessions is interesting. In Russia, in 2020, the Nevyansky City Court of the Sverdlovsk Region began using the WhatsApp messenger in its hearings, and by the end of 2021, amendments were made to the Criminal Procedure Code of

---

[25] Octávio L.M. Ferraz et al., *Brazil: Legal Response to COVID-19*, in Jeff King & Octávio L.M. Ferraz et al. (eds.), The Oxford Compendium of National Legal Responses to COVID-19 9 (2021).

the Russian Federation, according to which it is now possible to use videoconferencing both at the stage of judicial proceedings as well as the preliminary investigation during such investigative actions as interrogation, confrontation and presentation of identification.[26]

In India, during the spread of COVID-19, "important issues" were heard in the Supreme Court via videoconference.[27] The use of videoconferencing, which was implemented to reduce the risk of COVID-19 spreading in court, helped reduce the attendance of courthouses and, as a result, contributed to the subsequent transition to virtual courts. Indian researchers believe that "within a couple of years, a well-established system of virtual vessels will appear in India."[28] It is noted that it is more difficult to organize the provision of judicial services online than a videoconference, given the large number of nuances associated with the process of introducing digital technologies into the field of legal proceedings.[29]

In *Twentieth Century Fox Films Corporation v. NRI Film Production Association (Pvt) Ltd.*, the Court pointed out the conditions that must be met in order to confirm the authenticity of the video conference:

> i) Before a witness is examined in terms of the audio-video with as is to file an affidavit duly verified before a notary or a judge that the person who is shown as the witness is the same person who is about to depose on the screen. A copy is to be made available to the opposite side.
>
> ii) The person who examines the witness on the screen is also supposed to file on undertaking before examination along with a copy to the opposite counsel/party with regard to identification.
>
> iii) The witness has to be examined during working hours of Indian court and oath is to be administered through the media.
>
> iv) The witness should not plead any innocence on account of time difference between Indian and United States of America.
>
> v) The learned judge is to record such remarks as is material regarding the demeanour of the witness on the screen.
>
> vi) Before examination of the witness, a set of plaint, written statement and other documents must be sent so that the witness becomes acquainted

---

[26] *Дударев В.А.* Пандемия COVID-19 как катализатор цифровизации российского уголовного судопроизводства // Уголовная юстиция. 2021. № 17. С. 40 [Vitaly A. Dudarev, *COVID-19 Pandemic as a Catalyst for Digitalization of Russian Criminal Justice*, 17 Russ. J. Crim. L. 39, 40 (2021)].

[27] Tania Sourdin et al., *Court Innovations and Access to Justice in Times of Crisis*, 9(4) Health Pol'y & Tech. 447 (2020).

[28] Anku Anand, *Virtual Courts: The Changing Face of Indian Judicial System*, SSRN Electronic J. (2021) (Jan. 3, 2023), available at https://doi.org/10.2139/ssrn.3865629.

[29] *Id.*

with the document and an acknowledgement is to filed before the court in this regard.[30]

In China, court sessions have been held using the Internet since the early 2000s, and their progress has been recorded using technical means, such as audio and video recording. According to researchers, the first full-fledged hearing held via videoconference in China took place in 2007 in a criminal case related to a theft in Shanghai.[31] The most advanced courts in the Chinese legal system have evolved into specialized Internet courts, created to quickly and cost-effectively resolve the rapidly growing number of disputes on the Internet. The first Internet court was established in Hangzhou in 2017, and in 2018 two more were established in Beijing and Guangzhou.

> The Internet courts are the first courts in China where the entire litigation process can be conducted online, including filing and service of documents, collection and presentation of evidence, preservation of assets, the trial, judgment, enforcement, appeal and other processes. The Internet Courts have integrated mechanisms and network solutions to build a multi-level, diversified online dispute resolution system, which includes pre-trial mediation before initiating the litigation process. The online trial uses a videoconferencing system. Any parts of the proceedings can be conducted offline upon the request of the parties involved or the needs of the trial.[32]

One of the main technological subjects in the "informatization" of Chinese ships is the company "Xinshiyun," which specializes in cloud computing technologies and related services, including live streaming of court sessions and video recording. Thus, the company possesses the largest video storage facility for court trials in the country.[33]

It is worth noting that there are several circumstances in which a live or recorded broadcasts of hearings are prohibited. These include

> the explicit objection of disputing parties in civil and administrative cases, the explicit objection of the procuratorate in criminal cases and cases involving national secrets, commercial secrets, young offenders etc.[34]

---

30 Prakash & Duhan 2020, at 7–8.

31 Shi et al. 2021, at 7.

32 Zou, *supra* note 5.

33 Shi et al. 2021, at 18.

34 *Id.*

In South Africa, in 2020, in an effort to reduce the risks associated with the spread of COVID-19, the chairmen of the courts were given the right to decide at their discretion the format in which the hearing of their cases would be held. Thus, the hearing of the case could be held virtually, subject to the previously existing guarantees regarding virtual or absentee proceedings specified in the Criminal Procedure Act of 1977 of South Africa. A cloud-based collaboration solution was also implemented in the Supreme Courts of South Africa, which enabled the parties to file their objections electronically.[35] Nevertheless, despite the measures taken to ensure citizens' access to justice, there were concerns that there might be problems; for instance,

> there have been reports expressing concern that access to justice may be compromised by teething problems in conducting hearings via video conferencing, especially given uneven access to technological resources in remote areas.[36]

One of the primary advantages of using videoconferencing in criminal proceedings is that it increases the level of citizens' access to justice as a result of reducing time and financial costs, since participants in the process do not have to spend time and money travelling to and from court, particularly in cases where the parties reside in another city. Furthermore, the use of videoconferencing is considered justified if a participant in an ongoing investigative action cannot personally participate in it for such objective reasons as

> being in a different locality, in correctional institutions, in medical institutions where even a short-term violation of the regime prescribed by a doctor is impossible (for example, connected to medical equipment, a serious health condition, quarantine measures), compliance by a citizen with the regime of self-isolation and quarantine in a pandemic, etc.[37]

Additionally, the use of videoconferencing technology makes it possible to ensure the safety of participants in the criminal process. In cases where it is necessary to keep the identity of a participant in criminal proceedings confidential so as to prevent the participant from being recognized, then in the process of conducting such investigative actions as a confrontation or interrogation, as well as a court

---

35 Sourdin et al. 2020.

36 Petronell Kruger et al., *South Africa: Legal Response to Covid-19*, in Jeff King & Octávio L.M. Ferraz et al. (eds.), The Oxford Compendium of National Legal Responses to COVID-19 10 (2021).

37 *Буфетова М.Ш., Кобзарь Д.Н.* Применение систем видеоконференц-связи в уголовном судопроизводстве: перспектива изменения законодательства // Адвокатская практика. 2021. № 1. С. 17 [Maryam Sh. Bufetova & Dmitry N. Kobzar, *The Application of Video Conferencing in Criminal Proceedings: Prospects of Legal Changes*, 1 Law Prac. 14, 17 (2021)].

session, video conferencing that allows for the possibility of changing appearance and voice can be used. The use of videoconferencing in this manner allows for the avoidance of any physical or mental impact on witnesses or victims, thereby reducing the likelihood of their refusal to participate in the process.[38]

All of these factors working together lead to an increase in the reliability of testimony since participants safety concerns diminish and the honesty and frankness of their testimony increases.[39]

Nonetheless, despite these advantages, a number of issues related to technical equipment may arise in the criminal process. For example, participants should have the necessary technical resources in order to be able to hear and see the progress of an investigative action or a court session, as well as to connect at the right time to the process of their conduct. In addition, power outages, poor image quality and sound distortion, load from network users, poor Internet connection quality, etc. may lead to the results of the investigative action being deemed unacceptable or to the postponement of the court session.

The reliability and acceptability of the results of the hearing are thus directly related to the quality of image and sound, protection from external interference in the videoconferencing process, as well as the security of obtaining and preserving personal data. To solve these problems, it is necessary to allocate significant funds for the purchase of special equipment as well as to create specialized software to organize a secure videoconferencing session.

3. Application of Artificial Intelligence Technologies in Criminal Proceedings

To date, scientists believe that the main and most realistic way to use artificial intelligence technologies in criminal proceedings is to use them only as an auxiliary tool to assist in the work of the investigators, judges and other participants in criminal proceedings in order to increase the efficiency of their activities and reduce subjective errors to a minimum. This option is already firmly established in criminal procedure practice and will continue to remain widely prevalent for the foreseeable future.[40]

---

[38] *Силантьева И.Р.* Проблемы и перспективы использования систем видеоконференц-связи в процессе правореализации // Вектор науки Тольяттинского государственного университета. 2013. № 1(23). С. 248 [Inessa R. Silantieva, *Problems and Prospects of Use of Systems of a Video Conferencing in the Process of Right Realization*, 1(23) Science Vector of Togliatti State University 245, 248 (2013)].

[39] *Жайворонок Д.А., Бокова О.И.* Проблемы организации видеоконференц-связи в суде // Вестник Воронежского института высоких технологий. 2021. № 2. С. 41 [Denis A. Zhaivoronok & Oksana I. Bokova, *Problems of Video Organization in Court*, 2 Bulletin of the Voronezh Institute of High Technologies 40, 41 (2021)].

[40] *Соломатина А.Г.* Допустимость использования искусственного интеллекта в уголовном судопроизводстве // Вестник Московского университета МВД России. 2020. № 3. С. 97–99 [Anna G. Solomatina, *Admissibility of the Use of Artificial Intelligence in Criminal Proceedings*, 3 Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia 97 (2020)].

When examining the problems surrounding the permissibility of using the capabilities of artificial intelligence in the investigation, researchers from both Russia and other countries have pointed to the prospects[41] and increasing introduction of these technologies into investigative activities,[42] despite the possible difficulties in the assessment and admissibility of certain types of evidence in the future. This state of affairs is connected with the increasing volume of data subject to analysis (videos and images, information about telephone calls of subscribers, the content of content posted on social networks, etc.) and has the potential to significantly alter the investigative situation, reduce the time spent by the investigator (inquirer) and make the conduct of an investigative or other procedural action more effective.[43]

It should be noted that currently, artificial intelligence systems are not used in the production of investigative actions "in their purest form."

In Brazil, an experiment was conducted that was aimed at solving problems with the help of artificial intelligence related to the growing workload due to the large number of criminal cases opting for pre-trial detention. One of the objectives of the experiment was to investigate the possibility of artificial intelligence making a decision to release a prisoner in accordance with the decision on pre-trial detention. At the same time, the researchers emphasized that the experiment was in the nature of creating a model based on previous court decisions and not on their automatic issuance, since such decisions would typically be made by a human judge after an assessment. As a result, the researchers obtained satisfactory results on this question. The authors of the study believe that

> in terms of application, while the classification results can speed up the judgment, for example, when the period of pre-trial detention has already expired, the association results can identify patterns in judgments and thus reduce biases.[44]

---

41 *Бахтеев Д.В.* Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 3–6 [Dmitry V. Bakhteev, 9 *Artificial Intelligence in Investigative Activities: Tasks and Problems*, Russ. Investigator 3 (2020)].

42 Xiaoyu Du et al., *SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation*, Proceedings of the 15th International Conference on Availability, Reliability and Security 1 (2020).

43 *Русман Г.С., Смолин М.С.* Возможности использования искусственного интеллекта при производстве следственных и иных процессуальных действий // Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде / под ред. С.В. Зуева, Д.В. Бахтеева [Galina S. Rusman & Mikhail S. Smolin, *The Possibility of Using Artificial Intelligence in the Production of Investigative and Other Procedural Actions*, in Sergey V. Zuev & Dmitry V. Bakhteev (eds.), The Use of Artificial Intelligence in the Detection, Disclosure, Investigation of Crimes and Consideration of Criminal Cases in Court] 84 (2022).

44 Thiago R. Dal Pont et al., *Classification and Association Rules in Brazilian Supreme Court Judgments on Pretrial Detention*, 10th International Conference on Electronic Government and the Information Systems Perspective (2021) (Jan. 3, 2023), available at http://dx.doi.org/10.1007/978-3-030-86611-2_10.

Furthermore, in Brazil, the Prosecutor's Office of the State of Rio Grande do Norte (MPRN), in collaboration with the Federal University of Rio Grande do Norte (UFRN), developed the platform INSIDE (Integration, aNalySis, vIsualization of Data for invEstigation). This platform was conceived to process big data and speed up the procedures for their research, which in and of itself is a very time-consuming process.

> As a result of this paper, we can conclude that the proposed architecture is a viable option as a system to help the analysis of digital evidences. The architecture ability of reading, processing, and classifying large amounts of images, with agility and precision, allowing the forensic analyst to have an easier and faster process in the analysis of these digital evidences.[45]

In the Russian Federation, the use of artificial intelligence is most pronounced in the work of criminologists. As a result, in order to conduct a preliminary analysis in the course of an expert study of handwriting, a neural network was created at the Ural State Law University. This neural network was trained on the basis of handwriting samples and is capable of analyzing 480 parameters that are inaccessible to a human expert. As a result, the system is able to identify, with a high degree of accuracy, the signs that differentiate between genuine and forged signatures, as well as the private and general signs that characterize the person who executed them.[46]

Moreover, in Russia, artificial intelligence technologies are also used in the system of forensic registration of internal affairs bodies, in particular, forensic accounting is being developed in the country.[47]

As a rule, one of the advantages of using artificial intelligence in criminal proceedings is the possibility of the system making decisions in lieu of a judge. In support of this judgment, it is argued that the technology in question cannot be negatively influenced by emotions on decision-making and instead is able to adhere to the norms established by law. This can help reduce the likelihood of corrupt actions and decisions. Additionally, it is impossible not to mention the fact that artificial intelligence is able to process incomparably larger amounts of data and operate them significantly faster compared with the cognitive abilities of a human judge. Artificial intelligence makes decisions based on the analysis of a variety of

---

[45] Iaslan Silva et al., *Using Micro-Services and Artificial Intelligence to Analyze Images in Criminal Evidences*, 37 Forensic Sci. Int'l: Digital Investigation 301197, 301205 (2021).

[46] *Ушаков Р.М.* Технология Big Data как вектор развития криминалистической техники: перспективы применения в контексте их правомерности // Уральский журнал правовых исследований. 2020. № 2(9). С. 65 [Ruslan M. Ushakov, *Big Data Technology as a Direction of Development of Criminalistic Technique: Prospects for Application in the Context of their Lawfulness*, 2(9) Ural J. Legal Res. 54, 65 (2020)].

[47] Kim et al. 2020, at 14, 161.

data, in particular information characterizing the participants in the case. These advantages can be crucial when working with data from the repositories of public services, including criminal cases that have remained undisclosed for a long time for one reason or another, as well as when working with the archives of court cases and reference legal systems.[48]

However, there is also a significant drawback to the use of artificial intelligence, which, according to A.V. Kholopov, practically excludes the use of artificial intelligence in criminal proceedings. The process and logic of decision-making developed by artificial intelligence, as well as their objectivity and impartiality, cannot be rechecked, and therefore, it is impossible to implement the verification principle.[49]

As an example, we can cite the computer program "Laser," which was created to save time and improve the accuracy of the work of judges as well as help them in making decisions and sentencing. After the judge enters certain data from the materials of the criminal case into the program, the program issues a draft reasoned decision. However, "many judges do not see the point in its application because of a possible violation of the principles of criminal procedure."[50]

India also pays special attention to the development of artificial intelligence technologies aimed at collecting criminally significant information. A number of cities in India use facial recognition technology via a network of closed circuit television (CCTV) cameras to identify and track criminals. For example, in 2020, the Delhi police used artificial intelligence, along with other digital technical means, during the investigation of 755 cases of violence in Northeast Delhi. The criminals were arrested as a result of 945 recordings obtained from surveillance cameras and videos from smartphones that were analyzed using artificial intelligence capable of recognizing faces.[51]

In China, artificial intelligence, being one of the leading trends in the development of criminal justice, has found its application in electronic justice, for example, as part of the 'Smart Courts' system as well as a separate tool aimed at improving the efficiency of investigative actions.

---

[48] *Воскобитова Л.А.* Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5(150). С. 91–104 [Lydia A. Voskobitova, *Criminal Justice and Digital Technology: Compatibility Issue*, 5(150) Lex Russica 91 (2019)].

[49] *Холопов А.В.* Человек в условиях цифровизации права: проблемы и пути развития // Юридическая наука. 2020. №. 6. С. 10 [Alexey V. Kholopov, *A Person in the Conditions of Digitalization of Law: Problems and Ways of Development*, 6 Legal Sci. 8, 10 (2020)].

[50] *Степанов О.А., Басангов Д.А.* О перспективах влияния искусственного интеллекта на судопроизводство // Вестник Томского государственного университета. 2022. № 475. С. 232 [Oleg A. Stepanov & Denis A. Basangov, *On the Prospects for the Impact of Artificial Intelligence on Judicial Proceedings*, 475 Tomsk St. Univ. J. 229, 232 (2022)].

[51] Dr. O. Gambhir Singh, *Artificial Intelligence in Forensics & Criminal Investigation in Indian Perspective*, 7(8) Int'l J. Innovative Sci. & Res. Tech. (IJISRT) 142, 144 (2022).

Tools that are based on artificial intelligence can assist judges in making decisions, provide the parties with legal reference information, as well as scan and accept case materials in electronic form and compile and form procedural documents for the participating parties. This use of artificial intelligence significantly accelerates the presentation and classification of evidence, as well as the transfer of case materials between courts of different instances.[52]

To prevent possible contradictions that may arise as a result of the use of artificial intelligence technologies, scientists from China propose introducing a state policy aimed at prohibiting the use of artificial intelligence in the role of a judge. Such restrictions are related to the fact that the use of artificial intelligence can influence judges and make them hesitant to state in detail their position on the decision being made in the case. As a result, decisions made without the participation of a human judge may be unclear and difficult for the rest of the participants in the criminal process to understand.[53]

In addition to courtroom proceedings, artificial intelligence has found other applications, for instance, as a camera system aimed at recognizing faces for the subsequent arrest of suspects. Thus, the "Tian Yan" camera system, after an identity has been identified, can provide personal information, such as a name and a national identity card, using databases of police departments and state archives.[54]

Thanks to the 3.0 System, it became possible to automatically determine the importance of the content of evidence and create preliminary "chains of evidence" in criminal cases. These "chains" form the basis of investigative versions and are available for further correction by the investigator. This helps investigators determine the completeness of the investigation and judicial officers estimate the sufficiency of the sentence.[55]

Thus, participants in criminal proceedings should not rely solely on the results obtained through the use of such a useful tool as artificial intelligence technology. Unfortunately, the criminal procedure legislation cannot keep up with the rapid pace of technological progress and its incorporation into everyday life. This, in turn, causes serious gaps in the regulation of the permissibility of the use of digital technologies. That is why the advantages of using artificial intelligence in criminal proceedings, such as increasing the accuracy and speed of work, objectivity and reliability of evidence, should encourage scientists and legislators in the BRICS countries to clearly address the existing gaps in the system.

---

52 Zou, *supra* note 5.

53 Shi et al. 2021, at 10.

54 Nyu Wang & Michael Y. Tian, '*Intelligent Justice': AI Implementations in China's Legal Systems*, in Artificial Intelligence and its Discontents 202 (2022).

55 *Id.* at 208.

4. 3D Technologies in Criminal Proceedings

With regard to the issue of the use of technical means in criminal proceedings, particular attention is paid to the possibility of using various 3D technologies.

Researchers from Brazil reported on the successful implementation of forensic approximation (reconstruction) of a face based on photogrammetry. As a result, the visual representation of an appearance recreated in the virtual environment led to a successful identification.

> The methodology employed in the collection contemplated taking 22 digital photographs at a resolution of 300 ppi (pixels per inch) stored in JPG format with a high-quality factor, portraying the skull from several angles, totaling 360°. This process was repeated in two distinct positions, enabling the generation of a model that included all sides of the photographed piece. The images were then copied to the hard disks of the computers, without any modification, so that they could be processed in accordance with the examination needs.[56]

The appearance, which was recreated with the help of special software, was then adapted and modeled in 3D format. The resulting face was superimposed on the skull and its soft tissue markers, taking into account anatomical features, similar to how it would be done in a manual technique. On the basis of this information, the researchers came to the conclusion that such an approximation of a face, while not the predominant method of identifying a person, may be employed to identify a person. However, it is noted that although 3D facial reconstruction is widely researched and distributed in scientific circles, its use in criminal proceedings is extremely rare.

Russian scientists also believe that the use of a 3D scanner can significantly improve the quality and quantity of evidentiary information obtained, which can then be used during situational examinations, thereby allowing for the reconstruction of an event in conjunction with the actions of the criminal and the mechanisms of the incident event.[57]

The authors of this article conducted an experimental examination of the type of scene mentioned above using a software sample that creates a virtual copy by processing the results of a spherical panoramic survey conducted indoors from five different shooting points. The specified software sample combines spherical photography technologies and virtual reality. Such 3D modeling of the scene of the

---

[56] Rosane P. Baldasso et al., *3D Forensic Facial Approximation: Implementation Protocol in a Forensic Activity*, 66(1) J. Forensic Sci. 383, 384 (2021).

[57] Mailis 2022, at 20.

incident will contribute to increasing the level of detail, clarity and reliability of the presentation in the field of criminal proceedings and also:

> will solve a number of problems that arise during the examination the crime scene and further use of its results. These problems include: the incomplete view of the space during photographing, the variability of examination conditions due to objective and subjective factors, the insufficient reliability of the results of the examination the crime scene and the impossibility of reexamination the crime scene due to distortion of the situation.[58]

Researchers from South Africa conducted a large-scale systematic study of the literature, in which they analyzed research trends in the field of 3D reconstruction of the crime scene, as well as the tools, technologies, methods and techniques used in it over the last 17 years. However, as these researchers also point out, although 3D reconstruction of crime scenes has already been studied as an additional tool in the investigation process, such technology has not yet been widely used nor is it actively implemented in the regular operations of law enforcement agencies and courts, including in South Africa itself.[59]

Researchers from India also evaluated the knowledge and practical application of 3D scanning and 3D printing by criminologists. However, their results allowed them to conclude that these digital technologies are used only by researchers in a select number of laboratories and that knowledge about such technologies is limited among practicing criminologists in India.

> On assessing the knowledge regarding 3D scanning and printing technology, it was observed that, while the practitioners are aware of the technology, they had limited expertise because their primary source of information was either the internet or research publications.[60]

Therefore, the researchers propose to draw the attention of criminologists throughout India as well as the legal system of the state, to the importance of using these technologies in practice, which is especially important, since the researchers are confident that 3D printed models will become an integral tool for comparative identification of unidentified corpses. In addition, fired bullets can be scanned and

---

[58] Galina Rusman & Elizaveta Popova, *Development of the Software for Examination of the Crime Scene by Using Virtual Reality, Based on Spherical Panoramic Shot and 3D-Scanning*, 2020 Global Smart Industry Conference (GloSIC) 297 (2020).

[59] Mfundo A. Maneli & Omowunmi E. Isafiade, *3D Forensic Crime Scene Reconstruction Involving Immersive Technology: A Systematic Literature Review*, 10 IEEE Access 88821, 88849 (2022).

[60] Abraham Johnson et al., *Application of 3D Scanning and 3D Printing in Forensic Practices – A Preliminary Survey among Forensic Practitioners in India*, 28 Forensic Imaging 200498 (2022).

printed in 3D format for subsequent comparison of the degree of deformation with analogues.[61]

In China, special attention is paid to forensic imaging, namely 3D technology such as virtual autopsy (otherwise known as "virtopsy"). Virtual autopsy

> is a noninvasive or minimally invasive approach to autopsy that uses modern medical imaging and computer technologies, together with anatomical principles and technical adjuncts, to obtain both internal and external positive information and to ascertain the cause of death without causing damage – or at least mitigating damage – to the body.[62]

Virtopsy uses digital radiological methods to scan corpses and obtain their images in 3D format. This method meets the requirements of objectivity and repeatability in addition to being non-invasive. The resulting images are objective and independent of viewing at any time after the scan is completed, and therefore, they can either complement or become an alternative to traditional surgical autopsies. According to M. Zhang, such non-destructive 3D scanning can reveal damage as compared to the traditional way that can destroy or accidentally damage a part:

> For example, in forensic ballistics, it is important to find out the bullet path in victims, forensic imaging is definitely a fantastic method to investigate the original trajectory instead of destructively dissect the paths.[63]

Later, when the results of such a virtual autopsy are presented as evidence at a court hearing, all of the participants in the criminal process will be able to intuitively understand and easily perceive them.[64]

As a result of such advantages as three-dimensional visualization and the high accuracy and speed of the results obtained, the quality of perception and visibility of the materials presented to the participants in the criminal process increases. All of these factors together lead to an increase in the efficiency of law enforcement agencies and contribute to fair sentencing in the courts.

---

61 Gargi Jani et al., *Three-Dimensional (3D) Printing in Forensic Science – An Emerging Technology in India*, 1 Annals of 3D Printed Med. 1, 5–6 (2021).

62 Ligang Tang et al., *Application of Virtopsy in the Police Activities in China*, 7(1) J. Forensic Sci. & Med. 24 (2021).

63 Min Zhang, *Forensic Imaging: A Powerful Tool in Modern Forensic Investigation*, 7(3) Forensic Sci. Res. 385 (2022).

64 *Id*.

Conclusion

Currently, legislators in the BRICS member countries, including the Russian Federation, have not yet enacted any specific regulations regarding the potential of applying the results and findings of the use of digital technical means in criminal proceedings. At the same time, legal regulation is especially important in connection with the emergence of completely new technologies as well as the obsolescence of existing technologies and their replacement.

Scientists from each of the BRICS member countries have repeatedly emphasized the lack of a legal framework as the main problem faced by investigators and courts. Criminal proceedings are a highly formalized type of process due to the nature of coercion that they involve. Untimely amendments to the legislation lead to the appearance of significant gaps, which may consequently result in the failure to establish the circumstances of the criminal case. In order to ensure a fair trial, it is necessary to adapt to the latest realities of our time, namely, to introduce digital technologies and timely create the necessary regulatory framework aimed both at combating cybercrimes that are spreading today and at protecting the rights of individuals involved in criminal proceedings.

The researchers pay special attention to the conditions governing the use of the latest digital technical means in criminal proceedings, since their use entails new challenges for the legislative and judicial authorities. It is widely believed that even the most advanced technologies will never be able to replace a highly qualified lawyer. This applies, first and foremost, to the use of artificial intelligence and further evaluation of the results of its work.

The dominant place among the recent trends in the development of criminal proceedings in the BRICS member countries is occupied by the use of electronic evidence in proving cases. The advantages of using digital technology in the criminal proceedings of the BRICS countries include an emphasis on the introduction of electronic justice and the use of electronic data, which opens up new prospects for the further improvement of both the regulatory and theoretical frameworks.

In turn, the expanding introduction of videoconferencing, especially during the preliminary investigation, necessitates amendments to the criminal procedure legislation. In other words, it requires regulating the procedural process for the use of technology and subsequent consolidation of the results of such investigative actions. This is necessary in order to provide an opportunity to use the results of the use of videoconferencing in establishing proof and to ensure their compliance with the criteria of admissibility and reliability of evidence.

At the same time, it is necessary to pay due attention to problems such as the lack of specialized bodies, the insufficient level of qualification of investigators and specialists, as well as the vagueness of wording in the criminal law legislation of all the BRICS member countries and the provisions of relevant regulations. In order for

participants to be able to adapt to the rapidly changing global trends, they need to have an understanding of the modern technologies that are capable of radically changing the law, improving it, and thereby increasing its overall effectiveness with the help of modern digital technical means. To accomplish this, it is necessary to involve experts from a variety of fields to understand the nuances of each of these technologies, as well as to train law enforcement officers and courts; for example, in the field of 3D technologies, in order to promote their dissemination and implementation in practice.

Thus, the prospects for further development of criminal proceedings based on the use of advanced digital technologies depend on the results of their application being permissible and not violating the rights of the individual involved in criminal proceedings. It is necessary that the introduction and use of such technologies at any stage of the criminal process comply with the criminal procedure legislation so as to ensure maximum objectivity of criminal procedural activities as well as procedural efficiency and efficacy.

References

Baldasso R.P. et al. *3D Forensic Facial Approximation: Implementation Protocol in a Forensic Activity*, 66(1) Journal of Forensic Science 383 (2021). https://doi.org/10.1111/1556-4029.14587

Du X. et al. *SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation*, Proceedings of the 15th International Conference on Availability, Reliability and Security 1 (2020).

Johnson A. et al. *Application of 3D Scanning and 3D Printing in Forensic Practices – A Preliminary Survey among Forensic Practitioners in India*, 28 Forensic Imaging 200498 (2022). https://doi.org/10.1016/j.fri.2022.200498.

Maneli M.A. & Isafiade O.E. *3D Forensic Crime Scene Reconstruction Involving Immersive Technology: A Systematic Literature Review*, 10 IEEE Access 88821 (2022). https://doi.org/10.1109/ACCESS.2022.3199437

Mishra B. et al. *Traditional Judicial Systems Need Ammunition for Future*, 24(2) Journal of Legal, Ethical and Regulatory Issues 1 (2021).

Oliveira E., Jr. et al. *Digital Forensics Experimentation: Analysis and Recommendations*, 34(1) Forensic Science Review 21 (2022).

Reddy E. *Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill*, 41(2) Statute Law Review 226 (2019). https://doi.org/10.1093/slr/hmz001

Rusman G. & Popova E. *Development of the Software for Examination of the Crime Scene by Using Virtual Reality, Based on Spherical Panoramic Shot and 3D-Scanning*, 2020 Global Smart Industry Conference (GloSIC) 297 (2020). https://doi.org/10.1109/GloSIC50886.2020.9267871

Silva I. et al. *Using Micro-Services and Artificial Intelligence to Analyze Images in Criminal Evidences*, 37 Forensic Science International: Digital Investigation 301197 (2021). https://doi.org/10.1016/j.fsidi.2021.301197

Sourdin T. et al. *Court Innovations and Access to Justice in Times of Crisis*, 9(4) Health Policy & Technology 447 (2020). https://doi.org/10.1016/j.hlpt.2020.08.020

Tang L. et al. *Application of Virtopsy in the Police Activities in China*, 7(1) Journal of Forensic Science and Medicine 24 (2021).

Yang F. & Feng J. *Rules of Electronic Data in Criminal Cases in China*, 64 International Journal of Law, Crime and Justice (Article 100453) (2021).

Yu J. & Xia J. *E-Justice Evaluation Factors: The Case of Smart Court of China*, 37(4) Information Development 658 (2021).

Zhang M. *Forensic Imaging: A Powerful Tool in Modern Forensic Investigation*, 7(3) Forensic Sciences Research 385 (2022). https://doi.org/10.1080/20961790.2021.2008705

Information about the authors

Galina Rusman (Chelyabinsk, Russia) – Head, Department of Criminal Procedure, Criminalistics and Forensic Examination, South Ural State University (National Research University) (76 Lenina Ave., Chelyabinsk, 454080, Russia; e-mail: rusmangs@susu.ru).

Eugenio D'Orio (Ischia, Italy) – Director, Bio Forensics Research Center (181 Via Michele Mazella, Ischia, NA, 80077, Italy; e-mail: eugenio.dorio@bioforensics.it).

Elizaveta Popova (Chelyabinsk, Russia) – PhD candidate, Department of Criminal Procedure, Criminalistics and Forensic Examination, South Ural State University (National Research University) (76 Lenina Ave., Chelyabinsk, 454080, Russia; e-mail: popovaes@susu.ru).

Pavlos Kipouras (Naples, Italy) – Document Examiner, Professional Graphologist, Lawyer, School of Forensic Graphology (40 Ioulianoy Rd., Athens, 10434, Greece; e-mail: contact@grafologoskipouras.gr).

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).

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).

LEGITIMATE EXPECTATIONS OF PRIVACY IN THE ERA OF DIGITALIZATION

ELENA OSTANINA,

Chelyabinsk State University (Chelyabinsk, Russia)

ELENA TITOVA,

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

https://doi.org/10.21684/2412-2343-2023-10-1-109-125

This article contends that in the present era of digitalization people's right to privacy should be protected no less than it was before the widespread use of digital technologies. When taking into account the fact that digitalization has led to a greater exchange of information, it is important that the ways and forms of protecting privacy undergo certain changes. Firstly, more emphasis should be placed on the use of methods for the self-protection of privacy rights, including restricting access to information and configuring website settings so that reviews and comments can be posted only by registered users, and not anonymously. Secondly, the legal means of protection should be improved to prevent violations of privacy rights from occurring as well as to ensure that rights which have been violated are properly restored. In the event of a violation of the secrecy of personal data, the authors recommend the use of class actions. When a violation of the secrecy of correspondence, medical information or telephone conversations by a business entity or the owner of a website occurs, a claim for compensation for moral damage should be available. However, the authors of the article propose modifying such a claim for compensation for moral damage to more closely model a claim for the recovery of punitive damages. Furthermore, the authors establish a connection between the protection of the right to privacy and the variety of relevant information on the topic that is freely available.

Keywords: personal data; right to privacy; compensation for moral damage; punitive damages; medical secrecy; correspondence secrecy; banking secrecy.

Recommended citation: Elena Ostanina & Elena Titova, *Legitimate Expectations of Privacy in the Era of Digitalization*, 10(1) BRICS Law Journal 109–125 (2023).

Table of Contents

Introduction

Privacy is one of the most important intangible personal benefits protected by constitutional and civil law. In the present era of digitalization, people voluntarily share their personal information as well as post their photographs on social media networks and other websites where they pay for goods, labor and services. As a result the question arises: How much should privacy protection change in the face of digitalization? Related to this question are other questions. In particular, can a person expect not to be filmed in public places without warning? And to what extent can a person object if a segment of this filming is used, for instance, on the network to illustrate news (such as, for example, the news about the fall of the meteorite that occurred in Chelyabinsk)? A person who participates in communication on a particular website or conducts transactions through an online platform typically expects that the information provided by him or her will be used only temporarily and only for the purposes for which it is provided.

Meanwhile, published jurisprudence shows that the use of information provided by a person is not always limited to the immediate purpose for which the information is provided. Two examples of unexpected (from the person's perspective) uses of the information provided by a person can be given.

The first is the case concerning the Prodoctorov.ru website (Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 12 November 2019 No. 14-KG19-15). A person granted permission to an employer to post information about the person's education, experience and expertise, as well as

a photograph on the company's website. All this information was published on the website of the medical organization, that is, it was freely accessible. Furthermore, the information was posted on the website "Prodoctorov.ru" such that users of the site could leave feedback on the professional activities of the doctor. Citing the fact that it was private information, the person demanded that it be removed from the Prodoctorov.ru website The Supreme Court of the Russian Federation sent the case for a new trial, stating that during the new trial it should be determined whether or not the discussion of the doctor's professional activities is of public interest, and it should also be determined whether or not the plaintiff has effective means of protection against the anonymous reviews left on this website.

The second example is the well-known dispute that occurred between the Vkontakte society and the Data society (case no. A40-18827/2017, which was resolved by an amicable agreement reached between the two parties). The essence of the dispute was that the defendant had developed a program for processing the information posted by users on the Vkontakte social network. This information was made available in a machine-readable form and used for commercial purposes. According to the plaintiff, the defendant did not have the right to extract and use the information that was posted on the social network "VKontakte." It is noteworthy that the focus of the discussion was on the potential commercial opportunities presented by the use and processing of data. To what extent did users who posted information about themselves on a social network understand that they were adding their "brick" to a commercially valuable data array? This question remained open.

The age of digitalization has thus posed new challenges to constitutional and civil law. People, as participants in property and non-property relations, on the one hand, are clearly reluctant to part with privacy, medical, banking and other confidential information; on the other hand, generalized and machine-readable information about the activities of people on the network, their inclinations, preferences, habits, as well as their usual locations and places of residence have commercial value, including for targeted advertising. The commercial demand for information data creates supply. On the one hand, site owners are expected to make increased technical efforts to protect the information provided by users. On the other hand, it takes effort on the part of lawyers to distinguish the legitimate use of user information from the improper use of information. If the development of technical methods of protection is a task for an engineer rather than for a lawyer, then the definition of acceptable forms and methods of protection is a legal task in and of itself.

1. Privacy as a Protected Intangible Personal Good

Privacy is one of the most traditional and essential components of intangible personal benefits. The right to privacy is one of the indispensable foundations of personal well-being, and respect for privacy is a *sine qua non* of a democratic society.

The right to privacy is an absolute subjective civil right. This right covers the physical and psychological integrity of the individual, including the right to live in solitude without attracting unwanted attention.

At the same time, activities of a professional or business nature cannot be completely excluded from the content of private life.

Like any other moral right, the right to privacy may be limited in the name of public interest or to protect a more significant private interest, such as the protection of the right to life or health, and its boundaries in any given dispute are determined by taking into account the nature and value of those interests for the sake of which it is supposed to limit the personal non-property right.

In particular, the free use of a photograph of a person is not allowed as a general rule; the consent of the person depicted is required. However, in certain cases provided for by law, the consent of the person depicted is not required. One of the exceptions is the case when the use of the image is carried out in the interests of the state or public or other public interests (Art. 152.1 of the Civil Code of the Russian Federation). A similar provision is contained in the case law of other countries. For example, the Austrian Supreme Court heard a dispute regarding the use during a newscast of a photograph of a girl who had been abducted and then managed to escape from her abductor. The defendant, in an effort to prove the legitimacy of the use of the photograph, referred to the fact that during the search for the girl, her photograph was widely distributed and published by almost all local media. The court, however, disagreed with these arguments, stating that while the search for the missing girl was ongoing, the use of the photograph was justified by a purpose that was of public significance. Once the girl was found, however, there was no public interest in showing her photograph, and the privacy of the person depicted should certainly not have been compromised. Therefore, the court considered the use of a photograph in a news release without the consent of the person depicted a violation of the personal non-property right of the depicted person.[1]

In the era of digitalization, when information is being shared at an increasing rate, personal non-property rights need to be protected in a more effective manner. The fact that information about private life and personal data can be accessed from open sources does not, in and of itself, deprive people of the right to protect their privacy and personal data.

---

[1] *See* the details of this argument in Elena A. Ostanina, *Is It Allowed to Quote Photos in Austria? Translation of the Decision of the Supreme Court of Austria Dated 26 Sept. 2017 No. 4 Ob 81/17S and Commentary to It*, 10 Bull. Econ. Just. RF 49 (2018).

2. The Concept of Reasonable Expectations in Relation to the Protection of Privacy

In the legal literature, legitimate expectations are defined as one of the means of legal certainty, as a reaction of the rule of law to the need to protect the rights and legitimate interests of people from potential arbitrariness and abuse that arise in a situation of constant change, including those that are objectively predetermined. Legitimate expectations are an important means of ensuring people's confidence in the law and the courts.[2] If the legitimate expectations of people are taken into account, it is more likely that a norm that corresponds to legal expectations will operate effectively, not only because it is provided with sanctions but also because it is perceived as fair or even as the only possible option.

What legitimate expectations do people have in the era of digitalization? In sociology, the uneven processes of the digitalization of society are noted.[3] The majority of people who have been immersed into the process of digitalization are residents of large cities, and they, as a rule, are accustomed to remaining "unrecognized in the crowd" and disclosing as little information as possible about their private lives. On the other hand, people, who later became involved in the digitalization process, gained access to the already established Internet culture, which allowed them to maintain their anonymity, the ability to use pseudonyms and pictures instead of their own images and other means to distinguish between their own "I" and the character acting online. In other words, the Internet community has developed to a point where there is sufficient respect for privacy. There are, of course, exceptions, such as websites that debate news from the sports or entertainment industries, but even in these cases, the reduction in privacy protection applies only to those whom the European Court of Human Rights once referred to as "faces of modern history." These faces of modern history are actors, writers, politicians, members of the ruling royal families and anyone who has a significant influence on the formation of public opinion. According to the precedent that has been set by the European Court of Human Rights, the activities of influential people in modern history that may have an impact on the life of society may be discussed freely. However, private life events that are not considered significant to society remain the subject of protection and are included in the concept of "privacy."[4]

Furthermore, when many services became available online, consumers typically believed that the personal data they transmitted was protected at least as well as

---

[2] Mikhail V. Presnyakov, *The Problem of Substantive Certainty and Constitutional Protection of Social Rights*, 6 Const. & Mun. L. 16 (2020).

[3] Olga M. Slepova, *Formation of Adaptive Behavior in Conditions of Deepening Information and Digital Inequality*, Author's review to the thesis of Candidate of Sociology, Penza 8 (2019).

[4] ECHR Ruling of 24 June 2004 in the case *Von Hanover (Princess of Hanover) (Von Hannover) v. Germany* (complaint No. 59320/00).

if the information were transmitted on paper. When people enter into contractual or public law relationships and exchange information about themselves, they have a legitimate expectation to receive the maximum care from the person who receives, processes and stores the information in digitized form.

Thus, the legitimate expectation of people in relation to the inviolability of their private lives is that both their personal data and their private lives will be protected with the utmost diligence.

The extent to which these legitimate expectations are realized or not realized can be inferred from news reports concerning the "leakage" of certain information about a person.

"In the first half of 2019, the Central Bank found 1.5 thousand ads on the Web for the sale and purchase of databases of personal data of clients of financial institutions," according to an excerpt from a report by the Royal Bank of Canada (RBC).[5]

According to a 2022 Report on the Study of Leaks of Restricted Access Information:

> Almost weekly in the first half of the year, information was published about major leaks from Russian companies and government agencies, including: Russian Railways, the Pobeda airline, the telecommunications companies Rostelecom and VimpelCom, the Ykt.ru information portal, the services of Mir Tesen services, Fotostrana.ru and Text.ru, entertainment resource Pikabu, delivery services Yandex.Food, Delivery Club and 2 Berega, Skolkovo School of Management, educational portal GeekBrains.[6]

Even based on these examples, it is reasonable to conclude that the legitimate expectations of people who entrust information about themselves to the owners of large sites in the process of obtaining entertainment content or Internet services are either not realized or are not sufficiently realized. However, the fact that the protections in place are not as effective as they could be does not indicate that we need new legislation: existing civil law norms (and, in part, some public law norms) make it possible to provide more effective protection of the privacy of people in the digital environment. In the next section, we will consider possible options for interpreting the norms of civil law in order to provide a more serious and thorough protection of the rights of Internet users.

---

[5] Число баз данных банковских клиентов на продажу в даркнете упало вдвое // РБК. 21 декабря 2021 г. [*The number of bank customer databases for sale on the dark web has halved*, RBC, 21 December 2021] (Jan. 15, 2023), available at https://www.rbc.ru/finances/21/12/2021/61c04ef59a79476d4782d2b9.

[6] Report on the Study of Leaks of Restricted Access Information in the First Half of 2022, Expert and Analytical Center InfoWatch (2022); *see* Expert and Analytical Center InfoWatch 2022.

3. Protection of Personal Data

In both public and private law, the instruments for protecting privacy are (a) the institution that receives and holds personal data and (b) the rules on the protection of medical, legal and banking secrecy.

The Russian legislation on the protection of personal data proceeds from the fact that, as a general rule, any action for the processing and storage of personal data requires the consent of the person to whom the personal data relates (Art. 6 of the Law on Personal Data[7]). In this regard, the Russian legislator stands in solidarity with the legislators of the other BRICS countries.

China has specifically adopted laws to protect the personal data of its people, including the Personal Information Protection Law (PIPL), which came into force on 1 November 2021 and the Data Security Law (Data Security Law), which came into force on 1 September 2021. With 1.01 billion Internet users in China, the largest Internet community in the world, the PIPL has the potential to have a significant impact on the protection of personal data. Article 3 of the PIPL provides for the operation of the rules on the processing of personal data not only in the territory of the state, but also in the case when the consumer is located outside of China and the provision of goods or services to individuals is supposed to take place within the borders of China.

In India, a personal data protection bill was submitted by the government to parliament, but the bill was withdrawn for revision in 2022.

In Brazil, the General Data Protection Law was passed in 2019. The body of academic literature has already noted a feature of China's approach to the protection of personal data, which consists in the fact that the theory of identification is used, and personal information is understood as everything that can directly or indirectly identify a person.[8] The processing of personal data requires the consent of the owner of the personal data (Art. 4 PIPL).

Let us turn our attention to some very successful rules of the new Chinese law (PIPL). Firstly, the legislator emphasizes that the forms of consent and standard contracts providing for the processing of personal data must be understandable to people (Art. 17 PIPL). This requirement deserves support, given that many sites frequently publish standard contracts that are so long that the average user is unlikely to finish reading them.

In addition, it is possible to take note of a beneficial rule regarding the need for an agreement between the persons responsible for processing personal data. According

---

[7] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954 [Federal Law No. 152-FZ of 27 July 2006. On Personal Data, Legislation Bulletin of the Russian Federation, 2006, No. 31 (part 1), Art. 3451].

[8] Ts. Shaoxue, *Administrative and Legal Protection of Personal Data in China: Problems and Solutions*, 12 Admin. L. & Proc. 64 (2020).

to Article 20 of the PIPL, if two or more subjects of professional activity jointly decide on the methods of processing or storing personal data, these persons must determine by mutual agreement the rights and obligations of each, after which they are then jointly and severally liable to the person whose personal data is processed or stored. A person may address the prohibition of further use of personal data to all these subjects, as well as to one of them. This norm seems reasonable due to the fact that multiple subjects can be allowed access to the personal data of a person when carrying out a wide range of activities. With regard to Russian law, the joint and several liability of persons who caused damage during the joint processing or storage of personal data can be justified by applying Article 1080 of the Civil Code.

The Russian legislator supplemented the Civil Code with a norm designed to regulate the relationships among the parties when exchanging information. An agreement by virtue of which the contractor agrees to take certain actions in order to provide certain information to the customer (a contract for the provision of information services) may provide for the obligation of one or both parties not to take certain actions for a predetermined period of time, as a result of which information may be disclosed to a third person (Art. 783.1 of the Civil Code). According to research that has been conducted, relations related to data analytics can be formalized by certain kinds of agreements under which one party transfers a specific set of information to the other party, and the other party, on a reimbursable basis, processes and analyzes such information using various algorithms and then provides a specialized report containing the results of such analytics. In particular, such a model can analyze the data contained in social networks in order to determine consumer sentiment regarding a recently released product. It is important that the person or persons collecting information do not violate the prohibitions established by the law on the protection of personal data.

4. Features of the Protection of Medical Secrets and Other Types of Secrets in the Era of Digitalization

In order to emphasize the particular value of some information related to a person or activity, as well as to emphasize the obligation of those admitted to this information to keep it confidential, the legislation uses the concept of "secret." Examples of such information include, for example, banking secrecy and medical secrecy.

The secrecy of medical information originates in a special relationship between the patient and the doctor that is based on trust.[9] The doctor and medical organizations are obliged to maintain medical secrecy since, on the one hand, a patient's concealment

[9] Erwin Deutsch & Andreas Spickhoff, *Medizinrecht: Arztrecht, Arzneimittelrecht, Medizinprodukterecht, und Transfusionsrecht* 602 (2014).

of certain information may be detrimental to the patient's health and life and possibly the health of others, and on the other hand, a patient may choose to keep silent about potentially compromising information if he or she is not sure that the doctor will uphold confidentiality. The same trusting relationship between a person and a service provider underlies other forms of secrets, including banking secrecy and notarial secrecy. Since today almost all patient-related information is held in a digitized form, the question arises as to whether a medical institution is responsible if a third party illegally obtains information regarding material constituting a medical secret and stored in a digitized form by a medical organization. A similar question arises in relation to other types of secrets. Is a notary responsible if a third party, using technical knowledge, illegally gains access to digitized information constituting a notarial secret? Is a bank responsible in the case of illegal access to information constituting bank secrecy? In relationships between an organization and a person, the person represents the weaker party, whereas the commercial organization (and occasionally a non-profit organization) is the economically and organizationally stronger party. As a result, it is reasonable for there to be some degree of paternalism in the relationship that exists between the person and the owner of the site.

In addition, a person who entrusts personal information to a commercial or non-profit organization or the owner of the website does not have the opportunity to check how reliable the programs that protect the site from hacking are or how qualified the employees of the organization that owns the site are. As a result, a relationship that is based on trust will be impossible if the patient, consumer, or any other person acting in a different social role cannot expect the most stringent and reliable measures to protect their personal information from the person who accumulates such information constituting a secret.

In this regard, it is unreasonable to require the site owner to take simply the customary measures to protect information constituting a medical or other secret. It is advisable to assign the risks associated with illegal access by third parties to information consisting of banking secrets, medical secrets and other types of secrets to a person who, by virtue of his entrepreneurial or other professional activities, collects or stores that information in digitized form.

As a result, the owner of a website, or any other person, who, by virtue of his or her professional activity, collects or stores information constituting medical, banking or other secrets is responsible for the disclosure of that information and for any illegal access to that information by a third party, regardless of fault.

The legislation of the BRICS countries does not contain detailed rules on imposing the risks of unauthorized access by third parties to information that is stored in digitized form by a subject of professional activity. At the same time, the general rules that state that the subject of professional activity having access to personal information must ensure the security of this information, allow us to draw a conclusion about liability on the basis of the risk involved.

One such provision can be found, for example, in Article 111 of the Civil Code of China, which states:

> A natural person's personal information is protected by law. Any organization or individual that needs to access other's personal information must do so in accordance with law and guarantee the safety of such information, and may not illegally collect, use, process, or transmit other's personal information, or illegally trade, provide, or publicize such information [Article 111 Civil Code of the People's Republic of China].[10]

In Russian law, a similar general standard is established by the norms establishing the concepts of medical secrecy and banking secrecy, as well as by Article 24 of the Law on Personal Data.

The doctrine recognizes that liability for damage caused by actions that create an increased risk of harm to others is permissible in both public and private interests. First, liability without fault (known as "strict liability" in English-language sources) encourages the person engaging in a potentially harmful activity to take the utmost precautions. Secondly, strict liability provides greater protection for the victim than liability based on guilt.

Responsibility established on the basis of risk (strict liability) for a person who, due to entrepreneurial or professional activities, stores or is responsible for actions related to one or more types of secrets protected by law, can be deduced from a systematic interpretation of the norms of paragraph 3 of Article 401 of the Civil Code and Article 1100 of the Civil Code.

At the same time, the negligence or even the intent of the person to whom the information relates should also not be underestimated. Consider a scenario in which a bank or a medical organization was provided with information about a person, or a person published information about his or her diagnosis and treatment on social networks and later deleted it. Proven gross negligence reduces the amount of damages to be compensated; in other words, if intent is proven to disclose information constituting a medical, banking or other secret, a claim for compensation for damage caused by disclosure may be denied.

---

[10] Civil Code of the People's Republic of China, adopted at the Third Session of the Thirteenth National People's Congress on 28 May 2020 (Jan. 15, 2023), available at http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf.

5. Forms and Methods of Protecting Privacy

5.1. Self-Defense of Personal Non-property Rights

Self-defense measures play an important role in the protection of intangible personal benefits. In the literature, self-defense of civil rights is defined as the actions of people and organizations to protect civil rights and legally protected interests, which are performed by them independently, without seeking help from the state and other competent authorities.[11] Self-defense measures include both factual and legal measures.[12]

In the era of digitalization, some of these measures of an actual nature will likely include certain site settings, requirements for posting on the site, registration on the site and so forth.

For example, the site owner may allow comments and reviews only from registered users, and may also require the registration of a real name and surname as well as the submission of documentation proving the identity of the user as prerequisites for registration. This will serve as a sort of self-defense to prevent anonymous users from spreading information determining honor, dignity and business reputation. As examples of typical situations, we can cite the narratives of two different cases considered by the Supreme Court of the Russian Federation.

In the first case, a surgeon demanded that negative reviews written about him be removed from the website of a medical organization. The case was sent for a new trial since the courts could not determine what the attitude of patients were toward the process of conducting surgical operations and their outcomes, whether these events actually took place or not, whether it was their evaluative opinion or a statement of facts, and in the event that they were statements of facts, then whether they were relevant or not corresponding to reality (Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 26 April 2022 No. 5-KG22-28-K2). It was important that the reviewers' identities not be revealed.

In another case (Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 25 May 2021 5-KG21-32-K2, 2-6217/2019), it could not even be established whether the surgeon in question had actually performed any surgical procedures. The case was also sent for further consideration.

Based on the results of the resolution of these disputes, it is clear that site settings that allow only registered users to leave reviews would prevent anonymous reviews (or

---

[11] Igor A. Aksenov, *The Practice of Applying Legislation on the Protection of the Rights and Legitimate Interests of Individuals in the Implementation of Activities for the Repayment of Overdue Debts: Trends and Results*, 4 Bull. Enforcement Proc. 64 (2017).

[12] Andrei A. Gromov, *Commentary to Article 14 of the Civil Code of the Russian Federation*, in Artem G. Karapetov (ed.), The Main Provisions of Civil Law: Commentary to Articles 1–16.1 of the Civil Code of the Russian Federation 1469 (2020).

at least reduce the risk of such anonymous reviews) and make it easier to verify whether the doctors actually provided medical care to the persons who left reviews. The reviews would also be more valuable in terms of their relevance in such a situation.

5.2. Compensation for Moral Damage as a Way to Protect the Right to Privacy

For all of the importance of self-defense, the jurisdictional form of protection is more visible to both the right holder and the infringer. In the event that the disclosure of information constituting banking, medical or other secrets causes property damage, the person has the right to demand compensation for the damage caused according to the provisions of Article 15 of the Civil Code.

If, under the circumstances of the case, such a method of protection as a requirement to restore the situation that existed before the violation of the right appears acceptable (for example, changing the information previously entered by the Credit Bureau in the credit history of a person, due to the fact that an unidentified person, using personal information, concluded a contract on behalf of that person), this requirement can also be used. Both the claim for damages and the claim for the restoration of the situation that existed before the violation of the right are claims of a property nature (even if the claim for the restoration of the situation that existed before the violation of the right is not subject to monetary value). In the event that a person incurs no property damage but only moral and physical suffering, the most acceptable method of protection is a claim for compensation for moral damage.

Compensation for moral damage is a central part of the system of methods that are used to protect people's right to privacy.

> Compensation for non-pecuniary damage is a legal instrument that gives the necessary completeness to the system of ensuring the security of intangible goods. Even the removal of illegally disseminated information or its refutation will not help a citizen to forget the moral suffering suffered. The experience of experiencing negative emotions is irreversible. Therefore, legal protection against the distortion of a citizen's public assessment and from a negative intrusion into the formation of his self-esteem will not be complete without monetary compensation for the moral suffering that inevitably arises from defamation.[13]

Moral damage is defined as compensation for moral suffering as well as responsibility for moral and physical suffering. It should be noted that the amount of compensation for moral damage depends on the circumstances of the case, including the degree of moral and physical suffering, the duration of the violation and the degree of guilt of the offender.

---

[13] Natalia N. Parygina, *Compensation for Moral Damage in Defamation against a Citizen*, 10 Judge 24 (2018).

The problem with Russian judicial practice is that the amount of compensation awarded for moral damage is often insignificant. It is well known that the compensations exacted by the Russian courts are typically modest, especially when there is no evidence of substantial physical harm, but only moral suffering.

The issue of determining the appropriate amount of compensation has been discussed in the practices of the European Court of Human Rights.

> The task of calculating the amount of compensation for non-pecuniary damage is complex. It is especially difficult in a case whose subject is personal suffering, physical or moral. There is no standard to measure pain, physical inconvenience, mental suffering and anguish in monetary terms (decision of 18 March 2010 in the case *Maksimov v. Russian Federation* (complaint no. 43233/02)).[14]

One possible explanation for the insignificance of compensation in the event of a violation of the right to privacy may be that the amount of the alleged compensation is compared with the compensation already awarded in connection with the injury. Therefore, we can agree that it is necessary to distinguish between moral damage in the strict sense of the word, which occurs when a person's non-property rights are violated, such as the right to a name, image, privacy and the moral (non-property) damage that a person may suffer from an infringement on his life and health.[15]

5.3. Possibility of Changing the Protection Method for More Complete Protection

The amount of compensation for non-pecuniary damage should be determined taking into account the personality of the offender. However, the fact is that the amount of compensation is frequently determined without taking into account the economic inequality that exists between those who did not provide proper confidentiality and those who suffered as a result of this lack of confidentiality. In most cases, the amount of compensation will be calculated as if the tortfeasor and the victim were in an equal position and an equal situation. This is a differentiated approach in which the amount of compensation varies depending on the degree and nature of suffering as well as the duration of the offense. However, the identity of the offender is not taken into account. At the same time, neither the current legislation nor the clarifications of the Plenum of the Supreme Court of the Russian Federation prohibit taking into account the economic inequality that exists between the tortfeasor and the victim in order to determine the amount of compensation. This characteristic could be taken into account as "other circumstances." The list of

---

[14] ECHR Ruling of 18 March 2010 in the case of *Maksimov v. the Russian Federation* (complaint no. 43233/02), 8 Bulletin of the European Court of Human Rights (2010).

[15] Alexandra M. Lobacheva, *Determination of the Amount of Compensation for Moral Damage in Connection with Encroachments on Human Life and Health in France*, 3 Bull. Econ. Just. RF 116 (2020).

circumstances that the court may take into account when determining the amount of compensation in accordance with Article 151 of the Civil Code of the Russian Federation is long.

It is therefore reasonable to assume that the economic inequality between the tortfeasor and the victim must be taken into account. This will prevent subsequent violations and implement the preventive function of civil liability.

The concept of "punitive damages" in the English-language doctrine may serve as a useful guideline in determining the appropriate level of such liability. Punitive damages is an amount of money awarded to the plaintiff in excess of the damage caused to him or her and serves as a punishment against the defendant for especially outrageous behavior.[16] Punitive damages are typically issued when the severity of the offense and the economic inequality between the tortfeasor and the victim induce the court not only to compensate the victim for the damage caused but also to punish the tortfeasor exponentially.

Punitive damages are a well-known theoretical concept in both Russian and foreign civil law. However, attitudes towards this concept vary from country to country. In the US doctrine, the attitude towards the concept of punitive damages is very positive. Punitive damages are used in disputes involving commercial organizations (including cigarette manufacturers, energy supply organizations) and consumers, as well as medical organizations and patients. UK jurisprudence and doctrine have taken a slightly more cautious approach to claims for punitive damages. It is proposed to limit the circumstances under which punitive damages can be recovered.[17] In the French doctrine, the attitude towards punitive damages is even more wary.[18]

One advantage of the institution of punitive damages is the more serious protection provided to the victim. Of course, this has to do with the amount of compensation. In addition, the possibility of receiving exemplary increased compensation motivates the lawyer to represent the interests of the victim on the terms of the success fee. Thus, claims for which (without the possibility of recovering punitive damages) the plaintiff could not find a representative turn out to be more promising, and at the same time, the interests of the victim are protected.

The disadvantages of the institution of punitive damages are that, firstly, the most enterprising plaintiff receives protection as if for himself and other victims, while other

---

16 Sergey L. Budylin, *Punitive Damages. Now in Russia?*, 4 Bull. Civ. L. 19 (2013).

17 *See* Henry N. Butler & Jason S. Johnston, *Reforming State Consumer Protection Liability: An Economic Approach*, (2010)1 Colum. Bus. L. Rev. 1 (2010).

18 François-Xavier Licari, *Prendre Les Punitive Damages Au Sérieux: Propos Critiques Sur un Refus d'Accorder l'Exequatur À une Décison Californienne Ayant Alloué des Dommages-Intérêts Punitifs* [*Taking Punitive Damages Seriously: Why a French Court Did Not Recognize An American Decision Awarding Punitive Damages and Why it Should Have*], 137 J. du Droit Int'l 1230 (2010) (Jan. 15, 2023), available at https://ssrn.com/abstract=1664350.

plaintiffs who have not filed a claim do not receive protection. Another drawback of the institution of punitive damages is that the possibility of paying compensation for punitive damages is taken into account by commercial organizations when determining the cost of providing services; in order to redistribute the risk of liability, a liability insurance contract is concluded, which is also taken into account when determining prices under contracts with consumers. Thus, it can be assumed that the possibility of filing a claim for punitive damages may entail a change in the terms of obligations not in favor of the person.

Should the model of punitive damages be used to improve the system of compensation for non-pecuniary damage? In other words, should the amount of compensation for non-pecuniary damage be determined in such a way as to not only compensate for the suffering of the victim but also punish the offender? The doctrine of China, for example, discusses the application of the institution of punitive damages in relations between the tortfeasor and the victim.[19] We do not deny that the institution of punitive damages has its drawbacks; however, the economic disparity between the offender and the victim must be reflected in determining the amount of compensation. In the event that an organization receives and processes personal data, including information constituting medical, banking or other secrets, the organization must make every possible effort to protect that information in a way that ensures its confidentiality.

People have the right to expect that a commercial organization that accumulates, collects, stores or processes information relating to them while carrying out its income-generating activities will make every effort to protect this information. In order to motivate a commercial organization to exert the maximum effort, the risk of paying the customary minimal compensation for non-pecuniary damage is not enough; instead, the amount of compensation should be increased, taking into account the preventive function of civil liability. In this regard, the method of seeking compensation will be based on the model of punitive damages.

Conclusion

In the era of digitalization, people, as a rule, rightly expect that the personal data entrusted to one site will not then be used without restriction by a dozen other websites. In order to ensure the realization of these legitimate expectations, one should treat the obligations of a professional entity (commercial organization, individual entrepreneur or any other person carrying out professional activities) that involve the processing of personal data of a person or receiving information constituting a secret with the same level of strictness as the obligations of a commercial organizations to fulfill contractual obligations to consumers. The

[19] Bu Yuanshi (ed.), *Chinese Civil Law* 164 (2013).

responsibility of the professional for the disclosure of information should be carried out regardless of fault, in accordance with the rules of strict liability. In addition, in the event that a person suffers moral damage as opposed to property damage, the amount of compensation should be determined taking into account the economic inequality between the tortfeasor and the victim and taking into account the preventive function of civil liability. In this case, the claim for compensation for non-pecuniary damage acquires a certain similarity to the claim for punitive damages, since the victim may receive compensation in an amount slightly larger than the suffering the victim has endured. This excess appears to be justified due to the economic and organizational inequality of the subjects of legal relations. People who share personal information with a commercial organization are unable to verify the reliability of the programs and tools that are used by the organization to protect their data. Therefore, the organization must be motivated to take the best possible precautions to protect the privacy of people's personal data, even if these best practices are relatively expensive.

References

Aksenov I.A. *The Practice of Applying Legislation on the Protection of the Rights and Legitimate Interests of Individuals in the Implementation of Activities for the Repayment of Overdue Debts: Trends and Results*, 4 Bulletin of Enforcement Proceedings 64 (2017).

Bu Y. (ed.). *Chinese Civil Law* (2013).

Budylin S.L. *Punitive Damages. Now in Russia?*, 4 Bulletin of Civil Law 19 (2013).

Butler H.N. & Johnston J.S. *Reforming State Consumer Protection Liability: An Economic Approach*, 2010(1) Columbia Business Law Review 1 (2010). https://doi.org/10.7916/cblr.v2010i1.2917

Deutsch E. & Spickhoff A. *Medizinrecht: Arztrecht, Arzneimittelrecht, Medizinprodukterecht, und Transfusionsrecht* (2014). https://doi.org/10.1007/978-3-642-38149-2

Lobacheva A.M. *Determination of the Amount of Compensation for Moral Damage in Connection with Encroachments on Human Life and Health in France*, 3 Bulletin of Economic Justice of the Russian Federation 116 (2020).

Ostanina E.A. *Is It Allowed to Quote Photos in Austria? Translation of the Decision of the Supreme Court of Austria Dated 26 Sept. 2017 No. 4 Ob 81/17S and Commentary to It*, 10 Bulletin of Economic Justice of the Russian Federation 49 (2018).

Parygina N.N. *Compensation for Moral Damage in Defamation against a Citizen*, 10 Judge 24 (2018).

Presnyakov M.V. *The Problem of Substantive Certainty and Constitutional Protection of Social Rights*, 6 Constitutional and Municipal Law 16 (2020).

Information about the authors

Elena Ostanina (Chelyabinsk, Russia) – Head, Department of Civil Law and Procedure, Chelyabinsk State University (129 Bratiev Kashirinykh St., Chelyabinsk, 454001, Russia; e-mail: elenaostanina@mail.ru).

Elena Titova (Chelyabinsk, Russia) – Director, Institute of Law, South Ural State University (National Research University) (47a Elektrostalskaya St., Chelyabinsk, 454038, Russia; e-mail: titovaev@susu.ru).

DIGITAL TECHNOLOGIES AND LABOUR RELATIONS: LEGAL REGULATION IN RUSSIA AND CHINA

ELENA OFMAN,

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

MIKHAIL SAGANDYKOV,

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

https://doi.org/10.21684/2412-2343-2023-10-1-126-146

The widespread use of digital technologies in the field of labour relations raises the issue of examining the readiness and capability of the legislation in Russia and China to adequately regulate labour in modern workplace conditions while respecting the balance of interests and the rights of employees, employers and the state. This article draws a number of conclusions, one of which is that currently in the Russian Federation, the legal regulation of the use of digital technologies in the field of labour is haphazard, contradictory and not designed for the long term. Despite a number of significant scientific studies conducted in this area and the serious commitment of the People's Republic of China to the issues of informatization, the legal regulation of the digitalization of labour relations lags behind technological progress. A number of issues in urgent need of legal regulation remain outside the legal field (robotization and algorithmization in the field of labour; protection of personal data of job applicants; the problem of unemployment in the application of artificial intelligence in the labour process). It appears that today there is an urgent need for the federal authorities of the Russian Federation to adopt a strategy for the transformation of labour relations in the application of digital (information) technologies as well as a need to develop a concept of robotization and algorithmization of the labour process. Furthermore, when creating these documents and adjusting the current regulatory framework, the Russian legislator should take into account the experience of international and foreign regulation of labour relations in the field of digitalization of labour relations.

Keywords: labour relations; digital technologies; control over employees; employees of Internet platforms; remote workers; private life of employees.

Recommended citation: Elena Ofman & Mikhail Sagandykov, *Digital Technologies and Labour Relations: Legal Regulation in Russia and China*, 10(1) BRICS Law Journal 126–146 (2023).

Table of Contents

Introduction

Modern society today faces a difficult task: it needs to adapt to the almost universal introduction of digital technologies in the many spheres of daily life. This also applies to the field of labour relations. However,

> due to fundamental reasons, the law does not have the necessary flexibility for the rapid introduction of digital technologies into its sphere, which allows us to talk about such a feature of the influence of digital technologies in this branch of law as the heterogeneity of the pace of bifurcation of legal norms.[1]

We can say that today we are witnessing the proliferation of artificial intelligence in various spheres of public life.[2]

Of course, scientific and technological progress, robotization and automation are transforming the workplace. These changes are far-reaching and multifaceted. The introduction of new (digital) technologies, the algorithmization of processes, the use of big data and automated decision-making using artificial intelligence can have a significant impact on people's lives, especially on those who are already working and are already immersed in a situation where the distribution of legal and economic power is prone to disruptions or the specified power is unstable.[3]

---

[1] Механизмы и модели регулирования цифровых технологий: монография / под общ. ред. А.В. Минбалеева [Aleksey V. Minbaleev (ed.), *Digital Regulatory Mechanisms and Models: A Monograph*] 26 (2020).

[2] Anton Korinek, *Labor in the Age of Automation and Artificial Intelligence*, Economists for Inclusive Prosperity (January 2019) (Nov. 10, 2022) (Nov. 10, 2022), available at https://econfip.org/wp-content/uploads/2019/02/6.Labor-in-the-Age-of-Automation-and-Artificial-Intelligence.pdf.

[3] The report of the International Labour Organization "The Future of Work We Want: A Global Dialogue" on 6–7 April 2017 (Nov. 10, 2022), available at https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_570282.pdf.

At the same time, in Russia as in China, the development of digital technologies lags behind their legal regulation.[4]

In fact, since the beginning of the 21st century, we are faced with the emergence of a gap in time between the emergence of new technologies, the possibility of their use in everyday life and the availability of appropriate legal regulation.[5]

1. Theoretical and Regulatory Framework for Introducing Digital Technologies in Labour Relations

The conceptual apparatus in the field of digitalization of relations is in its early stages of development.

By information technologies, the Federal Law "On Information, Information Technologies and Information Protection"[6] refers to processes, methods of searching, collecting, storing, processing, providing and distributing information, as well as ways of implementing such processes and methods into practice (Art. 2).

Algorithms using artificial intelligence or machine learning have achieved superhuman characteristics in a wide range of economically valuable tasks.[7]

Automation should be aimed not only at replacing manual labour with mechanical labour, but also at a qualitative change in the structure of production and a significant increase in labour productivity. Otherwise, there will be no demand for labour in the other fields, which will certainly affect the social standing of the person who performs the labour.[8] In essence, artificial intelligence should contribute to the restructuring of production.[9]

The Russian Federation has adopted a number of strategic (programmatic) documents on the legal regulation of the use of digital technologies.

---

[4] *Трощинский П.В., Молотников А.Е.* Особенности нормативно-правового регулирования цифровой экономики и цифровых технологий в Китае // Правоведение. 2019. № 63(2). С. 310 [Pavel V. Troshchinskiy & Alexander E. Molotnikov, *Features of Legal Regulation of the Digital Economy and Digital Technologies in China*, 63(2) Pravovedenie 309, 310 (2019)].

[5] Minbaleev (ed.) 2020, at 45.

[6] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. 29 июля. № 165 [Federal Law No. 149-FZ of 27 July 2006. On Information, Information Technologies and Information Protection, Rossiyskaya Gazeta, 29 July 2006, No. 165].

[7] Mechael Webb, *The Impact of Artificial Intelligence on the Labor Market*, SSRN Electronic J. (2020) (Nov. 10, 2022), available at https://ssrn.com/abstract=3482150.

[8] *Daron Acemoglu & Pascual Restrepo,* The Wrong Kind of AI? Artificial Intelligence and the Future of Labor Demand*, w25682 NBER Working Paper (2019) (Nov. 10, 2022), available at https://ssrn.com/abstract=3359482.*

[9] Eric Brynjolfsson et al., *What Can Machines Learn and What Does it Mean for Occupations and the Economy?*, 108 Am. Econ. Ass'n Papers & Proc. 43–47 (2018).

The strategy for the development of the information society in the Russian Federation for 2017–2030[10] states that one of the main tasks of using information and communication technologies for the development of the social sphere is to stimulate Russian organizations in order to provide employees with opportunities for remote employment and the creation of information and communication technology-based management and monitoring systems in all spheres of public life. In the sphere of interaction between the state and business, the following main tasks are established in relation to the labour sphere: the promotion of electronic document management and the implementation in electronic form of the identification and authentication of participants in legal relations.

It is important to note that when formulating and ensuring these strategies of national interest, there is no mention of ensuring the protection of the rights of employees and employers (businesses) from the impact of digital (information) technologies on labour relations.

Of particular interest to this study is the "National Action Plan for the Restoration of Employment and Incomes of the Population, Economic Growth and Long-Term Structural Changes in the Economy" of 23 September 2020.[11] The labour market in the digital era is characterized by the regulatory and legal support for remote work, including a combination of remote work and on-site work, improved regulations for part-time employment and self-employment, and the introduction of electronic personnel document management.

In addition to the above, it is planned, in particular, to introduce a single digital platform for education, advanced training and employment support in order to increase labour productivity and labour market flexibility based on integrating interaction with educational institutions, employment centers, employers, citizens and other labour market participants.

As part of the implementation of the national program "Digital Economy of the Russian Federation," the federal project "Regulatory Regulation of the Digital Environment" was adopted,[12] according to which it is planned to implement a number of

---

[10] Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901 [Presidential Decree No. 203 of 9 May 2017. On the Strategy for the Development of Information Society in the Russian Federation for 2017–2030, Legislation Bulletin of the Russian Federation, 2008, No. 20, Art. 2901].

[11] «Общенациональный план действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике», одобрен Правительством Российской Федерации 23 сентября 2020 г., протокол № 36, раздел VII [A Nationwide Action Plan for Employment and Income Recovery, Economic Growth and Long-Term Structural Change in the Economy, approved by the Government of the Russian Federation, Minutes No. 36 of 23 September 2020, Section VII] (Nov. 10, 2022), available at https://pravdaosro.ru/.

[12] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7) // СПС «Консуль-

measures through the adoption of federal laws. These measures relate to electronic document management, personal data protection and the creation of a platform for interaction in labour relations. Much of what has been said has already been done.

It should be noted that despite the very high level of digitalization in the People's Republic of China, the legal regulation of this phenomenon has remained insignificant and cautious for a long time.[13]

China's legislation in the field of regulation of digital and information technologies is focused on the following main vectors: ensuring the security of users and the state in cyberspace, as well as in the information technology industry; centralized regulation of the digitalization of public administration; building global digital platforms and developing online systems in the fields of economics, finance, labour market, justice and others.

In China, as in Russia, a number of policy documents have been adopted in the field of the development of information and digital technologies.[14]

In 2016, the "National Strategy for Informatization and Development" was adopted in order to implement the information policy of the People's Republic of China. According to this strategy as well as a number of other documents, China should become a leading country in advanced technologies and software by the year 2025. Furthermore, the country aims to take the lead in the production of high-tech products and the creation of software by the middle of the twenty-first century. These concepts are based on previously adopted strategic initiatives such as "Internet Plus" and "Made in China – 2025."[15]

An important direction in the development of digital innovation is the creation of global online platforms.[16] At the same time, the legal regulation of their activities has certain specifics in China. If in other countries this kind of regulation is largely

---

тантПлюс» [Passport of the National Project, National Programme "Digital Economy of the Russian Federation" (approved by the Presidium of the Presidential Council for Strategic Development and National Projects, Minutes No. 7 of 6 July 2019), SPS "ConsultantPlus"] (Nov. 10, 2022), available at http://www.consultant.ru/online/.

13 Troshchinskiy & Molotnikov 2019, at 317.

14 *Томайчук Л.В.* Цифровизация экономики Китая: риски и возможности для общества // Евразийская интеграция: экономика, право, политика. 2019. № 3(29). С. 33 [Lilia V. Tomaichuk, *Digitalization of China's Economy: Risks and Opportunities for Society*, 3(29) Eurasian Integration: Econ., L., Pol. 31, 33 (2019)].

15 *Понька Т.И., Рамич М.С., Юйяо У.* Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. № 20(2). С. 385. [Tatyana I. Ponka et al., *Information Policy and Information Security of PRC: Development, Approaches and Implementation*, 20(2) Vestnik RUDN, Int'l Rel. 382, 385 (2020)].

16 Dun Li et al., *How Do Platforms Improve Social Capital within Sharing Economy-Based Service Triads: An Information Processing Perspective*, Production Plan. & Control (2022) (Nov. 10, 2022), available at https://doi.org/10.1080/09537287.2022.2101959.

built along the path of compliance with antimonopoly legislation, then in China, from this point of view, global online platforms have relative freedom as well as some kind of protection from antimonopoly interference.[17]

It should be noted that in China, as in Russia, much attention is paid to the creation of state-regulated online platforms, both in the field of economics and public administration, such as the online justice platform.[18]

It should also be noted that in recent years, a great deal of effort has been expended in Russia to create online platforms related to providing citizens and entrepreneurs with a wide range of services. After conducting an experiment on the adoption of technologies for electronic (paperless) registration of labour relations[19] in 2021, amendments and additions were made to the Labour Code of the Russian Federation,[20] legalizing these rules.[21]

At the same time, the logic underlying the development of Russian legislation in this area points to the nationalization of electronic personnel document management, since the most effective way of facilitating remote interaction between an employee and an employer is a single digital platform in the field of employment and labour relations known as "Work in Russia." As a result, the state has the ability to control the details of employment contracts and influence the way labour relations are registered.

There is no such platform in China yet, but the idea is being considered.[22] This will be further discussed in more detail.

It appears that these legislative decisions will not have an entirely positive impact on the effective regulation of labour relations, since the issues relating to regulating the interaction between an employee and an employer remain outside the scope of legal regulation. It is the mechanism of exercising labour rights and fulfilling labour

---

17 Yang Cao, *Regulating Digital Platforms in China: Current Practice and Future Developments*, 11(3–4) J. Eur. Comp. L. Pract. 173 (2020).

18 Yulia Kharitonova & Larisa Sannikova, *Digital Platforms in China and Europe: Legal Challenges*, 8(3) BRICS L.J. 133 (2021).

19 Федеральный закон от 24 апреля 2020 г. № 122-ФЗ «О проведении эксперимента по использованию электронных документов, связанных с работой» // Российская газета. 2020. 28 апреля. № 92 [Federal Law No. 122-FZ of 24 April 2020. On the Experiment on the Use of Electronic Work Related Documents, Rossiyskaya Gazeta, 28 April 2020, No. 92].

20 Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (ч. 1). Ст. 3 [Labour Code of the Russian Federation No. 197-FZ of 30 December 2001, Legislation Bulletin of the Russian Federation, 2002, No. 1(3), Art. 3].

21 Федеральный закон от 22 ноября 2021 г. № 377-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации» // Российская газета. 2021. 24 ноября. № 266 [Federal Law No. 377-FZ of 22 November 2021. On Amendments to the Labour Code of the Russian Federation, Rossiyskaya Gazeta, 24 November 2021, No. 266].

22 Liu Dun & Geng Yuan, *The Model of the State Digital Platform on Labor Contracts in China,* 3(1) Digital L.J. 20–31 (2022).

duties with the help of digital technologies and in the field of digital space that should be the subject of attention for the legislator. Electronic personnel document management and digital signatures in labour relations are, (relatively speaking), the external face of communication between an employee and an employer, the so-called "technical aspect of the impact of information technology on labour relations,"[23] and the core of this relationship has remained outside the purview of legal regulation.

There is mounting evidence that employers are attempting to avoid or circumvent the fulfilment of the obligations established for them by labour legislation while employing strategies to attract employees to work for minimal wages.[24] There have been numerous studies devoted to various aspects of the transformation of labour relations in the context of digitalization. Employment is undergoing not only quantitative but also qualitative changes.[25] The approach to the workplace (work based on an Internet platform) is being modernized, leading to the realization by employees of the right to training, advanced training or retraining, which, in fact, now, in the conditions of globalization, becomes lifelong.[26] Additionally, the concept of 'disciplinary misconduct' is evolving[27] and the interaction between employees and employers are carried out in new ways. Employment contracts are now concluded for the most part as fixed-term agreements, wages are reduced and employer control takes on the features of surveillance. An interesting conclusion reached by the researchers is that there is a high probability that a significant disparity in the remuneration of the "head" and "ordinary" employees causes employees to commit labour violations.[28] According to legal scientists, patriarchy, slavery and racism have once again become markers of

---

[23] *Костян И.А., Куренной А.М., Хныкин Г.В.* Трудовое право и цифровая экономика: сочетаются ли они? // Трудовое право в России и за рубежом. 2017. № 4. С. 10–12 [Irina A. Kostyan et al., *Labor Law and Digital Economy: Do They Match?*, 4 Lab. L. in Russ. & Abroad 10 (2017)]; *Лютов Н.Л.* Адаптация трудового права к развитию цифровых технологий: вызовы и перспективы // Актуальные проблемы российского права. 2019. № 6(103). С. 103 [Nikita L. Lyutov, *Adaptation of Labor Law to the Development of Digital Technologies: Challenges and Prospects*, 6(103) Current Probs. Russian L. 98, 103 (2019)].

[24] Fuxi Wang, *China's Employment Contract Law: Does it Deliver Employment Security?*, 30(2) Econ. & Lab. Rel. Rev. (2019) (Nov. 10, 2022), available at https://journals.sagepub.com/doi/10.1177/1035304619827758.

[25] Lyutov 2019, at 98–107.

[26] *Томашевский К.Л.* Цифровизация и ее влияние на рынок труда и трудовые отношения (теоретический и сравнительно-правовой аспекты) // Вестник Санкт-Петербургского университета. Право. 2020. № 11(2). С. 404, 405 [Kirill L. Tomashevski, *Digitalization and its Impact on the Labour Market and Employment Relations (Theoretical and Comparative Legal Aspects)*, 11(2) Vestnik of Saint Petersburg Univ. L. 404, 405 (2020)].

[27] *Забрамная Е.Ю.* Эволюция понятия «дисциплинарный проступок» в условиях цифровизации экономики // Вопросы трудового права. 2021. № 1. С. 18–25 [Elena Yu. Zabramnaya, *Evolution of the Concept of "Disciplinary Misconduct" in the Context of Digitalisation of the Economy,* 1 Emp. L. Issues 18 (2021)].

[28] Stephen Smulowitz & Juan Almandoz, *Predicting Employee Wrongdoing: The Complementary Effect of CEO Option Pay and the Pay Gap,* 162(3) Organizational Behav. & Hum. Decision Procs 123 (2021).

digital labour.[29] For example, Bingqing Xia, a scientist from China, described modern workers of the digital era as 'working hard' (workers face problems such as inequality and injustice, unequal pay for long working hours and violation of labour protection requirements by employers);[30] and Ping Sun, Julie Yujie Chen and Uma Rani in a joint article demonstrated the trend of deflection of digital platform workers, referring to the work of these workers as "sticky" ("Sticky Labour").[31] Time has shown that the notions of providing digital platform workers with greater flexibility, autonomy and independence in regulating labour issues are utopian; on the contrary, the work of such persons is highly demanding, stressful and hazardous.[32]

The violations committed by employees and employers in the digital environment are becoming more sophisticated and non-standard, challenging the classical understanding of labour law offenses. Let us give a vivid example. An employer used an employee's electronic digital signature to log into the employee's personal account and sign an agreement on the extension of the employment contract by mutual agreement of the parties. However, the employee was able to prove the illegality of this extension: the personal computer from which the agreement was signed was located on the employer's property and the employee objectively could not have performed the action of signing the specified agreement because the employee at the time was at an interview with another employer.[33]

A perfectly reasonable question arises: how to achieve the implementation of the above goals, objectives and interests? Even if we subordinate digital technologies to global human needs rather than profit, there will still remain many social, economic and political problems.[34]

It would appear that the legal transformation in the conditions of digitalization should be regulated by conventional labour law institutions, such as working hours and rest time, remuneration, and control over the behaviour of employees during the

---

[29] Christian Fuchs, *Capitalism, Patriarchy, Slavery and Racism in the Age of Digital Capitalism and Digital Labour,* 44(4–5) Critical Soc. (2018) (Nov. 10, 2022), available at https://doi.org/10.1177/0896920517691108.

[30] Bingqing Xia, *Digital Labour in Chinese Internet Industries*, 12(2) Comm., Capitalism & Critique 668 (2014).

[31] Ping Sun et al., *From Flexible Labour to "Sticky Labour": A Tracking Study of Workers in the Food-Delivery Platform Economy of China*, Work, Emp. & Soc'y (2021) (Nov. 10, 2022), available at https://doi.org/10.1177/09500170211021570.

[32] Eleonore Kofman et al., *China and the Internationalisation of the Sociology of Contemporary Work and Employment,* Work, Emp. & Soc'y (2016) (Nov. 10, 2022), available at https://doi.org/10.1177/0950017021105942.

[33] Определение Седьмого кассационного суда общей юрисдикции от 11 января 2022 г. № 88-1761/2022 (88-2120/2021) [Decision of the Seventh Court of Cassation of General Jurisdiction No. 88-1761/2022 (88-2120/2021) of 11 January 2022].

[34] Michael M. Peters, *Beyond Technological Unemployment: The Future of Work*, 5 Educ. Phil. & Theory 485 (2020) (Nov. 10, 2022), available at https://www.tandfonline.com/doi/full/10.1080/00131857.2019.1608625?scroll=top&needAccess=true.

performance of their work duties. In the absence of legal regulation of these issues, these aspects of employee–employer interaction are modified, but spontaneously, without taking into account the interests of the employee, the weaker party in the legal relationship, which entails an infringement of the employee's rights and exposure to even greater pressure from the employer.

2. Digital Technologies and Classical Labour Relations

Modern information technology and communication systems enable people to work in ways that seemed impossible a few decades ago.

O.V. Chesalina, when considering such a form of employment as work based on an Internet platform (Crowdwork), poses a number of valid questions. "Do the new forms of work contain signs of independent work? And if so, should the norms of labour law and social security law be extended to them?"[35]

However, this new form of employment is also being transformed under unstable and rapidly developing conditions.[36] Scientists like to draw a distinction between solo-crowdworkers (single crowdworkers) and workers employed by "crowd farms."[37] The results of their research have shown that the work experiences and working conditions of solo crowdworkers differ significantly from the working conditions of employees of "crowd farms" (in terms of their motivation, methods of interaction, assigned tasks and the resolution of issues which they are working on).[38]

Definitely, such a form of employment (Crowdwork) has similarities with remote labour. At the same time, it assumes that the customer (employer) does not issue a task to a specific employee, as in remote work, but to an indefinite circle of people.[39]

---

[35] *Чесалина О.В.* Работа на основе интернет-платформ (crowdwork и work on-demand via apps) как вызов трудовому праву и праву социального обеспечения // Трудовое право в России и за рубежом. 2017. № 1. С. 52–55 [Olga V. Chessalina, *Crowdwork and Work on Demand via Apps as a Challenge to Labor and Social Law*, 1 Lab. L. in Russ. & Abroad 52 (2017)].

[36] Michelle Olgun et al., *Croudwork & the Trade Regime: Opportunites and Challenges* (Nov. 10, 2022), available at https://www.researchgate.net/publication/349967459_Crowdwork_and_international_trade_Opportunities_and_challenges#pf25; Kumiko Kawashima, *Service Outsourcing and Labour Mobility in a Digital Age: Transnational Linkages Between Japan and Dalian, China*, 17(4) Global Networks (2017) (Nov. 10, 2022), available at https://www.researchgate.net/publication/312516805_Service_outsourcing_and_labour_mobility_in_a_digital_age_Transnational_linkages_between_Japan_and_Dalian_China.

[37] Yihong Wang et al., *The Changing Landscape of Crowdsourcing in China: From Individual Crowdworkers to Crowdfarms*, CSCW'19: Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing (2019) (Nov. 10, 2022), available at https://doi.org/10.1145/3311957.3359469.

[38] Yihong Wang et al., *Crowdsourcing in China: Exploring the Work Experiences of Solo Crowdworkers and Crowdfarm Workers*, CHI'20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020) (Nov. 10, 2022), available at https://doi.org/10.1145/3313831.3376473.

[39] Chessalina 2017, at 53.

As an example of such a form of employment, one can cite work done using the Uber application. The main feature of working on an Internet-based platform is the absence of any formal documentation of the relationship defining the rights and obligations of the parties, which ultimately can lead to employees being deprived of the ability to protect their labour rights.[40]

Working with digital platforms is one of the most important aspects of the broader trend towards delegating work to individual independent contractors without any obligations on the part of the customer caused by the burden of labour relations.[41]

The reason for this is the peculiarity of the business model of crowdwork platforms combined with the conceptual constraints imposed by traditional ideas about the status of an employee.[42]

Alternative ways of organizing work create disputes over the distinction between "employees" and "independent contractors," and occasionally, the employer (customer) will go to great lengths deliberately to distort the essence of the relationship with the employee.[43] The emergence of the digital economy tends to "accelerate the erosion of traditional ('classical') labour relations."[44] The employer becomes "invisible," appearing to "disappear" while retaining the ability to bring employees to labour and legal responsibility (disciplinary, material).[45]

The law should be aimed at eliminating the opportunities for leading firms to evade their duties and responsibilities to employees. Some rights should apply to independent contractors, for example, freedom from discrimination or the right to safe work under the supervision of a contractor.[46]

At the moment, such guarantees do not apply to them: for instance, Uber refers to its drivers as independent service providers, which does not require the company

---

[40] *Чиканова Л.А., Серегина Л.В.* Правовая защита граждан от безработицы в условиях информационных технологических новаций в сфере труда и занятости // Право. Журнал Высшей школы экономики. 2018. № 3. С. 149–171 [Ludmila A. Chikanova & Larisa V. Seregina, *Legal Protection of Citizens against Unemployment in Conditions of Information Technological Innovations in the Field of Labour and Employment*, 3 L.J. Higher Sch. Econ. 151 (2018)].

[41] Cynthia Estlund, *What Should We Do after Work? Automation and Employment Law*, 2 Yale L.J. 254 (2018) (Nov. 10, 2022), available at https://ssrn.com/abstract=3007972.

[42] Jeremias Prassl & Martin Risak, *Uber, Taskrabbit, & Co: Platforms as Employers? Rethinking the Legal Analysis of Crowdwork*, 37 Comp. Lab. L. & Pol. J. 619 (2015).

[43] Gay Davidov, *The Status of Uber Drivers: A Purposive Approach*, 6 Spanish Lab. L. & Emp. Rel. J. 8 (2017).

[44] Miriam Kullmann, *Flexibilization of Work: Leave it, Love it, Change it*, Festskrift till Ann Numhauser-Henning 405 (2017) (Nov. 10, 2022), available at https://www.researchgate.net/publication/316824962_Flexibilization_of_Work_Leave_It_Love_It_Change_It.

[45] The report of the International Labour Organization "The Future of Work We Want: A Global Dialogue" of 6–7 April 2017 (Nov. 10, 2022), available at https://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_570282.pdf.

[46] Estlund 2018, at 268–70.

to comply with standards regarding working hours and salaries, occupational safety requirements and prohibitions of discrimination. Furthermore, the company does not give its employees the opportunity to use federal guarantees of unionization. It is believed that independent service providers have stronger negotiating capabilities than employees, and hence they do not need such guarantees. This applies to numerous other independent service providers, such as doctors, lawyers and architects. But what if, for example, an Uber driver gets injured while transporting a passenger? Is this entirely the employee's responsibility or should the platform support the employee in some way? It turns out that such employees do not have the freedom of contract inherent in independent contractors, nor do they have the ability to use collective contractual regulation, which is the most important mechanism for protecting the rights of employees.[47]

Given that such employees enjoy a relatively high degree of freedom, it is frequently difficult to identify their relationship as an employment relationship and to provide them with protection by labour legislation.[48]

The answer to the question about the status of the categories of employees (service providers) under consideration should be sought on the basis of an analysis of the concept of labour relations.

Let us start from the understanding of the labour relationship that is given in the Recommendation of the International Labour Organization (ILO) dated 15 June 2006 No. 198 "On Labour Relations."[49] Subparagraph "a" of paragraph 13 of this act defines the key features of an employment relationship: work that is performed under the direction and in the interests of another person; integration into the organizational structure of the enterprise; personal performance of work; coordination of the schedule or period of work; and provision of tools, materials and mechanisms by the party who ordered the work.

In addition, paragraph 12 of the Recommendation states that

> Member States may provide for a clear definition of the conditions used to establish the existence of an employment relationship, for example, such as subordination or dependence.

The above gives reason to believe that an employee's affiliation with his or her employer is one of the main factors determining the status of an employee.

---

47 Elizabeth J. Kennedy, *Employed by an Algorithm: Labor Rights in the On-Demand Economy*, 40 Seattle U.L. Rev. 1011 (2017) (Nov. 10, 2022), available at https://digitalcommons. law.seattleu.edu/cgi/viewcontent.cgi?article=2417&context=sulr.

48 Xie Zengyi, *The Changing Mode of Legal Regulation of Labor Relations in China*, 39(4) Soc. Sci. in China 96, 100 (2018).

49 Рекомендация № 198 Международной организации труда «О трудовом правоотношении» // СПС «КонсультантПлюс» [International Labour Organisation Recommendation No. 198 "On the Employment Relationship," SPS "ConsultantPlus"] (Nov. 10, 2022), available at http://www.consultant.ru/online/.

The relationship between the platform and its employees is long-lasting and strong: the platform fully controls the existence and nature of the relationship. In the case of Uber, for instance, the company inspects the drivers' vehicles as well as verifies their driving rights and insurance coverage. Uber is also in control of restricting its drivers' access to the platform.[50]

There is a hierarchy within Uber, and it is expressed through a rating system and the collection of other information regarding how well drivers perform their duties.[51]

Chinese researchers have highlighted the most important strategies developed by Uber to control the labour process of employees: a system of incentive payments; a system of customer ratings; and flexible work hours.[52]

Furthermore, studies conducted in China have shown that Uber uses a dynamic pricing method to build a system of remuneration for drivers, which significantly affects the quality of services provided, as well as the attraction of drivers during periods of peak demand.[53]

Drivers have complete freedom to choose their hours of work, yet there is an economic dependency. The company dictates the fare and the amount of money that is paid to the driver. The driver's ability to influence profits is practically nonexistent. The only way for the drivers to generate profits is to increase working hours, which is considered by some to be an indication of the absence of effective labour relations.[54]

We do not think so. The system of maintaining the reputation of the driver, which is based on the number of positive ratings, keeps the crowdworker under pressure to work as much as possible in order to achieve and maintain a positive rating.[55]

This is confirmed by judicial practice in the United States and the United Kingdom.

According to E. Kennedy, at least two courts in the United States have already recognized that Uber drivers are employees. And in the United Kingdom, the labour dispute court ruled in 2016 that they are employees and that the company's attempts to present the situation differently are pure fiction and in no way reflect the actual relationship between the parties (*Aslam v. Uber*).[56] In 2021, a final ruling was made on this case.[57]

---

50 Prassl & Risak 2015.

51 Davidov 2017, at 12.

52 Qingjun Wu et al., *Labor Control in the Gig Economy: Evidence from Uber in China*, 61(4) J. Indus. Relation 574 (2019).

53 Feng Xiong, Si Xu & Dongzhu Zheng, *An Investigation of the Uber Driver Reward System in China – An Application of a Dynamic Pricing Model*, 33(1) Tech. Analysis & Strategic Mgmt. 46 (2011).

54 Davidov 2017, at 12–13.

55 Prassl & Risak 2015.

56 Kennedy 2017, at 994–1022.

57 «Удар в самое сердце»: Uber проиграл дело о правах водителей в Великобритании // Forbes.ru ["Punch to the Heart": Uber Loses Driver's Rights Case in the UK, Forbes.ru] (Nov. 10, 2022), available at https://www.forbes.ru/newsroom/biznes/421609-udar-v-samoe-serdce-uber-proigral-delo-o-pravah-voditeley-v-velikobritanii

The above gives reason to conclude that work based on Internet platforms possesses the majority of the features specified in Recommendation No. 198 of the International Labour Organization. At the same time, the peculiarity of the labour relations of employees with an employer of an Internet platform cannot be denied.

Of course, labour legislation must be flexible in order to adapt to the changing labour market. Thus, in China, labour legislation is practically not differentiated, as it does not take into account the peculiarities of the work performed by certain categories of workers. According to the current universal model, China's labour law ignores not only the differences between different types of employees, but it also does not recognize differences that exist between the different categories of employers.[58]

In this sense, Russia's labour law is more flexible. This is facilitated by the widespread use of the method of differentiation in the legal regulation of labour relations.

Similarly, in many countries, a category-based regulatory model is used, which takes into account the division of labour and employment into classical and special labour relations, as well as the different types of employers. Taking into account the complexity and diversity of labour relations, as well as the introduction of information technologies, it is urgently necessary to change the model of legal regulation of labour relations in order to provide appropriate institutional mechanisms and introduce rules that are different from traditional ones for new, flexible types of employment and their corresponding employees.[59]

In China, there is also a discussion at the political level about the status of employees of Internet platforms. Thus, local authorities establish rules for hiring drivers, including requirements for their qualifications. At the same time, the authorities are cautious about attempting to unambiguously qualify the relationship between drivers and Uber as one of employment.[60]

Based on scientific discussions and judicial practice, as well as taking into account the peculiarities of the digital economy, it has been proposed that criteria be formulated for determining the legal nature of Internet workers. So far, it has been proposed to include the duration of work and the type of service in such criteria. At the same time, the established approach to the status of employees of Internet platforms should reflect the need to ensure their rights, particularly those related to labour protection.[61]

---

58 Zengyi 2018, at 99.

59 *Id.* at 100.

60 Chenguo Zhang, *China's New Regulatory Regime Tailored for the Sharing Economy: The Case of Uber under Chinese Local Government Regulation in Comparison to the EU, US, and the UK*, 35 Comp. L. & Sec. Rev. 470 (2019).

61 *Id.*

According to legal scientists in China, an important factor that determines the status of Uber drivers (as well as employees of other Internet platforms) is the primary or supplemental nature of the work. Those drivers for whom this work is their primary source of employment are more likely to comply with the requirements of the company and to adapt to the conditions that are already in place. This indicates their greater economic dependence on the platform, which is typical for labour relations.[62]

In Russia, the issue of the nature of relations arising between, for example, drivers and Internet platforms is resolved in favor of the civil nature of these relations (such as a contract for the provision of paid services[63] or a vehicle rental agreement[64]). We consider this approach to be not quite appropriate.

Due to certain circumstances that allow us to reach this conclusion, it appears that people who perform their work responsibilities on Internet platforms should be classified as employees, and not as "performers."

We mentioned earlier that China is considering the idea of creating a global Internet platform for employment contracts. The primary objective of the service known as "Work in Russia" is to facilitate the undocumented registration of "ordinary" labour relations. There was some discussion in China about the possibility of creating a platform for the employment of citizens on the basis of remote employment. The service could be designed not only to enable job searching but also to monitor compliance with the labour rights of employees of this online platform such as social guarantees, the terms of their employment contracts and trade union activities.[65] Considering China's state-led approach to solving such problems, the creation of an online platform for the employment of citizens is only a matter of time.

3. Electronic Monitoring of Employee Behaviour

Modern methods of monitoring employees pose an even greater threat to worker rights than traditional surveys, cameras or even a regular Global Positioning System (GPS) tracker. More modern devices, such as mobile phone apps, can be used for legitimate purposes, such as improving labour productivity or preventing theft. However, nothing prevents an employer from collecting information for other

---

62 Wu et al. 2019, at 580–90.

63 Апелляционное определение Московского городского суда от 12 апреля 2018 г. № 33-15213/2018 // СПС «КонсультантПлюс» [Appeal decision of the Moscow City Court No. 33-15213/2018 of 12 April 2018, SPS "ConsultantPlus"] (Nov. 10, 2022), available at http://www.consultant.ru/online/.

64 Решение Калининского районного суда г. Челябинска от 6 октября 2016 г. № 2003761/2016 // СПС «КонсультантПлюс» [Decision of the Kalininsky District Court of Chelyabinsk No. 2003761/2016 of 6 October 2016, SPS "ConsultantPlus"] (Nov. 10, 2022), available at http://www.consultant.ru/online/].

65 Liu Dun & Geng Yuan, *The Model of the State Digital Platform on Labor Contracts in China,* 3(1) Digital L.J. 20–21 (2022).

purposes as well, such as to monitor biological reactions, listen in on personal telephone conversations or even determine employees' opinions towards trade union activities.[66] In 2018, Amazon patented the "hapticwristband," which monitors every movement of their employees.[67]

The peculiarity of today's control systems is that computers make such monitoring and observation of employees invisible.[68]

Moreover, today an employer, for example, may utilize technologies such as facial scanning, brain wave monitoring and emotion tracking to evaluate job applicants. It goes without saying that the collection and use of brain data, as well as any other data processing aimed at tracking and scanning emotions, feelings and mental states, should be prohibited in the workplace.[69]

The largest Chinese information technology companies have a surveillance system called the "Third Eye." This software gathers data from cameras located throughout the workplace as well as from the laptops of each employee in order to determine who is worthy of a promotion and who should be dismissed. The "Third Eye" allows employers to monitor their programmers' screens in real time, record their chats, their browser activity and every document edit. Some companies even install the system in restrooms. The program automatically detects "suspicious behaviour," such as accessing job search sites or video streaming platforms. Reports are generated weekly, summing up the time spent on "non-core" websites and applications. Moreover, the system does not differentiate whether an employee behaved "suspiciously" during working hours or during off-hours. Such control (surveillance) over an employee has its own legal consequences: an employee may be denied career advancements or a salary increase, and along with any corresponding "suspicious" behaviour of the employee, it may even serve as a reason for dismissal. All of this contributes to an increase in the number of cases of professional burnout and workplace suicide among workers in China.[70]

The practices described above may lead to unjustified interference with the privacy of employees and encroachment on the confidentiality of their personal lives by providing management with access to purely personal information. These

---

66 Richard Bales & Katherine Stone, *The Invisible Web of Work: The Intertwining of AI, Electronic Surveillance, and Labor Law*, 41(1) Berkeley J. Emp. & Lab. L. 51 (2019).

67 *Id.* at 16–17.

68 *Морейра Т.К., Андраде Ф.* Электронный контроль в сфере трудовых отношений // Вестник Нижегородского университета им. Н.И. Лобачевского. 2015. № 3. С. 164–168 [Teresa C. Moreira & Francisco P. de Andrade, *Electronic Control in Labour Relations,* 3 Vestnik of Lobachevsky Univ. of Nizhni Novgorod 159, 164–68 (2015)].

69 Valerio de Stefano, *"Negotiating the Algorithm": Automation, Artificial Intelligence and Labour Protection*, 41(1) Comp. Lab. L. & Pol. J. (2019) (Nov. 10, 2022), available at https://ssrn.com/abstract=3178233.

70 *600,000 Chinese Die from Overworking Each Year*, China Daily, 11 December 2016 (Nov. 10, 2022), available at https://www.chinadaily.com.cn/china/2016-12/11/content_27635578.htm.

data not only do not contribute to improving the quality of work, but they can also cause stress in the employee, adverse reactions and, ultimately, lead to a decrease in the employee's efficiency and productivity.[71] This is especially true if such a system is installed without serious coordination with employees and explanations from the employer.[72]

According to accurate observations made by Richard A. Bales and Katherine V.W. Stone, the development of technologies for collecting and storing information about an employee will eventually lead to the fact that the accumulated data will be something like a "bank of information" about all employees, which all employers can use, for example, to evaluate a potential employee.[73] In our opinion, this is unacceptable.

Today, there is a disruption in the balance that exists in the workplace between one's professional and personal (or private) life. With a high degree of probability, it can be argued that digitalization is significantly transforming the workplace; however, states appear to be in no hurry to regulate these complex and crucial relationships at this time. For example, in Russia, the concept of robotization and algorithmization of the labour process has not been developed at the legislative level and the issue of the extent to which employers may exercise control over their employees using technological means has not been resolved.

And yet, in the majority of cases, the noted advantages of using digital monitoring and surveillance tools in labour relations do not negate concerns about violating the "boundaries of employee privacy."

> Such aggressive monitoring raises concerns about obtaining consent from an employee to collect personal information. The concept of employee consent, as defined in some national legislation, is not a valid basis for processing personal data due to an imbalance of forces in labour relations. Employees may agree to monitoring and supervision for fear of retaliation from the employer and possible job loss.[74]

The purpose of the social dialogue at the present stage is to agree on the same algorithm that affects the assessment of the labour relationship. For example, in 2017, UNI Global Union (formerly, Union Network International) released a series of

---

71 de Stefano 2019.

72 David Halpern et al., *Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace*, 80(2) J. Bus. Ethics 178 (2007).

73 Bales & Stone 2019, at 4.

74 Eurofound, *Employee Monitoring and Surveillance: The Challenges of Digitalisation*, Publications Office of the European Union, Luxembourg (2020) (Nov. 10, 2022), available at https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20008en.pdf.

advanced proposals on ethical artificial intelligence in the workplace.[75] A number of authors[76] report on several collective agreements that are already in force in various countries, where the use of technology is regulated not only in the supervision of workers but also in the management of their work in order to protect the dignity of people, ensure occupational safety and the safety of workers.[77]

Thus, the legislation of many countries is moving in the direction of restricting the rights of employers to exercise electronic control over the behaviour of employees.

The European Court of Human Rights, in its landmark ruling of 5 September 2017, the case of *Barbulescu v. Romania* (Complaint No. 61496/08), essentially recognized the fact that employers do not have the right to use digital technologies in any way they please, since these technologies are intrusive in the sense that they affect employees' rights to respect for "personal life" (paragraphs 61, 73). The employer, in exercising control over the behaviour of employees, cannot assess their actions adequately since there is a strong temptation to learn as much as possible about an employee and then evaluate that employee not only in their capacity as a worker but also as a member of the family, society and the state.

The Oklahoma Statutes, specifically paragraph 40, titled "Labor," is of significance in this regard.[78] Article 173.2 of this act establishes rules on prohibited actions in relation to personal accounts on social networks.

In Russia, violations that occur in connection with the implementation of electronic control by employers are often associated with violations of the requirements of Federal Law No. 152-FZ of 27 July 2006 "On Personal Data."[79] The supervisory authorities indicate that it is necessary to take into account the purpose pursued by the operator when carrying out actions that are related to the processing of personal data. If they are used by the operator to establish the identity of the subject of personal data, then this processing must be carried out with the consent of the employee. However, if the processing of personal data is carried out for purposes other than "identification," then the actions cannot be considered processing of

---

[75] Global Union Sets New Rules for the Next Frontier of Work–Ethical AI and Employee Data Protection (UNI Global Union, 11 December 2017) (Nov. 10, 2022), available at http://uniglobalunion.org/news/global-union-sets-new-rulesnext-frontier-work-ethical-ai-and-employee-data-protection.

[76] Phoebe V. Moore et al., *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, in Phoebe V. Moore et al. (eds.), Humans and Machines at Work. Dynamics of Virtual Work (Nov. 10, 2022), available at https://doi.org/10.1007/978-3-319-58232-0_1.

[77] de Stefano 2019.

[78] Oklahoma Statutes Title 40. Labor, secs. 40–173.2, Prohibited actions regarding personal social media accounts – Exemptions – Civil actions (2019) (Nov. 10, 2022), available at https://law.justia.com/codes/oklahoma/2019/title-40/section-40-173-2/.

[79] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. 2006. 29 июля. № 165 [Federal Law No. 152-FZ of 27 July 2006. On Personal Data, Rossiyskaya Gazeta, 29 July 2006, No. 165].

biometric personal data and can be carried out without the consent of the subject since it is necessary for the fulfilment of the contract.

An analysis of Russian legislation allows us to come to the following conclusion: the legality of the procedure for establishing video surveillance of employees at the workplace without obtaining consent from employees to process personal data is justified due to the employer's compliance with a number of organizational procedures. Such procedures include the following:

1) adoption of a relevant local regulatory act by the employer;

2) definition of the purposes for which video surveillance is being used;

3) familiarizing employees with the local regulatory act and notifying them of the introduction and implementation of video surveillance of them. Video surveillance must be conducted openly;

4) placement of information signs in the areas of visibility of the cameras on the premises where video cameras are installed;;

5) appointment of a specially authorized person who will be granted access to personal data of employees.

In Russia, the processing of such personal data, which allows the identification of an employee as a person, is carried out by the employer without the consent of the employee due to an incorrect formulation of the term "biometric personal data" as well as an incorrect interpretation of this concept by Roskomnadzor (Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media).[80] It turns out that determining the volume of the specified data is not necessary in order to recognize personal data as biometric; rather, it is necessary to establish and comply with the purpose of their processing. This approach appears to be flawed on a fundamental level.

Furthermore, it appears that the main, basic feature of biometric personal data is that they characterize the physiological and biological characteristics of a person, regardless of the purpose for which the employer processes them. In addition, with the aid of audio and video recordings, the employer can establish the identity of an employee who violates workplace discipline. Accordingly, such a feature of biometric personal data as 'identification of the subject of personal data' may manifest itself indirectly when the employer exercises control over the employee's performance of work duties in the form of video surveillance.

All of this allows us to make the following assertions:

1. Personal data that became known to the employer as part of the implementation of video surveillance of the employee's behaviour while at work or at the workplace should be attributed to biometric personal data.

---

[80] Разъяснения Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве» // СПС «КонсультантПлюс» [Clarifications by Roskomnadzor "Issues Related to the Processing of Personal Data of Employees, Applicants for Vacant Positions, as Well as Those in the Personnel Reserve," SPS "ConsultantPlus"] (Nov. 10, 2022), available at http://www.consultant.ru/online/.

2. The processing of these biometric personal data must be carried out with the consent of the employee whose personal data is being processed, except in the instances that are established by federal laws.[81]

3. An employer has the legal right to process the biometric personal data of employees in order to monitor their attendance and access to the employer's premises, as well as to protect other employees, clients and the employer's property from unlawful encroachments. The use of digital technologies for the sole purpose of monitoring the activities of employees is unacceptable and should not violate their privacy.

It appears that in order to maintain a balance between the interests of employees and employers, as well as to increase the confidence of the parties to the employment relationship, it is the legislator who should set the goals of electronic monitoring of employees at the level of federal law.

The same problem is faced by lawmakers in China, where workers are increasingly raising the issue of privacy violations when they are subjected to real-time video surveillance during working hours while working remotely. Courts in China are increasingly embracing a modern approach to this issue, which recognizes that it is unlawful for employers to dismiss employees for refusing to turn on their computer screens and webcams and leave them on during all working hours.[82] In other words, there is sufficient ground for legislative measures to restrict the use of electronic monitoring of employee behaviour.

Conclusion

Thus, this study showed that similar issues exist in Russia and China in terms of legislative support for digitalization of labour relations. The legal regulation of the use of digital technologies in the field of labour as it exists today is not designed for the long term and resembles "patching holes." A number of issues in urgent need of legal regulation remain outside the legal field (for example, robotization and algorithmization in the field of labour; the protection of personal data of job applicants and the problem of unemployment in the application of artificial intelligence in the labour process). Such a "silence" can affect the stabilization of labour relations and increase discrimination in the field of labour.

Often, the legislator, who sometimes acts as an employer and sometimes as a regulator of legal relations, takes into account the requirements of only one side of the employment relationship: the employer or the interests of the state.

---

[81] Elena Ofman & Mikhail Sagandykov, *Electronic Monitoring for Employees: Employer Rights in the XXI Century*, 23(1) J. Legal, Ethical & Reg. Issues (2020) (Nov. 10, 2022), available at https://www.abacademies.org/articles/electronic-monitoring-for-employees-employer-rights-in-the-xxi-century-9605.html.

[82] **国外一公司**远程监控居家员工被判赔偿50**多万元** [*A foreign company was awarded more than $500,000 in damages for remotely monitoring its home-based employees*] (Nov. 10, 2022), available at https://www.gamersky.com/news/202210/1525805.shtml.

A number of regulations, primarily at the level of policy documents, both in Russia and in China indicate the need for a clearer definition of the legal status of employees of Internet platforms.

We believe that persons performing work on Internet platforms should be classified as employees, and not as performers under a civil contract. Judging by the decisions of the authorities and judicial bodies reviewed, China is closer to this conclusion than Russia.

It appears that today there is an urgent need for the federal authorities of Russia to adopt a "strategy for the transformation of labour relations in the application of digital (information) technologies," paying special attention to establishing a balance between the rights and interests of employees, employers and the state and the need to develop a concept of robotization and algorithmization of the labour process.

It is necessary to use a model of differentiation for the legal regulation of labour based on the allocation of a special category of employees and employers, namely online platforms. In Russia, differentiation of labour legislation is one of the main trends, but it has not yet been applied to employees of Internet platforms. In China, in general, the differentiation of legal regulation of labour relations is not developed. Significant legislative efforts should be made in both countries in this area.

When performing work on Internet platforms, employees enjoy greater flexibility in terms of working hours and rest time. However, employees of Internet platforms are subject to new types of risks, different from the risks faced by "traditional" workers. One of the main problematic issues is the issue of wages and the establishment of a minimum amount in the first place. In connection with the above, it would appear that minimum wages and minimum permitted working hours (as opposed to only the maximum, as currently is the case in the labour legislation of Russia) should be established at the legal level of the law.

When developing these and other documents, as well as adjusting the current regulatory framework, the Russian legislator should take into account the experience of international and foreign regulation of labour relations in the field of digitalization of labour relations, for example, to set limits on the intrusion of employers into the privacy of employees when monitoring their behaviour. It seems necessary to adjust both the concept and conditions of how the biometric personal data of employees is processed.

The legislation of Russia, as well as China, is far from establishing legal limits for the employer to carry out electronic monitoring of employee behaviour despite the fact that in both countries this control is only increasing and, at times, taking unacceptable forms.

References

Cao Y. *Regulating Digital Platforms in China: Current Practice and Future Developments*, 11(3–4) Journal of European Competition Law & Practice 173 (2020). https://doi.org/10.1093/jeclap/lpaa001

Prassl J. & Risak M. *Uber, Taskrabbit, & Co: Platforms as Employers? Rethinking the Legal Analysis of Crowdwork*, 37 Comparative Labor Law & Policy Journal 619 (2015).

Wu Q. et al. *Labor Control in the Gig Economy: Evidence from Uber in China*, 61(4) Journal of Industrial Relations 574 (2019). https://doi.org/10.1177/0022185619854472

Zengyi X. *The Changing Mode of Legal Regulation of Labor Relations in China*, 39(4) Social Sciences in China 96 (2018). https://doi.org/10.1080/02529203.2018.1483103

Лютов Н.Л. Адаптация трудового права к развитию цифровых технологий: вызовы и перспективы // Актуальные проблемы российского права. 2019. № 6(103). С. 98–105 [Lyutov N.L. *Adaptation of Labor Law to the Development of Digital Technologies: Challenges and Prospects*, 6(103) Current Problems of Russian Law 98 (2019)]. https://doi.org/10.17803/1994-1471.2019.103.6.098-107

Трощинский П.В., Молотников А.Е. Особенности нормативно-правового регулирования цифровой экономики и цифровых технологий в Китае // Правоведение. 2019. № 63(2). С. 309–326 [Troshchinskiy P.V. & Molotnikov A.E. *Features of Legal Regulation of the Digital Economy and Digital Technologies in China,* 63(2) Pravovedenie 309 (2019)].

Information about the authors

Elena Ofman (Chelyabinsk, Russia) – Associate Professor, Department of State and Law Theory and Labour Law, South Ural State University (National Research University) (76 Lenina Ave., Chelyabinsk, 454080, Russia; e-mail: ofmanem@susu.ru).

Mikhail Sagandykov (Chelyabinsk, Russia) – Associate Professor, Head, Department of State and Law Theory and Labour Law, South Ural State University (National Research University) (76 Lenina Ave., Chelyabinsk, 454080, Russia; e-mail: sagandykovms@susu.ru).

THE LEGAL ISSUE OF DETERRENCE OF ALGORITHMIC CONTROL OF DIGITAL PLATFORMS: THE EXPERIENCE OF CHINA, THE EUROPEAN UNION, RUSSIA AND INDIA

YULIA KHARITONOVA,

Lomonosov Moscow State University (Moscow, Russia)

NAMITA SINGH MALIK,

Galgotias University (Greater Noida, India)

TIANFANG YANG,

Shenzhen MSU-BIT University (Shenzhen, China)

https://doi.org/10.21684/2412-2343-2023-10-1-147-170

The authorities in a number of states are concerned about the need for public disclosure of the recommendation algorithms that are used in online services. The introduction of regulations aimed at software developers is frequently proposed as a potential solution to this problem of algorithm transparency. These requirements, which must be fulfilled by the developers of software products, can be administrative regulations or standards regulations. However, despite these efforts, in the absence of direct legislative regulation, users continue to encounter the possibility that a social network feed or a search service result may present content that is unequal or unclear. This is due to the fact that the logic behind these recommendations is not clear and is concealed by IT giants. The following are among the main provisions of legislative initiatives: the liability of digital platforms to publish the mechanisms of recommendation services, the responsibility to inform the user about the processing of personal data and the possibility for the user to refuse such processing. States have recognized the problem and are approaching it from different positions. Each region chooses what to prioritize in terms of the law. We see that for China and Europe, all areas of platforms are important, whereas for Russia, news platforms and video hosting are of interest and for India, social media is the most important platform category. However, in all of the countries, the requirements for the disclosure of the

recommendation engine to a certain extent are expanding. The amount of information that is publicly available as well as the order in which it is disclosed are both variable. This study demonstrates the commonalities and differences in the approaches taken by various countries.

Keywords: artificial intelligence; digital platform; recommendation system; big data; personal data.

Recommended citation: Yulia Kharitonova et al., *The Legal Issue of Deterrence of Algorithmic Control of Digital Platforms: The Experience of China, the European Union, Russia and India*, 10(1) BRICS Law Journal 147–170 (2023).

Table of Contents

Introduction

Digital platforms are becoming increasingly important for a wider range of businesses, and are essentially an element of the architecture of the digital economy proper. Moreover, a digital platform is often the only way to launch a business as a whole. For example, in the case of streaming services, video hosting and cloud services, it is impossible to develop an effective analogue that functions without constant access to the Internet. Many services, such as ordering a taxi, food delivery, communications, telecommunications among others, have recently transformed to such an extent that they have become a platform or part of an ecosystem. The term platforms is used by scholars and researchers to mean "sites and services that host

public expression, store it on and serve it up from the cloud, organize access to it through search and recommendation."[1]

According to R. Alt, the domains of business intelligence (BI), big data (BD) and social media analytics (SMA) stand out from the standpoint of sustainable corporate information models because they gather the appropriate amount of information to enhance the effectiveness of business operations.[2] As a result, they are utilized by decision makers as a basis for automated systems, which also include adaptive skills, or more specifically, functionality for machine learning.

The term "online platforms" describes a broad category of digital businesses that provide a central hub that serves as a meeting place for two or more different groups of users over the Internet. Examples include search engines, online marketplaces, the collaborative or sharing economy and social networks.[3] According to some scholars, it is necessary to highlight two important aspects: (a) digital platforms as online intermediaries come between and facilitate the connection of others and (b) the content they transmit is produced by others. Unlike previous technologies, the multi-tiered modular architecture of digital platforms fuels generativity, defined as the ability of a platform to promote unprompted innovation through continuous recombination of different modules.[4] According to researchers, "leading digital platform companies have used generativity combined with efficient management to achieve positive network effects, value creation, and scalability."[5] Next-generation digital platforms are starting to develop as a result of artificial intelligence (AI) technology. These technologies provide endless opportunities for human-machine interaction in order to handle the process on digital platforms.

Big data technology is important for the application of artificial intelligence on platforms of all kinds. Artificial intelligence is the general term for the capacity of a computer to do cognitive functions that we connect with the human mind, such as perception, reasoning, learning, interacting with the environment, solving problems, making decisions and even demonstrating creative abilities (AI).[6] And all of this is made possible by attracting big data.

---

1 Tarleton Gillespie, *Governance of and by Platforms*, in SAGE Handbook of Social Media 254 (2017); Howard Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. Pa. L. Rev. 1663 (2012).

2 Rainer Alt, *Electronic Markets on Digital Platforms and AI*, 31(2) Electron. Mark. 233 (2021).

3 House of Lords, Select Committee on European Union, *Online Platforms and the Digital Single Market*, 10th Report of Session 2015–16 (Feb. 2, 2023), available at https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf.

4 Arun Rai et al., *Next Generation Digital Platforms: Toward Human-AI Hybrids*, 43(1) MISQ iii-ix (2019).

5 Panos Constantinides et al., *Introduction – Platforms and Infrastructures in the Digital Age*, 29(2) Info. Systems Res. 381 (2018); Peijian Song et al., *The Ecosystem of Software Platform: A Study of Asymmetric Cross-Side Network Effects and Platform Governance*, 42(1) MISQ 121 (2018).

6 Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искус-

Data for artificial intelligence operations are collected from separate digital platforms or from intermediate data platforms containing partially pre-processed data.[7]

In order to (at least partially) automate the data preprocessing operation itself and to detect whether or not the data have changed, AI algorithms have been utilized in predictive models (so-called concept drift or data drift[8]). Additionally, the function of platform providers, often known as gatekeepers, affects data access. These providers may elect to transfer or sell data to third parties in specific circumstances, but they may also decide to keep the data for their own use. There are a number of large-scale tech platforms with business structures that raise questions about how they use their power. In one review, the founder of several Internet companies assessed that this quasi-oligopolistic market structure could be detrimental to innovation and user freedom.[9] The recent investigation by the European Commission into Facebook, which is accused of manipulating advertising data from its online marketplace and online dating platform illegally to obtain a competitive advantage for its own services, is one instance where this is apparent.[10]

The European Commission opened an investigation into Facebook in 2019 pertaining to the company's suspected misuse of user data to impede competition.[11] More recently, the Commission launched a new antitrust probe in 2021 into Facebook's use of information gathered from advertisers.[12] The Commission is debating whether Facebook enjoys an unfair competitive advantage in the market for online classified ads where it competes with businesses from which it obtains data.[13]

In addition to the aspect of competition associated with the use of platform users' data for the purposes of artificial intelligence systems, the most important

---

ственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс» [Presidential Decree No. 490 of 10 October 2019. On the Development of Artificial Intelligence in the Russian Federation (with the "National Strategy for the Development of Artificial Intelligence for the period until 2030"), SPS "ConsultantPlus"] (Feb. 2, 2023), available at https://www.consultant.ru.

7 Boris Otto et al., *Information and Data Quality in Networked Business*, 21(2) Electron. Mark. 79 (2011).

8 João Gama et al., *A Survey on Concept Drift Adaptation*, 46(4) ACM Computing Surveys 1 (2014).

9 Andreas Göldi, *A Blind Spot for the Dark Side: The Monopolies We Didn't See Coming*, 30(1) Electron. Mark. 55 (2020).

10 Sam Schechner, *Facebook's Marketplace Faces Antitrust Probes in EU, UK*, Wall Street Journal, 4 June 2021 (Feb. 2, 2023), available at https://www.wsj.com/articles/eu-and-u-k-open-antitrust-probes-into-facebook-11622800304.

11 Elyssa Diamond, *Distrust & Antitrust: Using Facebook to Understand Competition Law's Role in Regulating Data and Data Privacy Concerns Around the World*, 45(5) Fordham Int'l L.J. 873 (2022).

12 Press Release, Eur. Comm'n, *Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct of Facebook*, 4 June 2021 (Feb. 2, 2023), available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2848.

13 Diamond 2022.

issue is user safety. This is because with algorithms the systems gain the ability to limit the user's information field, thereby immersing the user in an information bubble that is as complimentary as possible to his beliefs. In information societies, algorithmic selection has emerged as a significant source of both social order and shared social reality. Automated algorithmic selection applications influence people's daily realities, worldviews, and behavior.[14] Many people have long known that the main task of algorithms is to keep users in front of the screen and make them view their feed for as long as possible. For all that, it is the negative emotional content that engages audiences the most, such as false information, conspiracy theories, extremist and offensive statements and other destructive content,[15] which the online platforms do not effectively combat.

Thus, as C. Scardovi notes,

> The new problem of critical issue to address is to make sure the "great disruption" [which] will bring about a greater value for the multitudes will be around the ownership, management and utilization of data – avoiding the insurgence of a few "big brothers" that could build a quasi-monopolistic positioning in the market – hence stifling competition value-sharing for customers.[16]

1. Digital Platform Business Models: Recommendations and Manipulations

The range of digital platform monetization models is incredibly extensive.[17] The most common models include the following:

• Advertising is the main platform monetization model, which is often used along with other models, and in the case of the largest digital players (such as Yandex, Google, Amazon), is the primary source of income for the platform operator. The ability of platforms to leverage the attention of their users allows them, to this day, to generate enormous revenues from advertising services alone.

• Commission in which the platform frequently acts as an intermediary between the seller and the buyer, and takes a certain fee for its services.

• The Freemium business model implies that the platform provides a service for free, but to use the additional functionalities, users have to purchase a full version or

---

[14] Natascha Just & Michael Latzer, *Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet*, 39(2) Media, Culture & Soc'y 238 (2017).

[15] Lee Rainie et al., *The Future of Free Speech, Trolls, Anonymity and Fake News Online*, Pew Research Center, Washington, DC (2017).

[16] Claudio Scardovi, *Digital for the Greater Good,* in Digital Transformation in Financial Services 187 (2017).

[17] Tobias Mini & Thomas Widjaja, *Tensions in Digital Platform Business Models: A Literature Review*, ICIS (2019).

pay a subscription among other options. For example, watching videos on YouTube without the accompanying advertising is possible only with a YouTube Premium subscription; the ability to listen to music in the social network VKontakte with the screen turned off requires a subscription to VK Boom.

• An Extended Access model assumes that all platform users are granted access to it on equal terms, but for a certain fee, the user can be guaranteed additional advantages in its use compared to other users, such as highlighting and raising ads on Avito and Cian and accessing closed sales on Yandex.Market, Ozone and Farfetch.

There are also other ways of platform entrepreneurship. It is important to note, however, that a digital platform is not limited to using only one model.

The early years of this connected world were idealized as a free and open civic forum: a place where diverse opinions, thoughts and conversations might come together in a positive way.[18] Not only were the technical properties of the platforms assessed, but also the benefits that users can derive from their use (the result of user interaction).[19] Several studies suggest that user interaction results in a transaction or innovation.[20] By the term "transaction," it is understood to mean the actual actions of platform users aimed at the purchase of goods, works and services, as well as the exchange of information; by the term "innovation," we mean the actual actions of platform users aimed at the creation or development of a new product, technical solution or technological process. The following are some examples of the term "transaction": money transfers, purchase of goods through advertisements, booking hotel rooms, online distribution of movies and so on. Examples of innovations include: developing a smartphone application, a software algorithm design or a software library.

Recommender Systems serve as individualized decision aids that can assist users in making choices pertaining to concerns of personal preference.[21] Data access as the main problem of the digital platform is most evident in the operation of recommendation systems. Software tools and procedures called recommender systems (RSs) propose products that are most likely to be of interest to a particular user.[22] The recommendations are made in relation to numerous decision-making

---

18 Rainie et al. 2017.

19 Carla Bonina et al., *Digital Platforms for Development: Foundations and Research Agenda*, 31(6) Info. Systems J. 869 (2021).

20 Natalia Simchenko et al., *Digital Platforms of Networking in Industry*, 753(6) IOP Conference Series: Materials Science and Engineering (Article 062005) (2020).

21 Rashmi Sinha & Kirsten Swearingen, *The Role of Transparency in Recommender Systems*, in CHI' 02 Extended Abstracts on Human Factors in Computing Systems 830 (2002).

22 Tariq Mahmood & Francesco Ricci, *Improving Recommender Systems with Adaptive Conversational Strategies*, in Proceedings of the 20th ACM Conference on Hypertext and Hypermedia 73 (2009).

processes, such as what to buy, what music to listen to[23] or what news to read online.[24] The goal of the recommendation system is to predict the user's behavior with regard to the subject of his or her information search and to provide recommendations for subjects the user has not yet come into contact with.[25]

In computer science, in its most general form, recommendation systems are presented as a sub-technology of artificial intelligence. It is a class of solutions that provides process performance without human input, assistance in choosing decisions, and prediction of objects that will be of interest to the user.[26]

In the process, recommendation systems collect data about users using a combination of explicit and implicit preference elicitation methods,[27] analyzing user responses to questionnaires and answers to questions relating to their degree of satisfaction; analysis of direct individual preferences; as well as data on user browsing of certain content online; individual online browsing behavior and user activity tracking patterns.

D. Shin hypothesizes that

> the heuristic effect occurs when users' subjective feelings about transparency and accuracy act as a mental shortcut: users considered transparent and accurate systems to be convenient and useful. The mediating role of trust suggests that establishing algorithmic trust between users and NRS [news recommender system] can enhance algorithm performance.[28]

As a result of a wider perspective on combating illegal content online and the concerns to request proactive (automated) measures from online intermediaries, scholars have taken an interest in the impact of disinformation initiatives on freedom of expression, media pluralism and the exercise of democracy. Many of these initiatives are based on automated decision-making systems using artificial intelligence to cope with the scale of content being shared.[29] The impact of recommended services on

---

[23] Kirsten Swearingen & Rashmi Sinha, *Beyond Algorithms: An HCI Perspective on Recommender Systems*, 13(5–6) ACM SIGIR, Workshop on Recommender Systems 1 (2001).

[24] Francesco Ricci et al., *Introduction to Recommender Systems*, in Recommender Systems Handbook 1 (2011).

[25] Marco de Gemmis et al., *Semantics-Aware Content-Based Recommender Systems*, in Francesco Ricci et al. (eds.) Recommender Systems Handbook 119 (2015).

[26] *See* the 2019 Roadmap for the Development of "end-to-end" Digital Technology "Neurotechnology and Artificial Intelligence" (Feb. 2, 2023), available at https://digital.gov.ru/.

[27] Gediminas Adomavicius & Alexander Tuzhilin, *Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions*, 17(6) IEEE Transactions on Knowledge and Data Engineering 734 (2005).

[28] Donghee Shin, *How Do Users Interact with Algorithm Recommender Systems? The Interaction of Users, Algorithms, and Performance*, Comput. Hum. Behav. 109 (Article 106344) (2020).

[29] Chris Marsden et al., *Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation?*, 36 Computer L. & Security Rev. (Article 105373) (2020).

user awareness and pricing for different consumer groups has also increased in importance.

Moving away from data-centric assessment criteria and towards user-centered assessment criteria is also a significant subject in recommender systems, particularly in user-centric systems.[30]

When using apps with recommender systems, the users are constantly exposed to different stimuli (such as visual, auditory and so on) that cause them to feel different emotions. According to the bounded rationality model,[31] these feelings influence the user's decision regarding which content to select, at least in part. All of this has caused digital platforms to be viewed as algorithmic agents.[32] The application that makes up the recommender system must therefore be able to recognize and effectively adopt emotive data.

There have been numerous instances in which suggestions have worked in an undesirable way. For example, in the summer of 2021, researchers discovered that YouTube's recommendation engine recommended problematic videos that violated the online platform's own rules: unwanted content, selected by artificial intelligence, accounted for 71 percent of the total number of videos viewed by the experiment's participants.[33] According to experts the survey indicates that there is an "inherent contradiction" between YouTube's algorithms, some of which recommend undesirable videos while others attempt to remove them. At the same time, the platform refuses to disclose information about how its recommendation engine works.

In 2021, a Facebook[34] insider, Frances Haugen, described in detail how the social network's recommendation service is organized. In September, *The Wall Street Journal*[35] described how Facebook algorithms incite aggression and hate among users; how the social network is used for criminal purposes; how it spreads false information about the pandemic coronavirus and vaccination and how Instagram, Facebook's media partner, damages the self-esteem and psyche of teenagers by causing suicidal

---

30 Marko Tkalcic et al., *Affective Recommender Systems: The Role of Emotions in Recommender Systems*, in Proceedings of The RecSys 2011 Workshop on Human Decision Making in Recommender Systems 9 (2011).

31 Daniel Kahneman, *A Perspective on Judgment and Choice: Mapping Bounded Rationality*, 58(9) The American Psychologist 697 (2003).

32 Balazs Bodo et al., *Tackling the Algorithmic Control Crisis – The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents*, 19 Yale J.L. & Tech. 133 (2017); Evangelos Kranakis & Danny Krizanc, *An Algorithmic Theory of Mobile Agents*, Conference paper, International Symposium on Trustworthy Global Computing 86 (2006).

33 *YouTube's Search Algorithm Directs Viewers to False and Sexualized Videos, Study Finds*, Wall Street Journal, 7 July 2021 (Feb. 2, 2023), available at https://www.wsj.com/articles/youtubes-search-algorithm-directs-viewers-to-false-and-sexualized-videos-study-finds-11625644803.

34 Meta Corporation, which owns the social network, is recognized as extremist and banned in the Russian Federation.

35 *The Facebook Files*, A Wall Street Journal Investigation, 1 October 2021 (Feb. 2, 2023), available at https://www.wsj.com/articles/the-facebook-files-11631713039.

thoughts. Algorithm formation is allegedly designed so that people spend as much time as possible in empty discussions, insulting each other in the comments, because Facebook makes money on this. Facebook loses money and views when such content is blocked. From all of this one may conclude that the "Like and Share" functions, the platform's main tools, accelerate the spread of hate speech. This conclusion is in fact stated in the study titled "Collateral Damage." After all, basic product mechanics such as viral activity, recommendations and optimizing for engagement are a significant part of why these types of speech flourish on the platform.[36]

Policymakers and lawmakers worldwide are concerned about the issue of containing through regulation the control that informational digital platforms have over algorithms.[37] One clear idea today is to require that the algorithm recommendations be disclosed to the public. This is necessary so that the user understands how the service works, what data about it may be used and for what purposes. We are talking about making the recommendation service as transparent as possible, so that users will have confidence in the algorithmic recommendations, but they will also have the option to disable the suggestions.

Various studies have been conducted to explore the issue of transparency in the algorithms used to determine recommendation system selection. For example, the role of transparency in music recommendation systems has tentatively shown that users like recommendations that they perceive to be transparent and feel more confident about using.[38]

According to the findings of researchers L. Zhou and colleagues,

> (1) product transparency, vendor transparency, and transaction transparency significantly affect perceived information transparency; (2) perceived information transparency significantly increases consumers' online purchase intention; and (3) perceived risk partially mediates the effect of perceived information transparency on purchase intent.[39]

At the same time, the Regional Public Center for Internet Technologies (ROCIT) conducted a study of users' perceptions of recommendation engines. According to the survey, 77.5% of respondents believe that recommendation algorithms are a form of advertising. In this case, more than 48% of respondents believe that such

---

36 *The Facebook Files*, *supra* note 35.

37 Godofredo Ramizo, *Platform Playbook: A Typology of Consumer Strategies against Algorithmic Control in Digital Platforms*, Info., Comm. & Soc'y 1 (2021); Alex J. Wood et al., *Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy*, 33(1) Work, Emp. & Soc'y 56 (2019).

38 Sinha & Swearingen 2002.

39 Liying Zhou et al., *Perceived Information Transparency in B2C e-commerce: An Empirical Investigation*, 55(7) Info. & Mgmt. 912 (2018).

technology does not impact their decisions of purchasing items or services, and 53.2% declare that the suggestions cannot force them to buy a product or service (the opposing opinion is held by 33% of respondents). More than half of those surveyed (53.1%) believe that algorithms do not influence their choice of movies or television shows. At the same time, the vast majority of respondents (74%) would like to be able to disable recommendation engines. Approximately 11% of users do not agree with such a statement, and another 15% find it difficult to answer this question.

Surveys also reveal that many advertisements are contentious because they evoke wildly disparate responses from people in various socially important groups. The controversial advertisements target segments of society that are most resentful of the status quo. In addition, experts support proposals for more targeted political and commercial advertising as well as greater content transparency. For instance, Facebook's advertising application programming interface (API) enables such targeting by making available the enormous quantity of user-specific data that Facebook collects and provides to advertisers.[40]

The next step towards transparency should be the option for users to disable the recommendation engine with one click, prohibit processing of personal data, discontinue using the service and so on; thereby protecting their fundamental rights and freedom of choice. Regulation of the mechanisms and algorithms of the output of recommendation systems, including measures to protect children from certain types of content, the use of targeted advertising and attempts to manipulate users, is already underway in different states.

2. Legal Opportunities for Improving the Transparency of Recommendation Systems to Users' Protection

The problem of ensuring the transparency of recommendation algorithms has two possible solutions. The first would be the direction of self-organization of information technology (IT) companies to provide users with the most comfortable service.

Companies develop "privacy notices" for their websites that explain what the project is about, what research questions the platform operators are investigating, what kinds of data are collected, how data is used, whether data is shared with other players and how that data is protected. Moreover, providing clear information shows users that the company values them and wants their direct participation. Ideally, openness and clarity about what the platform does with the data provided will gain the trust of users and make them active participants in the research rather than mere subjects of research.

The second is to create strict regulation of this area. From a legal point of view, the use of recommendation systems comes up against the legal framework that governs

[40] Filipe N. Ribeiro et al., *On Microtargeting Socially Divisive Ads: A Case Study of Russia-linked Ad Campaigns on Facebook*, in Proceedings of the Conference on Fairness, Accountability, and Transparency 140 (2019).

the personal data of a citizen. The issue of data flow is now of critical importance in all jurisdictions. China, one of the leaders of the digital economy, introduced a "digital dictatorship" on 1 September 2022 and declared the personal data of its citizens a national treasure.[41] In the European Union, the Digital Services Act[42] (DSA) has been drafted. In Russia, the concept of publicly available data has been introduced, establishing a common approach to the digital profile of individuals, and there is an ongoing discussion about the general obligation to disclose the algorithm of recommendation systems for certain types of platforms.[43]

2.1. China's Experience: Managing Recommendation Algorithms

Since 1 March 2022, there has been a rather radical regulation in place in China that states "either declare or leave the market." According to the Regulation on the Management of Algorithmic Recommendations of Information Services on the Internet (hereinafter, the Regulation), the emphasis is precisely on algorithmic recommendations. The "application of algorithmic recommendation technologies"[44] refers to actions in which such types of algorithmic technologies as (a) generation and synthesis (data); (b) personalized suggestions; (c) sorting; (d) search and filtering (data) and (c) prediction and decision selection are used when providing information to users (Art. 2, para. 2 of the Regulation). These rules are addressed to algorithmic recommendation service providers. The recommendation algorithms must be created taking into account ethical guidelines (social, business and professional ethics) and following the principles of impartiality, fairness, openness and transparency; scientific rationality; honesty and integrity (Art. 4 of the Regulation).

The Regulation takes precedence over rules contained in other acts, including laws and administrative regulations (Art. 2 of the Regulation). At the same time, some of the regulations are partially based on other acts, such as the People's Republic of China Cyber Security Law,[45] the People's Republic of China Data Security Law,[46] the

---

41 互联网信息服务算法推荐管理规定, available at http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.

42 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Feb. 2, 2023), available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.

43 В России могут частично отменить рекомендательные алгоритмы интернет-сервисов // Ведомости. 19 мая 2022 г. [*In Russia, Recommender Algorithms for Internet Services May Be Partially Canceled*, Vedomosti, 19 May 2022] (Feb. 2, 2023), available at https://www.vedomosti.ru/technology/articles/2022/05/18/922642-otmenit-rekomendatelnie-algoritmi?ysclid=l45fakv5tn238038620.

44 算法推荐技术 – Algorithmic Recommendation Technology.

45 中华人民共和国网络安全法 (Feb. 2, 2023), available at http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm.

46 中华人民共和国数据安全法(Feb. 2, 2023), available at http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

People's Republic of China Personal Information Protection Law (PIPL),[47] which came into force on 1 November 2021 and the Internet Information Services Regulatory Measures.[48]

Furthermore, the Regulation contains several sections regulating different areas of the creation and application of recommendation systems. In terms of technical requirements for information services, Article 10 of the Regulation states that algorithmic recommendation service providers must manage user models and user tags (including allowing the user to select or remove tags related to their personal characteristics at their discretion – Art. 17), improve rules for geo location and recommendations of so-called "points of interest" (PoI) for user visits, and must not record illegal and undesirable information. Moreover, within the meaning of Article 12 of the Regulation, it is the duty of the algorithmic recommendation service provider to "optimize" the transparency and interpretability of rules, such as searching, sorting, selection, presentation and display of content, in order to protect users from the adverse effects of undesirable content.

The phrase "optimize (优化) the transparency and interpretability of the rules" for recommender algorithms refers to the two responsibilities of the recommender service provider – to optimize the interpretability of the algorithms and to optimize the transparency of the algorithms. The provider of algorithmic advice services must clearly inform users about the provision of algorithmic recommendation services and properly publish the basis, purpose and basic working mechanism of the algorithmic recommendation service (Art. 16 of the Regulation). Article 17 of the Regulation specifically emphasizes that the recommendation systems cannot base their offers on the user's personal profile, which allows stating the establishment of a non-discriminatory mechanism of user access to various kinds of information services and products. Additionally, users must be provided with convenient options for disconnecting the services of algorithmic recommendations. If the user decides to disable the service of algorithmic recommendation services, the provider of such services must immediately terminate the provision of the mentioned services. Users of a number of popular mobile apps in China, such as Toutiao (今日头条), Douyin (抖音, Tik-tok), Kuaishou (快手), Ele.me (饿了么), Taobao (淘宝) and Meituan Waimai (美团外卖), are now able to turn off personalized recommendations. Special rules are also in place for making recommendations for minors and the elderly.

According to the Regulation, China requires registration of algorithms for recommendation systems. This registration is intended to ensure that the authorized cybersecurity and information authorities (state, province, autonomous region or

---

[47] Personal Information Protection Law of the People's Republic of China [中华人民共和国个人信息保护法] (Feb. 2, 2023), available at https://www.pkulaw.com/en_law/d653ed619d0961c0bdfb.html.

[48] 联互网信息服务管理办法(Feb. 2, 2023), available at http://www.gov.cn/gongbao/content/2000/content_60531.htm.

central city) are notified of the risks of the algorithms used in practice in accordance with Article 25 of the Regulation. Full disclosure of technological solutions, the source code of algorithms, which is a hotly discussed subject in other countries, is not a subject for registration in China.

2.2. The European Union: Deterring Manipulation (Manipulating Users' Choices)

In the European Union, the introduction of the General Data Prevention Regulation (GDPR) and the Digital Services Act (DSA) Regulation was an important step in the development of legislation in the direction of transparency. Transparency is a central principle in the GDPR, as it promotes the strengthening of lawful and fair processing of personal data, accountability, and rights of individuals whose personal data are "collected, used, consulted or otherwise processed" (Recital 39, GDPR). The principle of transparency of data processing requires that the information provided to the data subject is "concise, easily accessible and easy to understand" (Recital 58, GDPR) and also that the data subject be informed "of the existence of the processing operation and its purposes" (Recital 60, GDPR). It may be argued that algorithmic transparency has a limited applicability since Article 22 only applies to "decisions based solely on automated processing." This could mean that a sort of a "right of explanation" for the data subject, together with the safeguards outlined in Article 22(3), may not be applied whenever there is even a minimal human intervention.[49]

It is worth noting the contrast between the transparency increasingly expected from Internet giants or governments, on the one hand, and the relative opaqueness promoted by regulations such as the General Data Protection Regulation (GDPR), regarding personal privacy. This different treatment is intended, at least in part, to correct the current asymmetry of information between these players and to restore citizen confidence.[50]

Under the new DSA rules, access to platforms' algorithms is now possible. The DSA specifies a number of strategies, including improved governance, increased openness and outcome monitoring. Online platforms that provide intermediary services, such as social media and marketplaces, will need to take precautions to keep their users from accessing illegal goods, services and content. Users will be better informed about the suggestions made for their content. The algorithms of extremely big internet platforms will be made available to the European Commission as well as all the member states. There are additional bans on targeting ads towards minors as well as targeting based on sensitive data.

---

[49] Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-making Does Not Exist in the General Data Protection Regulation*, 7(2) Int'l Data Privacy L. 76 (2017).

[50] Serge Abiteboul, *The Quality, Fairness, Transparency and Accountability of Algorithmic Decisions*, 13 Digital Issues, Confidence (March 2021) (Feb. 2, 2023), available at https://www.annales.org/edit/enjeux-numeriques/DG/2021/DG-2021-13/EnjNum21a_12Abiteboul.pdf.

In addition to the transparency of data and systems, there needs to be disclosure regarding the degree to which the AI system influences organizational decision-making and the factors that led to the decision to use it.[51]

The DSA also stipulates the following aspects of algorithmic transparency:

Fundamental rights to be protected online: stronger safeguards to ensure notices are processed in a "non-arbitrary and non-discriminatory manner" and with respect for fundamental rights, including freedom of expression and data protection;

More responsible online marketplaces: these marketplaces have to ensure that consumers can purchase safe products or services online by strengthening checks to prove that the information provided by traders is reliable (also known as the "Know Your Business Customer" principle) and making efforts to prevent illegal content from appearing on their platforms, including through random checks;

New transparency obligations for platforms: users will be better informed about how content is recommended to them (recommender systems) and will also be able to choose at least one option not based on profiling;

Manipulating users' choices through "dark patterns" will be prohibited: online platforms and marketplaces should not nudge people into using their services, for example by giving more prominence to a particular choice or urging the recipient to change their choice via interfering pop-ups. Moreover, cancelling a subscription to a service should be as easy as subscribing to it.

In contrast to the present debate in the European Parliament, the U.K. government has declared that it will pursue specific approaches to AI regulation and advisory algorithms. European officials intend to categorize AI technologies into different risk categories. The riskier the technology the stronger the rules will be, even going as far as a ban. On the other hand, the British want to switch from a generic to an individual approach, allowing businesses to show the regulator that a certain solution is secure.[52] The idea proposed in the United Kingdom is intriguing since it has some similarities to the Chinese law, which requires programmers to justify the logic behind their algorithms to Communist Party officials. The trend is clear: all digital powers hold firms directly accountable for the threats that their technologies pose to society because they are aware of the dangers of the AI sector's unchecked growth.

---

[51] European Parliament, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human Centric Artificial Intelligence (COM(2019)168).

[52] *Establishing a pro-innovation approach to regulating AI*, Policy paper (2022) (Feb. 2, 2023), available at https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement.

2.3. The Indian Experience: Message Verification and Social Media Ethics

New regulations under the Information Technology Act, 2000[53] (IT Act) for monitoring social media and digital media platforms have been notified by the Ministry of Electronics and Information Technology, Government of India, following years of deliberations and arguments. The new regulations, known as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Guidelines) among other things, have the dual goals of (a) increasing social media platforms' accountability to prevent abuse and misuse, and (b) empowering social media users by establishing a three-tiered grievance resolution mechanism. The Information Technology Intermediary Guidelines have been replaced by the Intermediary Guidelines, which were created in accordance with section 87(2) of the IT Act (Intermediary Guidelines).

The rules that were set via notification in India on 25 February 2021 and that went into effect on 26 May 2021 consist of three parts: the first part covers definitions in the rules; the second part covers intermediaries' due diligence and the third part covers the Code of Ethics and Procedure and Safeguards in relation to digital/online media.[54] These Rules strike the perfect balance between a permissive approach and a soft self-regulatory structure. In addition, protection from inappropriate user-generated content is offered by the new information technology rules 2021s guidelines and restrictions.

According to researchers, these regulations aim to regulate social media and digital news platforms and hold users and tech giants more accountable in the modern day. Under this legislation, important social media intermediaries are also subject to regulation.[55]

Furthermore, under this act, widely used social media intermediaries that primarily offer messaging services are required to make it possible to identify the original source of information when it is needed only for the prevention, detection, investigation, prosecution or punishment of an offense related to India's sovereignty and integrity; the security of the State; friendly relations with other countries; public order or the incitement of an offense. The intermediary is not compelled to reveal to the first originator the contents of any communication or any other information.[56]

In addition to setting up automated systems for content filtration and notifying users if their accounts have been blocked with reasons for doing so, social media

---

[53] Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (Feb. 2, 2023), available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749.

[54] *Id.*

[55] Amit Kumar & Amaresh Jha, *Information Technology Rules, 2021 of India in Dock! A Critical Evaluation of the Guidelines for Intermediaries and Digital Media Ethics Code*, 20(48) Global Media J. 1 (2022).

[56] Matthew Barnidge & Michael A. Xenos, *Social Media News Deserts: Digital Inequalities and Incidental News Exposure on Social Media Platforms*, New Media & Soc'y (2021).

networks, particularly Twitter, must change their user interfaces to clearly identify verified users from others. Platforms such as Facebook will also need to develop a new user interface for India that will allow users to verify users using valid know-your-customer (KYC) procedures and display a verification tag for those who want this.[57]

In India, there is an emphasis on user verification to control fake news and hate speech. There is also a focus on content filtration. Moreover, attention is also paid to the problem of blocking user accounts. The following is stated in the Rules regarding giving users a chance to be heard: In cases where significant social media intermediaries remove or disable access to any information of their own volition, a prior notification of the same shall be communicated to the user who shared that information with a notice explaining the grounds and reasons for such action. Users must be provided an adequate and reasonable opportunity to dispute the action taken by the intermediary.

Furthermore, it should be emphasized that in India, the Code of Ethics is not about the use of artificial intelligence technology but about the ethics of media content. However, in general, the Indian legislator focuses on the protection of users and the cyber sovereignty of the state while not directly addressing the commercial activities of digital platforms.

2.4. The Russian Experience: Ethics, Standards and Openness

In Russia, "soft law" instruments are actually the leading regulators of the application of algorithmic engines on online platforms. It is well known that publishing software design recommendations by administrative authorities is one possible way to limit developers' freedom of action without having restrictions in the law itself. Researchers back this viewpoint by stating that administrative authorities may collaborate with developers to ascertain the qualities they believe a piece of software ought to have, after which the program could be developed to satisfy those qualities and be permit-proof.[58]

In 2020, the Federal Agency for Technical Regulation and Metrology developed a promising standardization program in the priority area "Artificial Intelligence" for the period 2021–2024 and providing for the development of 217 standards in this area.[59] In accordance with this Program, in 2020, GOST R 59276-2020 "Artificial Intelligence Systems. Ways to build trust. General Provisions" which defines the concept of trust in artificial intelligence systems was released. This act provides for the classification of factors affecting the quality and ability of artificial intelligence systems to inspire

---

[57] Kumar & Jha 2022.

[58] Joshua Alexander Kroll, *Accountable Algorithms*, Diss., Princeton University (2015).

[59] Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект» на период 2021–2024 годы [A Promising Standardization Program in the Priority Area "Artificial Intelligence" for the Period 2021–2024] (Feb. 2, 2023), available at https://www.economy.gov.ru/material/file/28a4b183b4aee34051e85ddb3da87625/20201222.pdf.

trust at the various stages of their life cycle and the classification of the main ways to ensure confidence in artificial intelligence systems. Additionally, the act formalizes the relationship between the quality and ability of artificial intelligence systems to inspire trust. At the same time, this standard cannot be used for systems of "strong" or "general" artificial intelligence. The Big Data Code of Ethics outlines the risks of using recommendation systems, including the impact on a person's decision, as well as ensuring transparency and objectivity in data selection. The Code was signed on 12 December 2019 by Gazprom-Media Holding, Yandex, Megafon, Tinkoff Bank, Sberbank, Gazprombank, oneFactor, Qiwi Group, Mail.ru Group, VTB Group, Vimpelcom, Rostelecom, MTS and the Analytical Center under the Russian government. The Russian Association of Electronic Communication (RAEC) and the Big Data Association published the Big Data Code of Ethics White Paper in 2021. Furthermore, in the same year, leading Russian technology companies adopted a Code of Ethics for Artificial Intelligence,[60] which allowed for voluntary self-regulation and the implementation of a 'soft power' tool to achieve consensus between AI and humans. The Code of Ethics for Artificial Intelligence has a dedicated section for: Transparency (for example, transparency of data collection, data sets and information processing).

There is a link between ethics and ensuring that the algorithm is transparent so that consumers understand the reasoning behind why a particular suggestion was made.[61] On the one hand, standards and codes of ethics do not solve the issue of holding unconscionable platforms responsible. But on the other hand, beyond the scope of laws, even very strict ones, there remains an area that is still subject to ethical standards. In China, for example, the rule is that outside of direct regulations, platforms and recommendation system operators must follow self-regulation, industry standards, improve service specifications and provide services in accordance with the law and under public scrutiny. Thus, the bet is placed on self-regulation within the ethical and legal framework, as well as the requirements of Chinese society.

The same can be said of the European regulatory experience. Globally, in its acts and policies, the EU proposes to return to non-complex disclosure obligations. The European model is unable to balance information asymmetries and unequal bargaining power, from which small and medium-sized enterprises and users suffer. In practice, the EU model consists either of pure self-regulatory delegation (codes of conduct) or unenforceable co-regulatory schemes (with a set of technical standards for the platforms).[62]

---

60 AI Alliance Russia (Feb. 2, 2023), available at https://a-ai.ru/en/.

61 Bodo et al. 2017; Yulia S. Kharitonova et al., *Artificial Intelligence's Algorithmic Bias: Ethical and Legal Issues*, 53 Perm U. Herald Jurid. Sci. 488 (2021).

62 Fabiana Di Porto & Marialuisa Zuppetta, *Co-regulating Algorithmic Disclosure for Digital Platforms*, 40(2) Pol'y & Soc'y 272 (2021).

At the same time, the above cases of algorithmic control biases by digital platforms require a legal regulation of algorithm disclosure rules.

In Russia, the issue of openness of the recommendation algorithm has not yet been legally resolved. A draft law has been developed that should eliminate the problem of the unaccountability of the work of recommendation algorithms, which are based on a non-transparent data collection scheme and create risks of promoting a profitable agenda for service owners or third parties and hiding "inconvenient" content.[63] The draft law does not provide for a prohibition on the recommendations but is aimed at protecting users from attempts at manipulation.

In order to achieve this aim, the operators of the services will be required to disclose the terms of the recommendation systems engine and inform the users of the data they collect. In addition, users will be allowed to complain about the performance of recommendation algorithms. These proposed regulations in Russia relate to social networks and video hosting, as the two most popular segments with consumers. All platforms that use recommendation services will be required to make them transparent. Moreover, the draft law should prevent the manipulation of public opinion on the Internet and allow users to reject recommendations. According to the author of the draft law, the deputy chairman of the Committee on Information Policy of the State Duma of the Federal Assembly of the Russian Federation Anton Gorelkin, the most controversial point was the one that should oblige services to provide the technical possibility to refuse to use recommendation technologies in whole or in part, at the discretion of the company.[64]

3. Transparency Requirements for Artificial Intelligence in Algorithmic Recommendation Systems: Legal Challenges

We need to go back to the practice of digital platforms in order to see the general patterns revealed by the systems today. The recommendation algorithms of different systems work on similar principles. And this can be indirectly established by the descriptions of the technologies that can be found on the resources of the software operators. A comparison of the operating principles of artificial intelligence systems such as Amazon Recommendation (which creates a recommendation system to show the most appropriate products), Palantir (which creates a system that allows one to determine indirect connections between companies, based on data from a large number of sources) and Google (which creates a recommendation system to show the most appropriate advertising), has shown that despite such different

---

63 *In Russia, Recommender Algorithms*, *supra* note 43.

64 В России предложили частично отменить рекомендательные алгоритмы интернет-сервисов // Habr. 19 мая 2022 г. [In Russia, they proposed to partially cancel the recommendation algorithms of Internet services, Habr, 19 May 2022] (Feb. 2, 2023), available at https://habr.com/ru/news/t/666574/?ysclid=l45l9avxr9771982202.

fields, recommendation systems based on artificial intelligence use similar criteria for processing information about the user:

• items and services purchased in exchange for real payments (for example, Amazon Recomendation, Palantir and L'Oreal create a system to select the most appropriate cosmetics for a customer based on their previous purchases);

• products added to lists but abandoned (e.g. Amazon Recommendation, Palantir, NLP Architect and Phillips create recommender systems to determine the most suitable devices for the user and Netflix creates a system to recommend the most suitable series and movies to the user);

• referral sites (such as Amazon Recommendation, Palantir, NLP Architect, L'Oreal, Netflix) to expand the user's view of other interests and the number of items viewed before the final transaction; and

• search session time (Amazon Recommendation, Google, NLP Architect, Netflix) among other criteria.

To ensure consumers' and couriers' rights to information, the China-based delivery platform Meituan Waimai, (美团外卖) in November 2021, published on its website the working mechanism, basis and scheme of the planning and decision-making algorithms used to organize delivery routes, allocate orders and determine time, making it intuitive and directly guaranteeing transparency of the relevant algorithms.[65]

In addition, recommender systems are used for so-called pricing experiments (like A/B testing, etc.) in which the same products are offered at different prices and the results are analyzed (for e.g. Palantir, NLP Architect); "packaging experiments" where different products are offered in different "bundles" or have discounts on different item pairs and experiments with "wish lists" to analyze user data flow.

Surveys conducted to rate or rank the user or his or her community or social environment create an information environment that is shaped by positive content, allowing you to learn the details of the user's personal life even beyond the immediate operations on the platform and create a very complete profile of the subject.

In order to test the hypothesis about the usefulness and effectiveness of the disclosure of the recommendation algorithm, let us turn to the experience of the Russian consumer goods and services aggregator, Ozon, which has demonstrated the openness of its platform.[66]

Recommendations on Ozon are a set of widgets on the site and in the app that display a selection of products that may be of interest to the user. Ozon's recommendation system is responsible for selecting products that are relevant to

---

[65] Meituan Waimai publishes algorithms for "order allocation" to comprehensively enable tripartite collaboration [美团外卖公布"订单分配"算法，综合保障三方体验] (Feb. 2, 2023), available at https://new.qq.com/rain/a/20211107A08WP400.

[66] Алгоритм рекомендаций на Ozon [Recommendation Algorithm on Ozon] (Feb. 2, 2023), available at https://docs.ozon.ru/legal/algorithms/recomendation-algorithms/.

the context in which the widgets are displayed. Recommendations can be divided into two groups: product recommendations and personal recommendations.

How does the AI algorithm function? For example, one of the options is dedicated to selection of candidates.

The recommendation service selects several thousand candidates among Ozon (Russia's leading multi-category e-commerce platform) products that are relevant to the context of showing recommendations. Similar goods are selected in the same category as the current product. Related products are products from those categories that are frequently purchased together with the current product. For the personal recommendation widget, the product categories in which the user bought or looked at the products are analyzed.

After the selection process, it is necessary to rank the candidates. The selected 2,000–3,000 items are ranked according to the user's purchase probability. The ranking of these items depends on the attributes that the machine learning model deemed important. As a result of the ranking, each item is scored from 0 to 1.

The score obtained in the previous step is increased for the product if it is one that is also being promoted. Advertising promotion is the purchase of a boosting coefficient for money.

The top products may be similar, so no more than two products from each category are selected in the final listing.

Finally, depending on the widget, anywhere from 3 to 200 items selected in the previous step will be added to the recommendations.

In China, the information about the algorithms provided to the authorized bodies for registration is more detailed than the information disclosed to the public in order to achieve "transparency of the aquarium."[67] The authorized bodies, which receive the basic secrecy of the algorithms, also have a statutory duty of confidentiality, which can effectively eliminate the doubts of entrepreneurs about the improper disclosure of trade secrets due to the registration of algorithms and the occurrence of unfair competition by a third party. In addition, in practice, authorized authorities may also use the 'self-assessment report on algorithm' to clarify, supplement and expand the requirement for specific information to be registered, in order to avoid the algorithm recommendation service provider from refusing to provide the necessary information, such as the scope of the algorithm, the service user, the risk level of the algorithm and so on, on the grounds that there is no clear statutory provision.

Through the research, it was revealed that despite the significant steps in the development of legal acts that were taken by legislators in different countries, all of which were taken in the same direction, unsolved problems persist.

First, we noticed that recommendation algorithms are constantly improving and changing, becoming more complex and non-obvious. The legal requirement for transparency cannot be satisfied by a one-time publication of the principles of

[67] Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 1(6) Admin. L. Rev. 71 (2019).

the system. The problem is that algorithmic transparency strives to constantly learn to adapt to context in addition to acquiring the capability to detect the source of data flows used and generated by AI systems, to display and precisely recreate the mechanisms by which these models make certain decisions. Consequently, a legal mechanism for regular auditing of systems is required. It is necessary to regularly update the information disclosed.

Second, it is evident that at the legislative level, it is not possible to establish exactly what information should be required to be disclosed. According to the fundamental reasoning, there is no "one size fits all" solution. The "main parameters" that must be disclosed must be determined by the providers on a case-by-case and service-by-service basis.[68] A possible solution would be to establish best practices for platform or entire industry disclosure of recommendation systems principles.

This could mean a sort of a "right of explanation" under the General Data Protection Regulation (GDPR).[69] It is unclear, however, whether such an "explanation" should cover a specific algorithmic component that influences the decision or whether it should cover the entire operation of the algorithmic system.[70]

Finally, the most acute problem today is the collision between the rules on transparency of recommender systems and preserving the commercial secrecy of the digital platform. As stipulated by the Trade Secrets Directive, a trade secret is information which meets three requirements (Art. 2(1)): (a) it is secret; (b) it has commercial value due to its secrecy and (c) it is subject to reasonable steps by the information holder to keep it secret.[71] Insofar as algorithms are bits of information, particularly instructions, intended to carry out a production-related task, they may be categorized as trade secrets. As long as they meet the aforementioned criteria, algorithms can be protected as trade secrets and thus fall under the description.[72] It can be said that the Chinese authorities have also taken a prudent stance in balancing the management of algorithms and the protection of commercial secrets. In Russia, the disputes over these issues are only now starting to gain momentum.

In other words, experts have only to assess from a legal perspective the prospects of preserving the commercial information of digital platforms as opposed to ensuring the public interest in the openness of recommendation algorithms.

---

68 Giovanna Di Toro, *Algorithmic Transparency between Legal and Technical Issues* (2021).

69 Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-making Does Not Exist in the General Data Protection Regulation*, 7(2) Int'l Data Privacy L. 76 (2017).

70 Gianclaudio Malgieri, *Automated Decision-making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations*, 35(5) Computer L. & Sec. Rev. (Article 105327) (2019).

71 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

72 Di Toro 2021.

Thus, a number of different states have recognized the problem and are approaching it from different positions. Each region chooses what to prioritize in terms of the law. We can see that for China and Europe, all areas of platforms are important; for Russia, news platforms and video hosting are of interest and for India, primarily social media. However, in all of the countries, the requirements for the disclosure of the recommendation engine to a certain extent are expanding. Both the volume of open information and the order of its disclosure differ. Thus, this study demonstrates the commonalities and differences in the approaches of different countries.

Conclusion

It is now clear to lawmakers and politicians worldwide that government and public intervention in the operation of recommendation algorithms is unavoidable. The choice is between the law and the practices of companies in the order of self-regulation. Most likely, the middle way will be justified when the Codes of Ethics and industry standards continue to be applied against the background of the adoption of the law. We should not expect the legislature to completely reject recommendation systems, as this will have a negative impact on the processes of services. But even excessive additional regulation in the context of already existing requirements in the field of personal and big data may lead to a loss of consumer value for such services by making the process of developing and maintaining such systems more complicated and expensive.

Acknowledgements

This paper was written as part of the 2021–2024 research project: "The Rule of Law in the Digital Economy in China and Russia: Current State, Challenges and Future Development" (The Russian Foundation for Basic Research and the Academy of Social Sciences of China supported this research via grant No: 21-511-93004\21 KAOH_a).

References

Adomavicius G. & Tuzhilin A. *Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions,* 17(6) IEEE Transactions on Knowledge and Data Engineering 734 (2005).

Alt R. *Electronic Markets on Digital Platforms and AI*, 31(2) Electronic Markets 233 (2021).

Bodo B. et al. *Tackling the Algorithmic Control Crisis – The Technical, Legal and Ethical Challenges of Research into Algorithmic Agents*, 19 Yale J.L. & Tech. 133 (2017).

Bonina C. et al. *Digital Platforms for Development: Foundations and Research Agenda*, 31(6) Information Systems Journal 869 (2021).

Coglianese C. & Lehr D. *Transparency and Algorithmic Governance*, 1(6) Admin. L. Rev. 71 (2019).

Constantinides P. et al. *Introduction–Platforms and Infrastructures in the Digital Age*, 29(2) Information Systems Research 381 (2018).

de Gemmis M. et al. *Content-Based Recommender Systems*, in Ricci F. et al. (eds.), Recommender Systems Handbook (2015).

Di Porto F. & Zuppetta M. *Co-regulating Algorithmic Disclosure for Digital Platforms*, 40(2) Policy and Society 272 (2021).

Di Toro G. *Algorithmic Transparency between Legal and Technical Issues* (2021).

Diamond E. *Distrust & Antitrust: Using Facebook to Understand Competition Law's Role in Regulating Data and Data Privacy Concerns Around the World*, 45(5) Fordham International Law Journal 873 (2022).

Gama J. et al. *A Survey on Concept Drift Adaptation*, 46(4) ACM Computing Surveys 1 (2014). https://doi.org/10.1145/2523813

Gillespie T. *Governance of and by Platforms,* SAGE Handbook of Social Media 254 (2017).

Göldi A. *A Blind Spot for the Dark Side: The Monopolies We Didn't See Coming*, 30(1) Electronic Markets 55 (2020). https://doi.org/10.1007/s12525-020-00402-x

Just N. & Latzer M. *Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet*, 39(2) Media, Culture & Society 238 (2017).

Kahneman D.A. *Perspective on Judgment and Choice: Mapping Bounded Rationality*, 58(9) The American Psychologist 697 (2003).

Kharitonova Yu.S. et al. *Artificial Intelligence's Algorithmic Bias: Ethical and Legal Issues*, 53 Perm University Herald. Juridical Sciences 488 (2021).

Kumar A. & Jha A. *Information Technology Rules*, *2021 of India in Dock! A Critical Evaluation of the Guidelines for Intermediaries and Digital Media Ethics Code*, 20(48) Global Media Journal 1 (2022).

Malgieri G. *Automated Decision-making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations*, 35(5) Computer Law & Security Review (Article 105327) (2019).

Marsden C. et al. *Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation?*, 36 Computer Law & Security Review (Article 105373) (2020). https://doi.org/10.1016/j.clsr.2019.105373

Otto B. et al. *Information and Data Quality in Networked Business*, 21(2) Electronic Markets 79 (2011). https://doi.org/10.1007/s12525-011-0062-2

Rai A. et al. *Next Generation Digital Platforms: Toward Human-AI Hybrids*, 43(1) MIS Quarterly 3 (2019).

Ramizo G., Jr. *Platform Playbook: A Typology of Consumer Strategies against Algorithmic Control in Digital Platforms*, Information, Communication & Society 1 (2021).

Scardovi C. *Digital for the Greater Good*, in Digital Transformation in Financial Services 187 (2017).

Shelanski H.A. *Information, Innovation, and Competition Policy for the Internet*, 161 University of Pennsylvania Law Review 1663 (2012).

Shin D. *How Do Users Interact with Algorithm Recommender Systems? The Interaction of Users, Algorithms, and Performance,* Computers in Human Behavior 109 (Article 106344) (2020).

Sinha R. & Swearingen K. *The Role of Transparency in Recommender Systems*, CHI'02 Extended Abstracts on Human Factors in Computing Systems 830 (2002).

Song P. et al. *The Ecosystem of Software Platform: A Study of Asymmetric Cross-Side Network Effects and Platform Governance*, 42(1) MIS Quarterly 121 (2018).

Wachter S. et al. *Why a Right to Explanation of Automated Decision-making Does Not Exist in the General Data Protection Regulation*, 7(2) International Data Privacy Law 76 (2017).

Wood A.J. et al. *Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy*, 33(1) Work, Employment and Society 56 (2019).

Zhou L. et al. *Perceived Information Transparency in B2C E-commerce: An Empirical Investigation*, 55(7) Information & Management 912 (2018).

Information about the authors

Yuliya Kharitonova (Moscow, Russia) – Professor, Head, Research and Education Center for Legal Studies of Artificial Intelligence and Digital Economy, Business Law Department, Faculty of Law, Lomonosov Moscow State University (1, Bldg. 13–14 Leninskie Gory, GSP-1, Moscow, 119991, Russia; e-mail: sovet2009@rambler.ru).

Namita Singh Malik (Greater Noida, India) – Dean and Professor, School of Law, Galgotias University (e-mail: namitasmalik@gmail.com; namita.malik@galgotiasuniversity.edu.in).

Tianfang Yang (Shenzhen, China) – Lecturer, Sino-Russian Comparative Research Center for Law, Shenzhen MSU-BIT University (No. 1, International University Park Rd., Dayun New Town, Longgang District, Shenzhen, Guangdong Province, 518172, China; e-mail: danilyep@mail.ru).

COMMENTS

'POWER' AND TECHNOLOGICAL MACHINES: DREAMS ARE REPLACED BY GOAL-SETTING

IGOR ISAEV,
Kutafin Moscow State Law University (MSAL) (Moscow, Russia)

SERGEY ZENIN,
University of Tyumen (Tyumen, Russia)

VALENTINA RUMYANTSEVA,
Kutafin Moscow State Law University (MSAL) (Moscow, Russia)

https://doi.org/10.21684/2412-2343-2023-10-1-171-185

Modern technologies are rapidly changing the customary forms of being and reshaping the activities of social institutions. This transformation is accompanied by a belief in a long period of sustainable progress brought about through the media, the Internet, mobile telecommunication, robotics and artificial intelligence. Previously, science fiction as a literary genre served as an impetus for science and technology, today, the exact opposite is happening, i.e., scientific and technological breakthroughs inspire a variety of fantastic plots. The problem of gaining a scientific understanding of the mechanization of civilization has become a reality. Machines and technologies influence politics by some means or another. Previously differentiated forms of "the political" also show tendencies towards convergence and interpenetration. In this process, neutral technology tends to exhibit globalism, spreading its influence and its results to the whole world. Rationalization, without which techniques and technologies are unthinkable, revolutionizes the environment by offering its own logic and language to public and individual consciousness. As a result of the pacification of the irrational, structures of power and law frequently find themselves in a situation of isolation that is characterized as "lacking spirituality" and outside the interests of society. The technical elements are increasingly replacing the human elements. Formerly held humanitarian and organic ties are being replaced by technical, ethically neutral methods. Every "power machine"

wants to appear impartial and objective in its actions and decisions; yet, even though the machine has no fate, it cannot avoid accidents. The tendency to evaluate everything in terms of numbers – both infinitesimally small and infinitely large can be traced back to antiquity. Machinery needs an accurate calculation of probabilities: it focuses on foresight; therefore, it embodies a "process" and cares not about tradition, but only about the stability of the system. The machine begins to live for itself and for its future.

Keywords: politics; power; force; rule; dominance; subordination; management; control; state; society; law; technique; technic; machine.

Recommended citation: Igor Isaev et al., *'Power' and Technological Machines: Dreams Are Replaced by Goal-Setting*, 10(1) BRICS Law Journal 171–185 (2023).

Table of Contents

Introduction

The Mesopotamians associated authority with the power inherent in command. The first great victory of the gods over the forces of chaos, the victory of the forces of activity, was won not with the help of physical strength but precisely with power (the power of order, the magic of spells). All subsequent technical revolutions have covertly or openly used this method of influence, despite the changes in forms and conditions that accompany and determine the evolution of the megamachine itself and the ambitious claims of scientific and technical newspeak.

Techniques of power cannot be called static as they lack clear structures; rather, they are constantly changing under the influence of a large number of factors.[1]

[1] *Фуко М.* Безопасность, территория, население [Michel Foucault, *Security, Territory, Population*] 177 (2011).

A significant role here is played by the time factor or the obsolescence of the system, when it ceases to adequately respond according to the "call-response" model. The technical system expresses internal compatibility by equipping society for each era and without regard to any boundaries; whereas the cultural system provides, within the framework of a given society, a pre-existing sense of cohesion in the time interval between its past and present.

The first industrial revolution (the revolution of "dark satanic factories") devalued human hands due to the competition of machines. The monotonous repetition of actions inherent in machine technology and their calculation formed the quality of imperativeness – an integral component of any power or any order. Thus, power appeared to be freed from the emotional and ethical layers that it previously possessed and continued to exist in the sphere of pure technology. The motto of the "power machine" could well be summed up as: "power works like clockwork." The modern industrial revolution is devaluing the human brain, at least in its most basic and mundane functions.

1. Literature Review

The results of the conducted literature review are presented in the form of a table that lists researchers and features of their understanding of the concept of power and technological machines, as shown in Table 1 below.

Table 1: **Literature review**

Researchers	Features of the concept
Alain de Benoist	Politics can exist only to the extent that there is a choice between different possibilities, between different goal-settings. Management seeks to abolish such a choice by reducing social and political problems to technical ones, which have only one optimal solution that is assumed to be universally recognized
Max Weber	As experience shows, the most rational form of domination is bureaucratic management. Due to its qualities, it is universal for solving any problem and is inexhaustible in terms of purely technical improvement
Dean Mitchell	Since the 20th century, management has become more diverse (many agents introduced into the game by different strategies), diffused, optimized and empowered, nevertheless, in a strange way and more disciplinary, strict and punitive

Lewis Mumford	Technique today is an example of monotechnics: based on scientific achievements and skilled production, it is mainly focused on economic expansion, material saturation and military superiority. The roots of monotechnics date back to antiquity, when a man discovered a megamachine – a strict hierarchical social organization (e.g., large armies, associations of workers into groups)
Paul-Michel Foucault	The disciplinary techniques of power are able to control many people, turning them into individual bodies (to increase useful power), subject to supervision, training, use and punishment
Friedrich Jünger	The machine visibly manifests the human mind in its most basic form. This constructive, articulate mind acquires and accumulates more and more power, tirelessly gaining new triumphant victories over the elements, crushing and shaping them at will

2. Methods

The methodological basis of the article was formed by the principles of cognition of social phenomena in their historical development and at the same time, in interconnection and interdependence from the point of view of the connection between history and modernity.

The description of the process of mechanization of mankind requires the application of a dialectical method. According to this method, development depends on the collision of contradictions and the emergence of knowledge about facilities and technology in a society of a higher order as a result of this collision. Based on the historical and legal, historical and political, and comparative and legal analyses, it is possible to identify any new developments that arise in the course of interaction between the state, law, society and politics.

In order to identify the features of the nature of the power machine, as well as to reflect an interdisciplinary approach, the following methods are used: legalistic, systemic and structural, functional, mathematical, cybernetic, historical, sociological, psychological, etc.

An analytical study of issues related to the strengthening of the dominance of the power machine involves a combination of methods, including theoretical and legal abstraction, hypothesis, thought experiment and social modeling.

3. Results

3.1. "Machinization" of the Social

The concept of the term "technique" (in contrast to the Greek "techne," meaning art, skill or ability) denotes both a machine and the process of its functioning. When applied to the political sphere, the term "technical" refers to something ideologically neutral and beyond the boundaries of the moral and ethical.

The "technique" is limited, enclosed in the sphere of the lifeless:

• the reason, which controls technical activity, is proportional only to something mechanical;

• the technique can affect the living only when it turns into something inanimate.

Hence, there exists the demonization of technology. Created by people, it is transformed into something overwhelming, dominant, opposing and unknown.[2] The socio-technical dynamics can comprise the following:

• The 17th and beginning of the 18th centuries are referred to as the age of clocks.

• The 19th century is known as the age of steam engines.

• The 20th and early 21st centuries are regarded as the age of communication and control when information and its derivatives dominate and start to impose a desirable way of thinking.

The technique and machines themselves have emerged as the "New Heroes of the Socio-Political Space."[3] Everything is built on the model of a machine that has the properties of seductive rationalism, which include:

• accuracy;

• predestination of actions;

• bound by external rules.

The imperious aspirations of technology are also aimed at subjugating the state. The latter is appealing specifically because of its well-coordinated organizational structure.

The state evolved into a technical apparatus whose power acquired a predominantly organizational and managerial character. Michel Foucault, in a historical study of the techniques of power, names three major forms of a state:

• the "state of justice," which arose within the framework of the territoriality of the feudal type and, in general, corresponds to the society of law, both customary and written law;

• the administrative state (15th–16th centuries, but not feudal) within a territoriality determined by borders, which corresponds to a society of regulation and discipline;

---

[2] *Ясперс К.* Смысл и назначение истории: сборник [Karl Jaspers, *The Meaning and Purpose of History: A Collection*] 131–37 (1994).

[3] *Ленк Х.* Размышления о современной технике [Hans Lenk, *Reflections on Modern Technology*] 81 (1996).

• the state of governance, which is determined not by territoriality, but by the mass, size and dynamics of the population.[4]

The social machine is an aggregate of technical machines. Meanwhile, the difference in the nature of machines remains distinct, despite the fact that both are machines in the proper sense of the word. The social machine receives its information in the form of technical machines, but its axioms are not those of a simple technical machine (automatic or cybernetic) but include intuition. This is one of the reasons why the system of power is not reduced to the functioning of technical machines and that its organs create decisions, control and reactions in addition to its own unique technocracy and bureaucracy.[5]

Detached from the meaning of life, technology can turn into "a means of violent madness of non-humans and the entire globe can become a giant factory."[6] Thus, technology changes a person, making them dependent on themselves. In the process of expanding industrialization, our work activity is being transformed. Power leads to the institutionalization and identification of the individual. Ernst Junger describes the myth of the worker in the following ways:

• as an allegorical reflection of the technocratic era;

• as a metaphor for a person's aspirations to obey the original idea of labor, that is, the dominant ethical and state principle.[7]

A person integrated in the power machine and unable to get out of it turns into a function without properties or individuality. Being in the body of the social (people), he or she is like a cog in a mechanism. Even the Enlightenment – the Great Age of Reason – made a significant ideological contribution to genetic engineering by applying it to social technologies.[8] It was intended to create a new person, humane and fair. Thus, the very concept of 'the political' appears, taking on the functions of the social.

Politics finally becomes a technique:

> political action is required to represent the reality behind it as best as possible, to be transparent and to be moral and consistent with the social ideal of correct representation.[9]

---

[4] Foucault 2011, at 164.

[5] *Делёз Ж., Гваттари Ф.* Анти-Эдип. Капитализм и шизофрения [Gilles Deleuze & Félix Guattari, *Anti-Oedipus. Capitalism and Schizophrenia*] 396–97 (2007).

[6] Jaspers 1994, at 139–40.

[7] *Юнгер Э.* Рабочий. Господство и гештальт. Тотальная мобилизация. О боли [Ernst Jünger, *The Worker. Domination and Gestalt. Total Mobilization. About the Pain*] 55–429 (2000).

[8] *Бек У.* Общество риска. На пути к другому модерну [Ulrich Beck, *Risk Society. On the Way to Another Modern*] 21 (2000).

[9] *Бодрийяр Ж.* В тени молчаливого большинства, или Конец социального [Jean Baudrillard, *In the Shadow of the Silent Majority, or the End of the Social*] 24–25 (2000).

Strict functions and mechanisms of power and subordination arise in the social space. Even liberal regimes can readily assume the position of a "good despot" in order to restrict, coerce and intimidate, if only as a preventive measure.

3.2. The "Power Machine" and the Law

The technological revolution creates new social (including industrial, cultural, etc.) objects, relationships and statuses of various kinds. The legal field was formed as a result of the overall process of technological progress. New legal institutions appeared spontaneously rather than systematically and thoughtfully. The actual technical and technological needs gave rise to the creation of a significant number of carefully detailed instruments, regulations, instructions and prescriptions.

Evolving technology changes the goals and essence of the legal organization itself. The technician subordinates the logic of natural law to technical logic,

> everywhere brings to the fore precisely the material side of the law and replaces law, expressed in the form of laws, with technical prescriptions. The boundless growth of legal matter is connected with this: it seems that some kind of machine is working, producing laws and regulations ... The technician is fighting against the ability to interpret things inherent in jurisprudence.[10]

The law serves its own technical purposes.

Over time, the law increasingly resembles a norm. The role of the law (an instrument of sovereign coercion) is lost and then reappears in the form of a normative power:

• A law is not a product of someone's specific will; it does not stem from the will of the sovereign but organically grows out of the community, providing a social group with sovereignty based on a standard (not a social contract), i.e., values that are attached to the group and subject to change.[11]

• Laws are gradually concretized and turned into orders.

> If the leader in every case prescribes every detail of the action, his people will be mere tools, deprived of the opportunity to use their own knowledge and judgment, so that only the goals chosen by the leader will be pursued, and only the knowledge that he possesses will be used.[12]

---

[10] *Юнгер Ф.* Совершенство техники. Машина и собственность [Friedrich Junger, *Perfection of Technology. Car and Property*] 137–139, 384–385 (2002).

[11] *Митчел Д.* Правительность: власть и правление в современных обществах [Dean Mitchell, *Governmentality: Power and Governance in Modern Societies*] 300–01 (2016).

[12] *Хайек Ф.* Конституция свободы [Friedrich Hayek, *The Constitution of Liberty*] 189–90 (2018).

The vast majority of laws are, in essence, instructions issued by the state to its servants outlining how they should direct the apparatus and what means will be at their disposal for this purpose. Technical normalization, under the guise of a discourse of neutrality and management technique, seeks to abolish this political dimension. This is how legal norms are replaced by technical ones.

Legal technique, as a technical prescription, is both dispositive and causal in nature. It turns out that the technical norms, in their rationality of presentation, are more suited to the actual state of affairs than any other norms. In certain legal systems (for example, in the Soviet law of the 1920s), technical organizational norms were seen as a desirable model for emerging laws, while legal norms were accused of ideological distortion of reality.

The imperative nature of the law is in itself normative: the law addresses the norm and is called upon to codify it. Alongside the system of law, within its depths and frameworks (albeit in the opposite direction), are developed the techniques of normalization produced by the discipline. The distinction between normal and abnormal is established by agreement with the norm or lack thereof. Michel Foucault calls such actions normalization, "to emphasize that it is the norm that determines here."[13] Normalization does not depend on direct coercion, but rather on an external sense of guilt and self-censorship: the holder of power does not need to give orders, as they are carried out regardless of who gave them.

Norms seek to replace the law as a mere prescription suited to the case and dictated by technical arguments, and the principle of contractual relations is preferable to the principle of legality.

> To this end, the law as a way of constructing policy is being replaced by agreements on the ground. In legislative activity, general principles, norms, rules and procedures, as well as framework directives, are preferred.[14]

Regulatory prescriptions, according to Gary Becker, arise from tradition, but at the same time they can be artificially organized into codes; "such orderliness at least has the appearance of some kind of deductive systematization." In reality, however, it is often limited to only external similarity. In this case, the system is merely a "rough sequence of the catalog, determined by the succession of historical events and the convenience of remembering."[15]

---

[13] Foucault 2011, at 89.

[14] *Бенуа А.* Против либерализма: (к Четвертой политической теории) [Alain de Benois, *Against Liberalism: (To the Fourth Political Theory)*] 246–47 (2009).

[15] *Беккер Г.* Современная теория священного и светского // Современная социологическая теория в ее преемственности и изменении: сборник [Howard Becker, *Modern Theory of the Sacred and the Secular*, in Modern Sociological Theory in its Continuity and Change: A Collection] 181–183 (1961).

Legal norms give rise to institutions that need to be formalized, for which they themselves create even newer forms. The process seems endless. This is the fate of the technological revolution and the accompanying legal revolution.

Law progressively turns into an instrument of domination, which entails new relationships, i.e., or put another way:

• not the domination of the king, which played a central role in the state, but rather the domination in the mutual relations of subjects;

• not the domination of the supreme power in its uniqueness, but of the numerous existing forms of subordination.

Technique serves the social and political mechanisms, allegedly providing unanimity and law and order. The perfection of such techniques by no means replaces the need for goal-setting, which may or may not be based at all on the arguments of technical reason. Power functions on the other side of the law, embodied in the institutions of violence, and extends beyond the framework of the rules of law that organize and limit it.[16] When law implements technology, it can even serve entirely different purposes and roles.

The system of law turns out to be a permanent bearer of relations of domination and diverse technical forms of subordination.

4. Discussion: Dominance and Subordination Mechanisms

4.1. The "Power Machine": Management and Control

The technological revolution has raised many new problems and opened up many new ideas. The emerging pluralism (which found a response in the ideology of economic and political liberalism) required a revision of the basic principles, logic and metaphysical foundations of science and social life. In the first phase of European modernization, there was a confident demystification of traditional ranks and hierarchies.

Reason and rationality, based on technology (Julien de La Mettrie perceived the human as a machine), replace the Creator, from whom they take on the functions of managing the world:

• Space is a huge debugged machine.

• Management, being a special function, approved a certain non-authoritarian political model, which was attractive if only because of its systematic and universal goal-setting. It could be virtual world management.

The economic and political liberalism that accompanied the Industrial Revolution rejected the coercive techniques of sovereignty in favor of an equally rigid form of disciplinary governance. Jeremiah Bentham invented the concept of a strange and

---

[16] *Фуко М.* Нужно защищать общество: курс лекций, прочитанных в Коллеж де Франс в 1975–1976 учебном году [Michel Foucault, *We Need to Protect Society: A Course of Lectures Delivered at the Collège de France in the 1975–1976 Academic Year*] 46 (2005).

monstrous panopticon – an ideal prison in which control and police functions are carried out in an absolute and extreme form. The welfare state, as envisioned by Jeremiah Bentham, was born as a paternalistic mechanism of social control based on uniform provision (bureaucratic, hierarchical, sometimes coercive and despotic).

Serious changes are taking place in the field of political law itself. In addition to the old right of supreme power (to force to die or to allow to live), a new right began to operate (to force to live and allow to die), which did not destroy the first but penetrated into it, permeated it and formed a new power relationship:

• The issue of the right to life and death was first raised by lawyers in the 17th and 18th centuries. Sovereigns were established by a contractual act so that they themselves would then grant the right to live.

• Now, those very techniques of power are focused on the "individual body": all procedures that ensure the spatial distribution of individual bodies (their separation, alignment, establishment of their serialization and control over them), as well as the entire system of observations of them. These were techniques where the authorities took charge of these bodies, trying to increase their usable strength through training. This also includes the techniques of rationalization and austerity of power (since the end of the 18th century, a real disciplinary technology of labor has been established[17]).

As an assessment tool and a response to the new challenges of the emerging new democracy, governance still retained and established a certain postmodern form of authoritarianism: the people and deputies, who were the main actors in representative democracy in the 19th century, have been replaced by a new pair, namely, experts and members of civil society (who outline the boundaries of legitimate decisions and fill the essence of political power). The state, as it were, concludes a virtual contract with civil society. Its activities are subject to the requirements of society, but it still retains power, and the fading of its influence coincides with the increase in its power – "the state receives this power and legitimacy on the condition that it ensures security and welfare."[18]

The era of machinery and automation will further emphasize the need to combine management and control functions. Management proceeds from an unprovable premise with the goal of improving the situation in the future; it is carried out for obviously good purposes, but this is a forced "path to happiness." In any case, to manage means to lead. On this path, liberal movements quickly acquire the features of traditional authoritarianism in order to overcome misunderstandings on the part of their followers. The machine does not tolerate uncertainty. Thus:

• Discipline is the foundation of the building of power, the top levels of which are occupied by state power, and the support is provided by the rules of internal order (typical for such institutions as prisons, schools and armies).

---

17 Foucault 2005, at 255–256.

18 Benois 2009, at 257–258.

• Individuals are equalized, instructed, separated, registered and controlled ("carried out by disciplinary coercion and normalization"[19]).

The political instability that is inevitable in a democracy is giving way to the stability of technical administrators. Politics, which supposedly should eliminate conflicts in society, turns out to be somewhere between morality and economics. However, "the transformation of political problems into technical ones brings only a new kind of coercion, since it implies the suppression of choice itself."[20]

From the point of view of liberal technology and management rationality, in the 20th and 21st centuries, the ruled can participate in the election of managers since management, figuratively speaking, is created on the basis of the individuals themselves. As a result:

• The individual is present as a norm and standard for governing and for being governed.

• The institution of representation is only a managerial response to the democratization that has taken place, a guarantee of cutting off the ruled from the managers.[21]

The truth no longer resides in the center of the state, and the law ceases to be understood only by the arbitrary establishment of the sovereign. Discipline has been proven to be capable of controlling all people, since this multitude could and had to turn into individual bodies subject to supervision, training, use and punishment.

Dreams had to be replaced by goal-setting.

4.2. The "Power Machine": Impersonal Management

The techniques of domination and coercion isolate and correct social elements, uniting into a single complex that expresses the all-conquering machine of power in the political space.

Politics is always action, and technology is also personified, embodied action. In contrast to politics, the concept of authority is alien to technology; only calculation and effectiveness matter here. The political, perceiving such goals, itself turns into a technique. In addition, the technical is also characterized by a certain "democratism," an "equality" of parts and details, which alone is capable of ensuring balance in the technical system. Technique in politics is not capable of anything other than building up or easing tensions, strengthening peace or war – unlike us, it is ready for both:

> Today we are penetrating through the fog of names and words with which the psychotechnical machinery of the mass suggestion ... Spirit fights against

---

19 *Самарская Е.А.* Вместо предисловия [Elena A. Samarskaya, *Instead of a Preface*] in Foucault 2005, at 8.

20 Benois 2009, at 241–243.

21 Mitchell 2016, at 304–305.

spirit, life against life, and from the power of integral knowledge arises the order of human things.[22]

Technique seeks to introduce its most significant element into the political sphere, namely, organized nature, organization and structured. The unifying effect of technology generates anonymity, or the Impersonal.

The phenomenon of the Impersonal, its dominance, is fully revealed in the bureaucracy. In its environment, it is difficult to find a person responsible for making a decision, despite the fact that the links of the control mechanism are always easy to replace. Thus it follows that:

• "The rationality of the modern organization implies that there is always room for improvement."

• "There is nothing sacred, and, therefore, nothing unchanging. Thus, rationality has a clear tendency to spread from the control of inanimate objects to the control of human relations: it confidently and defiantly intrudes into areas previously governed by traditional and informal norms."[23]

Bureaucratic government (Max Weber calls it the purest type of legal domination[24]) implies domination through professional knowledge, the absolute inevitability of which is due to modern technology. The advantage here is the inexhaustible possibilities of a purely technical improvement of bureaucratic domination, summarized by its following qualities:

• accuracy;
• stability;
• strict discipline;
• reliability;
• predictability;
• intensification;
• versatility.[25]

The bureaucracy seeks to strengthen its positions of power through rationing, which is an integral element of one or more mechanical processes.[26]

---

[22] *Шмитт К.* Понятие политического [Karl Schmitt, *The Concept of the Political*] 368–371 (2016).

[23] *Голднер Э.* Анализ организации // Социология сегодня. Проблемы и перспективы: американская буржуазная социология середины XX в.: сборник [Alvin Gouldner, *Organization Analysis*, in Sociology Today. Problems and Prospects: American Bourgeois Sociology of the Mid-20th Century: A Collection] 467 (1965).

[24] *Вебер М.* Хозяйство и общество: очерки понимающей социологии: в 4 т. Т. 1 [Max Weber, *Economy and Society: Essays of Understanding Sociology. In 4 vols. Vol. 1*] 256 (2016).

[25] *Id*. at 261.

[26] Junger 2022, at 385.

> Great political battles today are battles around the norms, and they are unfolding not in sight of the public and with its indifference. Whoever imposes his own order raises his own local to the level of the universal: thus, the dominance of the standardization of the world is encrypted in impartial, but defining seals.[27]

The activity of a political person consists of three main components: knowledge, desire and regulation, the latter of which is crucial in situations of crisis. Hence, it may be said that:

• Society can survive through a normative response to anomie (anomie is that which goes beyond the jurisdiction of the law);

• Society preserves fragments of the value system around which a new stabilizing crystallization can begin.

Governance ceases to be "a methodology of domination, turning into an economic technique oriented towards" progress "and borrowing basic principles from political economy."[28]

According to Max Weber, the positive aspects of the rationalism of bureaucracy include the following:

• formalism – "otherwise there would be arbitrariness, and compliance with formal requirements is the line of least effort";

• material utilitarianism of officials in understanding managerial tasks – the desire to please the public with their activities.[29]

In this form of rationality, governing is not the same as ruling. Giorgio Agamben states that it is a mistake to equate management and executive power:

> the innermost secret of politics is not sovereignty, but management, not God, but an angel, not a king, but a minister, not a law, but the police – in other words, that managerial the machine they form and maintain.[30]

Management itself can replace the state, because the state is only a "technical tool for achieving managerial goals."[31] Then political procedures turn into purely administrative ones; "global management is carried out through local types of management, starting from the field of economics, technology and finance and

---

[27] *Дебрэ Р.* Введение в медиологию [Régis Debray, *Introduction to Mediology*] 101 (2010).

[28] Benois 2009, at 255–256.

[29] Weber 2016, at 264.

[30] *Агамбен Дж.* Царство и Слава: к теологической генеалогии экономики и управления [Giorgio Agamben, *The Kingdom and Glory: Towards a Theological Genealogy of Economics and Management*] 453 (2018).

[31] Mitchell 2016, at 374.

ending with politics, everything is imbued with one desire – to transform political procedures into administrative ones."[32]

Perhaps the process of transitioning from the principle of government to the principle of management will still be completed in the end. If the state was once some kind of abstract unity, uniting separately functioning subsystems, in our time it turned out to be subordinate; "as a machine, it no longer defines the social system. It is now itself determined by the social system into which it is included in the play of its functions."[33]

The state serves as the central point of a certain enterprise, an indexing system and an automatic mechanism with functions and functionaries:

• Indexing and technical numbering indicate the disappearance of qualitative and "material" objects and objectivity;

• The enterprise is merely a system of indexing and only appears when objectivity disappears.[34]

The digital age is the realm of quantity and anonymity, manifested in management. It appears that the Impersonal rules in it. In reality, this is a hypothetical unity of very real public interests, and it rules no less despotically because it is not tied to any particular person.

Thus, for the machine of power, the process is the goal, and the construction is the means. As a result, the bureaucracy that exists in this situation is only a means and an instrument. The Impersonal and neutral turn into immoral. Inadequate perceptions of reality turn out to be a pattern for the management apparatus. As described in Serena Kierkegaard's *Fear and Amazement*, Kafkaesque hopelessness is not just a mood but a reflection of social reality.

Conclusion

In the wake of the technological revolution, technology is gradually breaking away from the Greek term "techne" and transforming into a tool for constructing a new reality. Artificiality now becomes quality.

Technique intervenes in the field of state administration, introducing its causal mechanism here and extending its inherent and desired automatism to relations of a completely different kind. Man is the object of mechanical coercion. The influence of technology becomes all-encompassing and penetrating.

The machine of power is devoid of sentiment; its evaluation relates exclusively to predictions of efficiency and quantity necessary for its operation, which can be summed up as:

---

[32] Benois 2009, at 246–247.

[33] Deleuze & Guattari 2007, at 348–349.

[34] *Юнгер Ф.* Язык и мышление [Friedrich Junger, *Language and Thinking*] 53–57 (2005).

• reliable, stable, long-lasting, ideally eternal (hence the perpetual motion machine);

• carefully organized mechanism that allows clear instructions to be given and carried out from "the headquarters of the power machine."

The state is changing from the dynastic to the bureaucratic type and moving away from the personal toward the impersonal.

Technique has finally incorporated us in its algorithm of existence and mentality. By smoothly organizing its life, society turns into one big machine. The machine materializes the body in a state of motionless regularity, turning the spiritual elements into matter in the process. Paradoxically, in the depths of political structures, there appear both huge machines of destruction and those designed to take care of individual life.

Technique emasculates all that is truly human, albeit irrational, achieving the greatest efficiency and demonstrating its rationality and organization in business. The task of overcoming technology through technology is unattainable. In this situation, technical troubles can only intensify, and therefore, fortunately, absolute technocracy is unattainable.

Acknowledgement

This article was created within the framework of the scientific project No. 18-29-16124 of the Russian Foundation for Basic Research (RFBR).

References

Dean M. *Governmentality: Power and Rule in Modern Society* (2009).
Deleuze J. & Guattari F. *Anti-Oedipus: Capitalism and Schizophrenia* (1977).
Hayek F. *The Constitution of Liberty* (1960).
Weber M *Economy and Society: An Outline of Interpretive Sociology* (1978).

Information about the authors

Igor Isaev (Moscow, Russia) – Professor, Head, Department of History of State and Law, Kutafin Moscow State Law University (MSAL) (9 Sadovo-Kudrinskaya St., Moscow, 125993, Russia; e-mail: kafedra-igp@yandex.ru).

Sergey Zenin (Tyumen, Russia) – Associate Professor, Director, Institute of State and Law; Vice-Rector, University of Tyumen (6 Volodarskogo St., Tyumen, 625003, Russia; e-mail: zeninsergei@mail.ru).

Valentina Rumyantseva (Moscow, Russia) – Associate Professor, Department of History of State and Law, Kutafin Moscow State Law University (MSAL) (9 Sadovo-Kudrinskaya St., Moscow, 125993, Russia; e-mail: valentinarum@mail.ru).

REVIEWS

REVIEW OF THE MONOGRAPH "LAW OF THE DIGITAL ENVIRONMENT" (TIKHON PODSHIVALOV ET AL. (EDS.), 2022)

ILDAR BEGISHEV,

Kazan Innovative University named after V.G. Timiryasov (Kazan, Russia)

https://doi.org/10.21684/2412-2343-2023-10-1-186-194

In the era of digitalization, a rapid development of technologies takes place in various spheres of human activity. The pace of introduction of these digital technologies is so high that a gap has emerged, and is constantly growing, between the capabilities of digitalization products and the legal regulation of their application and the consequences to which their erroneous or intended use may lead. The applied aspect of regulation of legal relations within the digital environment, caused by the need to operatively react to the rapidly developing digital technologies, is currently to a certain extent outrunning the theoretical one, entailing a number of legal collisions, as only fundamental scientific substantiation of introduction of certain legal norms may guarantee their consistency and legality. Most of the works in this sphere are, undoubtedly, fundamental, but they mainly refer to individual aspects of legal regulation or theoretical substantiation of the large-scale problem under consideration. In this regard, it is acutely necessary to systematize the current experience in substantiating various approaches to the legal regulation of public relations in the digital environment, which would comprise fundamental positions of researchers from different countries. This task was posed by the multi-national collective of the monograph "Law of the Digital Environment," the first large-scale research synthesizing theoretical and practical studies in the sphere of legal substantiation and support of events, phenomena and processes taking place in the digital era. Such work can undoubtedly be called a discovery in the sphere of digital law and an "encyclopedia" of the legal field under study.

Keywords: digital technologies; digital industry; digital law; digital environment; regulation; administration of law; liability; digitalization; artificial intelligence.

Recommended citation: Ildar Begishev, *Review of the Monograph "Law of the Digital Environment" (Tikhon Podshivalov et al. (eds.), 2022)*, 10(1) BRICS Law Journal 186–194 (2023).

Table of Contents

Introduction

Technological progress produces a large effect on many spheres of social and economic life. While this effect is largely positive, bringing new solutions to increase comfort, one should not forget that innovative technologies entail the emergence of new spheres not covered by relevant legal acts. Such situation often occurs due to the lack of adequate legal tools which could be applied. Such issues are most often solved by adequate application of the existing legal acts and formation of new statutes solving the problem.

However, today it is necessary not only to optimize the existing legal frameworks with regard to the emerging new digital subjects of legal relations, but also to boost the development of new legislative approaches in the sphere. This objective can be efficiently and rapidly achieved only if the existing theoretical and practical experience of legal scientists is taken as the basis and further developed. In this regard, the book "Law of the Digital Environment" seems fundamental, and presents the ideas and concepts of authors from Russia, Belarus, Brazil, India, Italy, Slovenia, Malaysia.

1. Authors' Approach to Researching the Theory of the Law of Digital Environment

The authors of the first section of the monograph thoroughly consider the prerequisites of the digital environment development. As the "initial" platform of this branch of law, they state the "emergence and formation of information-communication ecosystems of the internet- and cyberspaces, the Internet as the environment for information circulation." Further, with the emergence of new mechanisms and ecosystems, a need to elaborate and introduce new legal tools arose.

Evaluating the features of development of the legal digital environment, the authors come to the conclusion that the nature of digital environment is complex to define the frameworks of its legal regulation, as the current legislation cannot always be applied to certain legal relations, for example, those implemented in cyberspace.

Considering the object matter of the law of digital environment and the general factors of its development, the authors mark that it is necessary to establish two issues: to define the categories of the law of digital environment from the standpoint of its current state and to form general conceptions of the law of digital environment as a phenomenon of innovative format.

Considering the methodology of law of the digital environment, the authors distinguish a number of typical provisions against the background of analysis of the "methodological features of non-standard forms and instrumental mechanisms in the sphere of legal influence." The researchers come to the conclusion that

> deregulation, co-regulation, information technologies in regulation, new virtual-information means of consolidation and mediation of the processes and links challenge the possibility of formal, solid-legal regulation mechanism and bring to the forefront the methods of non-formalized, soft-legal regulation, based on flexible and broad legal means, associated, inter alia, with the development of digital technologies in regulation.

Considering the issue of the subjects of digital environment, the authors highlight the fact of changing the traditional system of legal subjects, as new subjects appear. As an important aspect, they state that the modern development of robotics and artificial intelligence systems has led to discussing a problem of legal subjectivity and legal status of the "electronic persons" as agents (mediators) endowed with the functions previously performed by humans. However, the legal status of such a person, within which it could be liable for its actions, is still not defined.

2. Correlation Between Digital Reality and Fundamentals of Constitutional Law

The authors introduce the notion of "electronic democracy," which allows implementing the ideas of direct democracy with modern technologies, balances the opportunities of all citizens-Internet users, leaving the field of self-implementation to the most active, and allows the citizens to implement their basic rights in the digital environment.

Researching the issues of digital constitutionalism and the problems of lawfulness of behavior in the Internet, the authors point out that

> the impact of digitalization as the most powerful and all-encompassing process on the society and state requires revealing and systematizing the risks associated with the introduction of relevant information technologies into the sphere of the citizens' participation in state governance. Using the information technologies transforms the institutes of direct democracy, conferring new qualities to them. The influence of modern information technologies on the legal and political reality is diverse and leads to correcting the content of the existing constitutional rights and freedoms.

Also, the monograph considers the correlation between constitutional public initiatives and digital constitutional rights. Researching this issue, with a view of creating constitutional certainty, the authors propose

> to adopt a special Federal Constitutional Law on the forms of constituent power in Russia, stipulating the guarantees of implementing the digital constitutional rights in the sphere of constitutional formation and declaration of will of the citizens.

3. Innovations, Investments and Digital Platforms in the Aspect of Legal Regulation Under Modern Conditions

In this section, the authors consider the so-called models of regulatory sandboxes in the sphere of digital innovations. Their advantage is implementation which allows business subjects to test innovations in a safe environment and minimize the probable harm for consumers, and control bodies – to examine the "functioning" of new technologies "from the outside," in the low-risk environment. The said mechanism is an example of rejection of traditional regulatory approaches for a more flexible regulation.[1]

---

[1] Elizaveta Gromova & Tjaša Ivanc, *Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS*, 7(2) BRICS L.J. 10 (2020); Elizaveta A. Gromova et al., *Preferential and Experimental Regimes in the Sphere of Creation of Biomedical Innovations*, S2 Hum. Sport Med. 161 (2021).

The section also illuminates the legal mechanisms of overcoming administrative barriers in the sphere of digital experimental innovations. The legal solutions, proposed by the authors, are the feasibility of legal experiments pursuant to the "maintenance of the balance of interests of various subjects and ensuring their guaranteed rights and freedoms under modification of the specific legislation."[2]

Considering the current legal conditions of the platform economy, the researchers point out that

> the topical problem today is to elaborate a balanced legal regulation of the activity of digital platforms, providing, with the account of common principles of civil law, their independent functioning, also stipulating liability of their owners to users for the security of the transmitted personal data, proper identification of a user personality, and exclusion of placing unlawful content by users and restriction of their abuse of rights in the sphere of activity of digital platforms.

4. Financial Tools and Legal Realities of Their Application

Discussing the financial tools application, the authors point out that "the modern innovative development stimulates the development of financial technologies, first of all, in relation to the currently existing financial services, among which are various payments and transfers via mobile banking, contactless payments, online services of crediting, insurance, management of assets, financial planning and accruing, algorithmic stock exchange trade, systems of client identification based on biometric data, etc.

The authors discuss the development of normative-legal base of financial tools' digitalization and come to the conclusion that there are certain contradictions in the legislation on this issue, which determines the need to improve normative acts.

Despite the high value of the material presented in this section, the holistic perception of the work is complicated, as the text in sub clauses is not always structured and the stated issues are not clearly highlighted for convenient systematization.

5. Civil-Legal Branch in the Era of Digital Transformation

In this section, the authors highlight the notion of a digital asset. They state that

> a digital asset, linked to an item with not only juridical but also physical links, becomes a phenomenon, with regard to which the subjects start

[2] Elizaveta A. Gromova et al., *Legal Barriers to the Implementation of Digital Industry (Industry 4.0) Components and Ways to Overcome Them*, 25(1) J. World Intellect. Prop. 186 (2022).

> entering public relation, at which their behavior is aimed, or what is thought by the subjects as the object of their behavior. That is why a digital asset, represented as a record in the blockchain ledger, unlike a record of real estate in a cadastre, can be qualified as an independent object of civil rights.

The notion of digital rights is also introduced, which are interpreted as "the object of rights (independent juridical phenomenon) and a juridical construct providing a legal link between the subject and the digital goods as an object of right." Digital law, in the researchers' opinion, must act "as a juridical mechanism consolidating the relations of possessing, using and disposing of digital assets as independent and separate from the subject's personality production means."

Considering the features of including digital assets and digital rights of citizens into civil circulation, the researchers substantiate their differences from other rights and consider the features of their implementation under modern conditions.[3]

Also, the authors consider the place of a smart contract in the pandect system of the Russian civil law and point out that under the forming digital economy such basic digital institutions as smart contract and digital rights must be properly statutorized; otherwise they can hardly be broadly applied. In practical terms, smart contracts require special knowledge and skills, and their actual use is only possible after a profound analysis of technical aspects, legal and economic risks.

6. Digital Technologies in the Contemporary Criminal Law and Process

One of the aspects considered in this section is the analysis of digital crimes against property. The researchers come to the conclusion that

> utilitarian digital rights, digital financial assets and the digital rights (in case of their further legal regulation by a special law) must be considered an object of crimes stipulated by Chapter 21 of the Russian Criminal Code, as their unlawful acquisition entails immediate infringement of direct property harm to the owner.

The authors also examine the features of the criminological model of crimes committed using digital technologies. In their opinion, based on typical elements

---

[3] Tikhon P. Podshivalov, *Improving Implementation of the Blockchain Technology in Real Estate Registration*, 33(2) J. High Technol. Mgmt. Res. 100440 (2022); Maria Bazhina, *Disputable Questions of the Use of Digital Technologies in Transportation*, 1(1) Int'l J. L. in Changing World 33 (2022); Elena Ofman & Mikhail Sagandykov, *Electronic Monitoring for Employees: Employer Rights in the XXI Century*, 23(1) J. Leg. Ethical Regul. Issues (2020) (Jan. 16, 2023), available at https://www.abacademies.org/articles/electronic-monitoring-for-employees-employer-rights-in-the-xxi-century-9605.html.

of criminal activity and taking into account their correlation dependence, one may distinguish the following "elements of a typical criminal model of crimes committed using digital technologies: the object of criminal infringement; the means of committing a crime; the situation of committing a crime; the personality of a criminal."

The monograph raises the question of digitalization of criminal sentencing and the fundamental approaches to digitalization of social systems (to which criminal legal relations refer). Based on various approaches, the authors distinguish the following "prospective directions of programming the procedure of criminal sentencing: method of hierarchies analysis; scoring system of assessment and building relations between the criteria which the law accepts as a basis for just criminal sentencing (found in the behavior of the guilty) and the types and scope of punishment stipulated by Articles of the Russian Criminal Code, via mathematical formulas."

The authors also discuss digitalization in the criminal procedure. In particular, there are the features of digitalization of investigation activities.[4] Considering this issue, the authors note the following:

> The process of investigative activities during investigation of a crime involving electronic (digital) carries of information, must be optimized and simplified with reduction of expenses for its implementation, even reject, to a certain extent, the formal rules of the traditional form of criminal procedure. That is why these problems require posthaste legislative solution.

7. Innovations Based on Digitalization in Procedural Legal Relations

One of the issues considered by the authors in this section is the role and place of electronic justice in the Russian civil process.[5] The authors note that, in general, the electronic technologies applied in dispute resolution are just a tool, while the related changes in procedural legislation only refer to the external form of procedural relations, without changing their essence or creating additional obligations for the participating persons.

Special attention should be paid to the issues of correlation between justice and mediation in digital reality. Highlighting the advantages of this phenomenon, the authors say that further development of electronic justice in Russia implies the

---

[4] Galina Rusman & Elizaveta Popova, *Development of the Software for Examination of the Crime Scene by Using Virtual Reality, Based on Spherical Panoramic Shot and 3D-Scanning*, in 2020 Global Smart Industry Conference (GloSIC) 297 (2020); Galina S. Rusman & Yulia A. Morozova, *Measures to Ensure Cybersecurity of Industrial Enterprises: A Legal Perspective*, 20(4) IEEE Secur. Priv. 23 (2022).

[5] Tikhon Podshivalov, *Models of Actio Negatoria in the Law of Russia and European Countries*, 7(2) Russian L.J. 128 (2019); Tikhon P. Podshivalov, *Property Legitimate Expectation as a Basis for the Application of Real Action*, 4 L.J. Higher Sch. Econ. 102 (2021).

need to solve a number of issues, still unresolved at the legislative level and arousing discussions in the scientific community. It is necessary to ensure such fundamental principles of judicial procedure as the principle of visibility and the principle of directness, as well as to protect against unsanctioned access to the court session or its recording. For that, it is feasible to use the blockchain technology.

8. Relevant Experience of Foreign Countries in the Sphere of Law Transformation Under Digital Realities

This section considers such issues as procedural law and judicial procedure under digital environment, as well as digitalization of law in certain types of public relations. This section of the monograph is written in English attracting larger readership. The authors of the chapter pursued the goal to demonstrate the complexity of developing digital platforms in the sphere of modern digital environment and to show how these problems are being solved in worldwide. Applying the foreign experience to the Russian legal theory and practice is, undoubtedly, very useful and may broaden the scope of legal awareness of the need to improve the legislative base in various aspects of development of the digital environment.

Conclusion

The book embraced various aspects of digitalization in various branches of law. Besides, the monograph provisions are of important applied significance, as it lists the probable legal risks related to the development of digital industry.

Especially noteworthy is the thorough analysis of legal acts and judicial practice, with recommendations formulated to improve the national legislation. The contribution of this monograph into the legal science is beyond doubt, as it provides the opportunity to consider the trends of using digital technologies in solving legal issues.

Acknowledgement

The article was supported by the Scholarship of the Kazan Innovative University named after V.G. Timiryasov.

References

Bazhina M. *Disputable Questions of the Use of Digital Technologies in Transportation*, 1(1) International Journal of Law in Changing World 33 (2022). https://doi.org/10.54934/ijlcw.v1i1.13

Gromova E. & Ivanc T. *Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS*, 7(2) BRICS Law Journal 10 (2020). https://doi.org/10.21684/2412-2343-2020-7-2-10-36

Gromova E.A. et al. *Legal Barriers to the Implementation of Digital Industry (Industry 4.0) Components and Ways to Overcome Them*, 25(1) Journal of World Intellectual Property 186 (2022). https://doi.org/10.1111/jwip.12215

Gromova E.A. et al. *Preferential and Experimental Regimes in the Sphere of Creation of Biomedical Innovations*, S2 Human. Sport. Medicine 161 (2021). https://doi.org/10.14529/hsm21s223

Gromova E.A. et al. *Quantum Law: The Beginning*, 1(1) Journal of Digital Technologies and Law 62 (2023).

Imasheva Y.I. et al. *Digital Inequality: Modernization of Kuznets Curve in the Digital Era*, 16(4) Russian Journal of Economics and Law 716 (2022). (In Russ.)

Podshivalov T. *Models of Actio Negatoria in the Law of Russia and European Countries*, 7(2) Russian Law Journal 128 (2019). https://doi.org/10.17589/2309-8678-2019-7-2-128-164

Podshivalov T.P. *Improving Implementation of the Blockchain Technology in Real Estate Registration*, 33(2) Journal of High Technology Management Research 100440 (2022). https://doi.org/10.1016/j.hitech.2022.100440

Podshivalov T.P. *Property Legitimate Expectation as a Basis for the Application of Real Action*, 4 Law. Journal of the Higher School of Economics 102 (2021). https://doi.org/10.17323/2072-8166.2021.4.102.123

Rusman G. & Popova E. *Development of the Software for Examination of the Crime Scene by Using Virtual Reality, Based on Spherical Panoramic Shot and 3D-Scanning*, in 2020 Global Smart Industry Conference (GloSIC) 297 (2020). https://doi.org/10.1109/GloSIC50886.2020.9267871

Rusman G.S. & Morozova Y.A. *Measures to Ensure Cybersecurity of Industrial Enterprises: A Legal Perspective*, 20(4) IEEE Security & Privacy 23 (2022). https://doi.org/10.1109/MSEC.2021.3129543

Information about the author

Ildar Begishev (Kazan, Russia) – Chief Researcher, Scientific-Research Institute of Digital Technologies and Law, Professor, Department of Criminal Law and Procedure, Kazan Innovative University named after V.G. Timiryasov (42 Moskovskaya St., 420111, Kazan, Russia; e-mail: begishev@mail.ru).

BRICS Law Journal

Volume X (2023) Issue 1

Оформление и компьютерная верстка:
ИП Резниченко А.С.

Подписано в печать 14.04.2023. Формат 70x100 $^{1}/_{16}$. Объем 12,25 п.л.
Цена свободная.

Наш адрес:
ООО «Издательство «Деловой стиль»
119330, Москва, вн. тер. г. муниципальный округ Раменки,
Мичуринский пр., дом 6, корп. 1, кв. 39
Тел.: +7 (495) 649-18-06
E-mail: o.leporskiy@ds-publishing.ru

Отпечатано в полном соответствии с качеством
предоставленных материалов в ООО «Фотоэксперт»
109316, г. Москва, Волгоградский проспект, д. 42,
корп. 5, эт. 1, пом. I, ком. 6.3-23Н