ISSN 2713-0525
eISSN 2713-0533

KUTAFIN LAW REVIEW

Volume 11 Issue 3 2024

Issue topics

DIGITAL LAW, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

SHANGHAI COOPERATION ORGANIZATION

STATE SOVEREIGNTY

LEGAL EDUCATION

https://kulawr.msal.ru/

KUTAFIN LAW REVIEW

Volume 11 Issue 3 2024

Founder and Publisher — Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

ISSN 2713-0525 eISSN 2713-0533

Publication Frequency	4 issues per year
Registered	Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Media Certificate PI No. FS 77-80833, dated 7 April 2021. Published since 2014
Website	https://kulawr.msal.ru/
Editorial Office contacts	kulawr@msal.ru + 7 (499) 244-88-88 (# 555, # 654)
Publisher contacts	Kutafin Moscow State Law University (MSAL) 9 Sadovaya-Kudrinskaya St., Moscow 125993, Russian Federation https://msal.ru/en/ msal@msal.ru + 7 (499) 244-88-88
Printing House	Kutafin Moscow State Law University (MSAL) 9 Sadovaya-Kudrinskaya St., Moscow 125993, Russian Federation
Subscription	Free distribution

Signed for printing 15.10.2024. 220 pp. 170 × 240 mm. An edition of 150 copies

CONTENTS

EDITORIAL

Dear Readers and Authors,

Advances in technologies have made it clear that the whole paradigm of social constructs is bound to change dramatically. At this very moment of the development of the humanity our perception of life, our mindsets are adjusting to this new reality. Artificial Intelligence (AI) technologies implementation is gaining momentum, redefining customary activities. There is no doubt that such innovations make our lives easier, however, fast pace of development and integration, that are often ahead of proper regulation, tend to lead to the emergence of new threats to society and an individual. This issue of the journal sets the task of highlighting such threats and challenges that might undermine our understanding of things.

Animesh Kumar Sharma and Rahul Sharma speak about one of the most relevant issues, namely generative AI that is capable to create almost anything in any sphere: texts, images, music, etc. On the one hand, it is useful. On the other, many questions arise. These include challenges to intellectual property, privacy, personal data protection, cyberbullying, deep fakes and many others. Besides, not only does the regulation matter, ethics and moral are also high on the agenda. As well as the fact that any text, including contracts — texts that have been inherently created by lawyers — can be generated not only by human mind, but with the help of chatbots and various modern language models, which may interfere with the very nature of many professions, legal profession being one of them.

Amid the development of generative AI and other digital tools, data breach is becoming a more frequent crime often targeting personal data and sensitive information. As easy as it becomes for an ordinary person to get access to different information, it seems much easier for criminals to commit cyber-attacks. As **Niharika Raizada and Pranjal Srivastava** mention, India is one of the most affected countries, especially when it comes to health industry. Electronic health records are at high risk since the legislation is yet to be developed properly, as well as healthcare infrastructure. Still, there is a question of why to target health data in the first place. The authors provide a comprehensive analysis of the situation in India, focusing on various cyber

threats, types of cyber-attacks, relevant legislation. Although the article primarily discusses the Indian experience (with a brief outlook on the problem in the US and EU), the ideas expressed can be of interest to any legislator and academia as the dangers and hazards that emerge in this regard are global.

Artur N. Mochalov discusses personal data from quite an unusual perspective. The information that individuals provide is stored in an organization that later might want to have more understanding of the client. This leads to the so-called digital profiling when by means of latest digital technologies and AI they process and analyze the data possible to obtain from the local storages, public resources and cross-references with other organizations drawing conclusions about similar groups of people, similar patterns of behavior, similar interests and the like. This process is also known as data mining and often fails to comply with the legislation related to personal data protection.

Such data can be mined through mobile applications that users download. As a rule when starting any application they agree to the terms of use and some other terms that include their consent to share specific information with other persons (interests, likes and dislikes, etc.). But the use of mobile applications poses other threats to the user, namely of criminal nature. **Arseniy A. Bimbinov** considers criminal risks that may arise while using different applications supporting the ideas expressed with the result of the survey conducted among different groups of young people. The research showed that many do not comprehend that some actions performed online are of criminal nature, the data they share may be at risk of breach, they may become victims of an array of offences.

Protection of private investment through bilateral investment treaties (BITs) in the modern day conditions is undergoing changes, in particular in cases involving member states of Shanghai Cooperation Organization. Analyzing the international investment arbitration cases involving the SCO states, **Ren Yanyan and Zhao Zhixin** not only define the most urgent issues but rather focus on a specific clause. At the core of their analysis is the Most-Favored-Nation (MFN) provision, namely it evolution, different approaches to its implementation and inter alia some difficulties of the MFN interpretation in China.

State sovereignty is another topical issue that requires reconsideration amid new challenges that the world has recently faced. **Sergey M. Zubarev and Denis B. Troshev** regard public law enforcement of state sovereignty as

a complex and multidimensional construct and examine the concept both in its broad and narrow sense. First, it is a combination of law making and law enforcement intrinsically intertwined with legal culture and legal consciousness, the balance of public and private interests, the rights and freedoms of citizens in the current geopolitical environment. Second, public law enforcement of state sovereignty is quite limited by statutory regulation and the way it is implemented. Still, it is possible to say that legal culture and consciousness are inherent in public law enforcement and can be a supportive tool, primarily through purposeful legal education activities provided for different groups of society.

Legal profession per se aims not only at internal activities but at external as well. **Natalia A. Abramova and Polina E. Marcheva** discuss the necessity to develop legal rhetoric skills in two languages: in Russian and in English. One major benefit is the facilitation of international cooperation and conservation of historical and cultural heritage. The ability to implement effective intercultural communication is of paramount importance for a highly qualified professional as it is relevant for different environments, for example, in the courtroom, where lawyers might have a challenge to use a different language, let alone the rules of a different system of law. Legal, linguistic, ethical elements of courtroom arguments require careful consideration and bilingual competence itself might be an extremely useful tool. In delivery of international student exchange programs bilingual training may be highly beneficial for a foreign student aiming to acquire such competences and wishing to advance in their profession.

The Academic events section features **Evgeniy V. Malyshkin** overview of the Conference titled "Thought as an Event: in Memory of Alexander Isakov" organized and hosted by St. Petersburg Academy of Postgraduate Pedagogical Education named after K.D. Ushinsky. The conference, which was also a tribute to Professor Isakov, focused on array of legal and philosophical issues developed in line with the Isakov's interests.

Anastasia N. Mitrushchenkova
Cand. Sci. (Philosophy), LLM
Deputy Editor-in-Chief

DIGITAL LAW, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

Article

DOI: 10.17803/2713-0533.2024.3.29.415-451

Generative Artificial Intelligence and Legal Frameworks: Identifying Challenges and Proposing Regulatory Reforms

Animesh Kumar Sharma, Rahul Sharma

Lovely Professional University, Phagwara, Punjab, India

***Abstract*:** This research paper seeks to understand the deficit arising from the generative AI and its potential in redefying various sectors and suggesting modification on the current laws. Generative AI systems can generate distinctive content which could be used in text, images, or music, among others, by training from the available data. It highlights how generative AI influences the legal profession in terms of work like contract writing, as well as how newer language models like GPT-4 and chatbots like ChatGPT and Gemini are evolving. Thus, while generative AI has numerous opportunities, it also raises concerns about ethical issues, authorship and ownership, privacy, and abuses, such as the propagation of deepfakes and fake news. This study focuses attention on the importance of strengthening the legal frameworks to answer the ethical issues and challenges linked to generative AI, such as deepfakes, piracy of contents, discriminative impact, or naked breaches of privacy. It calls for proper and sensitive use of generative AI through regulation, openness, and commonly agreed global guidelines. This paper emphasizes

that innovations need to be balanced by a set of effective regulations to unleash the potential of generative AI and minimize potential threats.

***Keywords*:** Generative Artificial Intelligence (Generative AI, GAI); legal frameworks; regulatory reforms; Intellectual Property (IP)

Cite as: Sharma, A.K. and Sharma, R., (2024). Generative Artificial Intelligence and Legal Frameworks: Identifying Challenges and Proposing Regulatory Reforms. *Kutafin Law Review*, 11(3), pp. 415–451, doi: 10.17803/2713-0533.2024.3.29.415-451

Contents

I. Introduction

Generative Artificial Intelligence (GAI), often known as Generative AI, is a significant achievement in the field of artificial intelligence (Dwivedi et al., 2021, p. 23). Unlike standard AI systems, which are geared for specialised tasks such as categorization or prediction, Generative AI focuses on creating new material. Text, photos, music, and even sophisticated data simulations can all be learned from current datasets using patterns and structures (Mondal et al., 2023, p. 12). Generative AI models such as GPT-4 and DALL-E excel in producing human-like text and visuals (Aydın and Karaarslan, 2023, p. 126). The rise of Generative AI has enormous promise across multiple disciplines. In the creative sectors, it can help artists generate ideas and content. In healthcare, it can aid in the development of novel medication molecules (Pérez et al., 2023). In education, it can give personalised learning materials (De Angelis et al., 2023, p. 4). The technology promises to revolutionise how we create and interact with digital information, providing unparalleled efficiency and creativity (Campbell et al., 2022, p. 25; Dwivedi et al., 2023, p. 37). However, the development and application of Generative AI poses considerable hurdles. Ethical problems are crucial, as the technology has the potential to generate deepfakes and spread misinformation, with major societal consequences (Porsdam Mann et al., 2023). There is also the issue of intellectual property, as these models frequently train from massive datasets containing copyrighted material, generating concerns about the ownership of generated content (Anderljung and Hazell, 2023). Furthermore, training large-scale AI models has a significant environmental impact due to the massive

computational resources required. Ensuring that Generative AI is used ethically and sustainably is a difficult task that requires technological, legal, and ethical concerns (He, 2019, p. 227).

While generative AI brings forth numerous benefits, it also poses significant challenges and potential misuse. Generative AI can be misused to generate deepfake content, misinformation, or for other malicious purposes. The rapid advancement of generative AI techniques requires proactive measures to mitigate potential risks, including the spread of manipulated or fabricated information (Chan, 2023, p. 57). One of the primary concerns is the generation of deepfake content, where AI systems can create incredibly realistic videos, images, or audio recordings that are difficult to distinguish from genuine ones (Maras and Alexandrou, 2019, p. 258). This has raised concerns about the potential for misinformation, identity theft, and the erosion of trust in media. Another area of concern is the potential for AI-generated content to infringe upon intellectual property rights. If generative AI is used to create content that closely resembles existing copyrighted works, it could lead to legal disputes and challenges in determining originality and ownership (Kietzmann et al., 2020, p. 141). There are ethical implications surrounding the use of generative AI, such as the creation of biased or discriminatory content (Illia et al., 2023, p. 206). If the AI models are trained on biased datasets, they may inadvertently generate content that perpetuates existing social inequalities or reinforces harmful stereotypes. Given the potential risks associated with generative AI, it is crucial to amend existing laws and regulations to ensure its responsible and ethical use (Mittelstadt, 2019, p. 503). These amendments should address issues such as the identification and labeling of AI-generated content, establishing guidelines for fair use and intellectual property rights, and implementing mechanisms to prevent the dissemination of malicious or harmful content (Lucaj et al., 2023, p. 1270). Moreover, there is a need to establish frameworks for auditing and certifying generative AI systems to ensure transparency, accountability, and fairness. This would involve defining standards for dataset collection, model training, and evaluation to mitigate biases and ensure that the technology is used in a manner that aligns with societal values and norms. Furthermore, international cooperation and

collaboration are essential to developing a cohesive global approach to regulating generative AI. As technology transcends geographical boundaries, harmonized efforts are required to address legal and ethical challenges consistently. Nevertheless, its potential for misuse, particularly in the creation of deepfakes and dissemination of false information, raises significant ethical concerns (Meskys et al., 2020, p. 25). To address these challenges, legal amendments are necessary to regulate the use of generative AI, protect privacy, and combat malicious activities. By striking the right balance between innovation and regulation, we can harness the transformative power of generative AI while safeguarding against its potential misuse. Generative AI, a rapidly advancing field of artificial intelligence, holds immense potential for revolutionizing various industries and empowering creative endeavors (Haluza and Jungwirth, 2023, p. 13). By employing advanced algorithms and neural networks, generative AI systems can generate realistic and original content such as images, videos, music, and even text. However, as with any powerful technology, there is a need to carefully consider its uses and potential misuse. While generative AI offers exciting possibilities, it also raises concerns regarding intellectual property rights, privacy, and ethical considerations. As society continues to navigate this technological frontier, it is imperative to strike a balance between fostering innovation and ensuring appropriate safeguards are in place. Therefore, there is a growing need to amend laws and regulations to address the unique challenges posed by generative AI, while also fostering its beneficial applications.

While Generative AI has transformative potential, understanding its hurdles is critical to reaping its benefits while minimizing its hazards. The future of Generative AI depends on the joint efforts of researchers, policymakers, and industry leaders to overcome these complex concerns. The emergence of Generative AI brings significant legal concerns that current laws are unprepared to address. By changing existing legal frameworks to handle issues of intellectual property, liability, data privacy, and bias, society may better reap the benefits of GAI while limiting the hazards. These legal changes are critical for creating a responsible and equitable AI environment that respects the rights and interests of all stakeholders.

II. Legal Challenges due to GAI and Possible Solutions

Generative Artificial Intelligence has gained significant attention in recent years due to its ability to produce original and creative content. This study examines the advantages and disadvantages of generative AI and highlights the need for legal amendments to address the ethical, social, and legal challenges associated with its use. GAI raises a slew of legal issues that demand broad changes to existing legislation (Moulaei et al., 2024). As these advanced AI systems develop new content, they blur the distinction between human creativity and machine-generated output, posing difficult legal problems about intellectual property, liability, and data privacy. Misuses of generative artificial intelligence are discussed below.

II.1. Intellectual Property Concerns

Generative artificial intelligence raises questions regarding intellectual property rights, as it can replicate existing creative works, potentially leading to copyright infringement and devaluation of original creations (Uzun, 2023, p. 49). GAI raises complex questions about intellectual property rights and ownership. The generated content often builds upon existing works, making it difficult to determine the boundaries of originality and the rights of creators. Legal frameworks need to adapt to address these challenges and provide adequate protection for creators and their works.

One of the most serious IP concerns is determining ownership rights for AI-generated material. Traditional IP rules are intended to safeguard creations that are the result of human intelligence, creativity, and labour. However, GAI systems, such as those used to create art, music, literature, and software code, develop content on their own using algorithms and training data. This raises a number of questions. Who owns the AI-generated content? Is it the AI model developer, the user who submitted the input prompt, or the company that controls the data used to train the AI? Can AI have intellectual property rights? While existing laws do not recognise AI as an entity with rights, this may change in the future as AI systems progress. For example, if an AI

system creates a new piece of music, establishing whether the copyright belongs to the AI developer, the user who instructed the AI, or another party becomes difficult. The lack of clear legal precedents and rules in respect of this problem leads to uncertainty and probable conflict among stakeholders.

Potential Infringement of Copyrights: Another key IP issue arises from the manner in which GAI systems are trained. These algorithms often need a large quantity of data to understand patterns and generate new content (Thongmeensuk, 2024, p. 7). This training data frequently includes copyrighted content, such as books, photographs, music, and videos. When AI systems use these materials without legal authority, various problems arise.

***Unauthorized Use of Copyrighted Works*:** If an AI system is trained on copyrighted content without the required permissions or licences, it may violate the rights of the original creators and owners. This unauthorised usage may result in legal issues and claims for damages.

Derivative Works and Plagiarism: AI-generated material may closely resemble the original works utilised in training. This similarity might blur the borders between original creativity and plagiarism, making it difficult to identify AI-generated works from actual copyrighted items. For example, if an AI-generated artwork closely mimics the style of a well-known artist whose works were included in the training dataset, there may be concerns that the resulting artwork is an unauthorised derivative work. Similarly, if an AI system generates language that is identical to the structure and content of a copyrighted book, this may be called plagiarism.

II.2. Regulatory Reforms Needed to Address IP Challenges

Addressing these intellectual property challenges necessitates broad legal and regulatory changes. Possible solutions are the following.

Creating New IP Categories: Adding new categories or extending existing IP rules to address AI-generated content. This could involve clarifying ownership rights for AI-generated works and creating policies for using copyrighted content in AI training.

Licencing and Fair Use Policies: Implementing licencing frameworks and fair use standards to allow AI developers to use copyrighted resources while compensating the original inventors and rights holders. This could entail developing common licences for AI training datasets.

Transparency and Documentation: Requiring AI developers to be transparent and document the training data utilised by their algorithms. This can assist ensure that copyrighted items are utilised lawfully and ethically, as well as providing a basis for dispute resolution.

The IP challenges raised by Generative AI are extensive and varied. Determining ownership of AI-generated work and mitigating potential copyright infringements are major difficulties that necessitate thoughtful legal and regulatory changes. By setting explicit norms and frameworks, it is possible to balance the interests of AI developers, users, and original content creators, promoting an atmosphere conducive to innovation while protecting IP rights.

II.3. Misinformation and Deepfake Content

The rapid progress of generative AI increases the risk of producing convincing fake content, including deepfake videos and counterfeit documents, which can have severe social, political, and economic consequences (Bontridder and Poullet, 2021, p. 15). Generative AI has the potential to facilitate the creation of sophisticated deep fakes, which are manipulated videos or images that appear genuine but are actually fabricated. This poses a significant threat to privacy, reputation, and the spread of misinformation. Regulations are necessary to combat the misuse of generative AI in generating malicious content.

Generative Artificial Intelligence (GAI) has the ability to generate highly realistic content, which can be both advantageous and detrimental. While it creates new opportunities for creative and technological innovation, it also introduces substantial threats such as misinformation and deepfakes. False and manipulated media can have a significant impact on public perception, security, and faith in information.

GAI systems may generate hyper-realistic images, movies, and audio materials that are indistinguishable from actual ones. This functionality can be used to create misinformation and deepfakes, resulting in a number of following issues.

Erosion of Trust: The spread of deepfakes and incorrect content threatens public faith in digital media. When people can no longer tell the difference between real and fake material, they lose trust in respectable news sources and truthful reporting.

Political Manipulation: Deepfakes can be used to influence political events and individuals. For example, manufactured movies depicting politicians making provocative words or indulging in unethical behaviour can be used to influence public opinion and disrupt elections. These manoeuvres can destabilise political structures and jeopardise democratic processes.

Personal Harm and Defamation: Individuals can be targeted with deepfakes that portray them in compromising situations, resulting in reputational damage, emotional suffering, and even legal ramifications. Such targeted attacks might be used for extortion, harassment, or retaliation.

Financial Fraud: Deepfakes can also be used in financial schemes, such as producing fake videos of chief executive officers (CEOs) or executives telling employees to transfer payments. These realistic deceptions can cause considerable financial losses for corporations.

II.4. Challenges in Detecting and Mitigating the Impact of Deepfakes

The realistic character of deepfakes and other AI-generated misinformation poses significant hurdles for detection and prevention (Romero Moreno, 2024, p. 15).

Technical Detection Difficulties: Advanced technology and expertise are required to detect deepfakes. As GAI systems become more advanced, the fake material they generate becomes increasingly difficult to detect using standard forensic approaches. Researchers and technology businesses must constantly create and upgrade detection algorithms to stay up with GAI improvements.

***Resource Intensive**:* Creating and deploying good deepfake detection technologies can be resource-intensive. It necessitates significant investment in research, technology, and infrastructure, which may not be possible for all organisations, particularly smaller corporations and individuals.

Rapid Spread of Misinformation: In today's digital age, misinformation can spread quickly via social media and other venues. Even if a deepfake is found, the bogus information may have already affected a huge audience.

II.5. Regulatory Measures Needed to Address the Problems of Misinformation and Deepfake Content

Current legal and regulatory structures are frequently unprepared to address the complications posed by deepfakes. There could be gaps in regulations governing the development, distribution, and use of modified media, making it difficult to hold culprits accountable. To mitigate the impact of deepfakes, the public must be made aware of their presence and potential dangers. Educating people to critically analyse the information they consume is crucial, but difficult given the disparities in media literacy between communities. Addressing the difficulties of misinformation and deepfakes requires a holistic approach that combines legal, technical, and pedagogical initiatives (Montasari, 2024, p. 247).

Misinformation and deepfakes generated by GAI present substantial and diverse issues. To limit these dangers and maintain the integrity of information in the digital age, a mix of legislative measures, advanced detection technology, collaborative efforts, platform regulations, and public education can be used.

Regulatory Measures: Governments and regulatory organisations must update existing laws and enact new legislation that expressly address the creation and dissemination of deepfakes and AI-generated misinformation. This includes providing clear legal definitions and punishments for offenders.

Advanced Detection Technologies: Continued investment in the development of better detecting technology is essential. This

includes employing machine learning and AI to detect tiny artefacts and inconsistencies in modified media that are not evident to the human eye.

Collaboration and Standardization: Collaboration among governments, technological businesses, and academic institutes can aid in knowledge exchange and the development of standardised methods for detecting and combating deepfakes. Creating industry standards for content verification and authentication might also be beneficial.

Platform Policies: Social media networks and online services must put in place strong policies and tools for detecting and removing deepfakes. This includes implementing AI-based moderation systems and giving users tools to report suspected deepfakes.

Public Education Campaigns*:* Running public education efforts to raise awareness about the presence and risks of deepfakes is critical. These initiatives should focus on enhancing media literacy by teaching people how to establish the veracity of the content they come across.

III. Ethical Challenges due to GAI and Possible Solutions

Generative artificial intelligence poses ethical concerns, as it can be used for malicious purposes, such as generating explicit or harmful content, invading privacy, or manipulating public opinion through the creation of misleading narratives (Fiske et al., 2019). There exist ethical concerns related to content ownership, copyright infringement, and authenticity. The automated generation of content blurs the lines between original and artificial creations, leading to challenges in determining the rightful ownership and proper attribution of generated works. GAI raises ethical concerns like misinformation through deepfake, immortalize of bias and possible discrimination due to biased training data. Various ethical concerns arising due to GAI and its potentials solutions are discussed below.

III.1. Perpetuation and Amplification of Existing Biases

AI systems are trained on large datasets that can contain inherent biases, which may be perpetuated in the generated content (Jobin et al.,

2019, p. 394). This bias poses a risk of discrimination and exacerbates societal inequalities, emphasizing the need for responsible training and bias mitigation strategies. Generative AI systems are trained on large datasets, which may contain biases present in the data. If not properly addressed, these biases can be amplified in the generated content, perpetuating societal inequalities and discrimination. Developing robust ethical guidelines and regulations is crucial to mitigate these concerns.

GAI systems have the potential to transform several fields by producing fresh information and insights. However, one of the major issues they face is the possibility of replicating and increasing existing biases in their training data. This can result in discriminatory decisions that harm individuals or groups, exacerbating societal disparities and prejudices. GAI systems are trained on big datasets, which frequently contain biases reflecting society prejudices and inequality (Khowaja et al., 2024). These biases can be unintentionally learned and repeated by the AI, resulting in following issues.

Bias in Data Collection: The data used to train AI models may be skewed due to historical injustices, a lack of diversity, or biased sampling techniques. For example, datasets with more data on particular demographics than others may result in an AI system that favours those demographics.

Bias in Data Annotation: When human annotators label training data, they may introduce their own biases. If the annotations represent stereotypical or prejudiced viewpoints, the AI system can learn and reproduce these biases.

Reinforcement of Stereotypes: GAI systems have the potential to generate information that reinforces existing stereotypes. For example, if an AI model is trained on literature containing gender biases, it may generate content that reinforces such biases, such as associating certain professions with a specific gender.

III.2. Discrimination in Respect of Certain Individuals or Groups

GAI system approaches can lead to biased decisions with major consequences for certain individuals or groups. GAI system can enhance biased decisions influencing marginalized communities, females,

persons with disabilities, and low income-group. Various religious groups, lesbian, gay, bisexual, transgender, queer or questioning, or another diverse gender identity (LGBTQ+) individuals, ethnic and racial minorities may be facing discrimination in law enforcement, recruitment, and healthcare. Females may encounter gender disparity in jobs, medical care and other fields. People with special needs may be refrained from services, while low-income individuals could be viciously penalized in financial support and employment opportunities. Older individuals and immigrants may also be in pain from AI biases in community services and legal works. These concerns focus attention on the need for trustworthy and inclusive AI design.

Unfair Treatment: AI-generated content may result in discriminatory treatment of people based on their ethnicity, gender, age, or other protected characteristics. If a generative AI employed in recruitment has learned biased patterns from prior hiring data, it may favour certain groups over others.

Misinformation and Harmful Content: Biases in AI-generated content can lead to the spread of disinformation and negative stereotypes. This has the potential to aggravate social differences and contribute to the marginalisation of already vulnerable populations.

Inequitable Access to Resources and Opportunities: Discriminatory AI systems can lead to unequal access to resources and opportunities. For example, an AI model used in lending may deny loans to particular groups more frequently due to biased training data, reinforcing financial inequities.

Compliance with Anti-Discrimination Laws: AI systems must follow anti-discrimination laws and regulations that prevent unfair treatment based on protected traits. To ensure compliance, AI models must be rigorously tested and validated to discover and mitigate biases.

III.3. Ethical Responsibility

Generative AI presents substantial issues in terms of prejudice and discrimination (Ferrara, 2023, p. 7). Developers and users of GAI may assist create more fair and equitable AI systems by identifying sources of bias in training data, understanding the potential for discriminatory

outcomes, and adopting robust solutions to address these issues. This necessitates a concerted effort to ensure that AI technologies are developed and deployed in ways that foster inclusivity, fairness, and ethical responsibility.

Developers and users of GAI systems must ensure that their AI technologies do not damage people or increase societal injustices. This includes applying justice and inclusion ideals to AI development and deployment. Several strategies can be used to reduce prejudice and discrimination in GAI systems.

Diverse and Representative Data: Keeping training datasets broad and representative of the population might help decrease biases. This entails actively searching out and incorporating data from underrepresented populations which include individuals with disabilities, minorities, low-income groups, less educated or uneducated individuals, older people and people with rural background etc.

Bias Detection and Mitigation Techniques*:* Implementing bias detection and mitigation strategies, such as reweighting data, employing fairness constraints, and using debiasing algorithms, can aid in the identification and reduction of biases in AI models.

Regular Audits and Transparency: Regular audits of AI systems to determine their fairness and transparency are required. Providing detailed documentation and explanations of AI decision-making processes can help to foster confidence and accountability.

Inclusive Design Practices: Adopting inclusive design methods that include diverse teams in the development process will assist ensure that different points of view are considered, lowering the likelihood of biased results.

Ongoing Monitoring and Evaluation: Continuously monitoring and reviewing AI systems after deployment to identify and resolve any developing biases or discriminatory effects is critical for long-term fairness.

IV. Data Privacy Concerns due to GAI

GAI systems are often trained on large datasets containing personal and sensitive information. The use of such data creates serious legal concerns, notably around permission and data protection. Existing

data privacy legislation, like as the General Data Protection Regulation (GDPR) in Europe, may need to be revised to account for the complexities of AI training procedures. To ensure that individuals' privacy rights are safeguarded under GAI, strong data governance procedures and unambiguous data usage and retention regulations are required.

The deployment of GAI systems creates serious privacy problems (Kar et al., 2023, p. 675). These issues originate from the considerable usage of personal and sensitive information in AI model training, as well as the problems of guaranteeing compliance with existing data protection rules, such as the GDPR. Addressing these challenges is crucial for protecting individuals' privacy rights and preserving public trust in AI technologies.

IV.1. Challenges in Protecting Personal and Sensitive Information

Generative AI systems frequently require large volumes of data to learn and generate new information effectively. This data may contain personal and sensitive information, such as text from social media posts, medical records, financial data, and other private information. The usage of such data presents the following challenges.

Data Collection and Consent: Obtaining and using personal data for training AI models requires proper consent. However, it can be difficult to confirm that all data utilised in training was obtained legally and with the informed agreement of all parties involved. Datasets are frequently aggregated from multiple sources, making it difficult to track the consent status of each piece of data.

Anonymization and De-Identification: To maintain privacy, data used to train AI models should be anonymised or de-identified. However, complete anonymization is difficult to achieve, and there is always the possibility that anonymized data will be re-identified, particularly when paired with other data sources. This poses a serious threat to people's privacy.

Data Minimization and Purpose Limitation: Data protection principles promote data reduction (using only the data required for the

purpose) and purpose limitation. Ensuring that generative AI models adhere to these principles is difficult, especially given the large and diverse datasets they require.

IV.2. Ensuring Compliance with Data Protection Laws like GDPR

The GDPR and other data protection legislation impose strict restrictions on the processing and protection of personal data. Ensuring compliance with these regulations when building and deploying generative AI systems presents the following three important challenges.

Right to be Forgotten: Individuals have the right under GDPR to request that their personal data be deleted. This presents a problem to AI systems that have already been trained on data including the personal information of persons who later exercise this right. Retraining models to exclude such data, as well as developing technical solutions to meet these needs, can be time-consuming and costly.

Data Subject Rights: Individuals have a variety of data-related rights under GDPR, including the ability to access, correct, and restrict data processing. Implementing measures to protect these rights in the context of generative AI is difficult, especially when dealing with huge, dynamic datasets.

Data Breach Notification: Data breaches are a risk for generative AI systems, as they are for any other digital system. Respective law of the land needs to be either updated or put in place, systems to detect, respond to, and alert affected individuals.

IV.3. Legal and Technological Solutions to the Problem of Protecting Personal and Sensitive Information

Protecting data privacy in the context of Generative AI entails tackling the issues of using personal and sensitive information to train AI models while also guaranteeing compliance with data protection legislation such as GDPR. These dangers can be mitigated and individuals' privacy rights protected by adopting strong data governance

frameworks, utilising privacy-enhancing technologies, conducting regular audits, and maintaining transparent policies. To address these data privacy challenges, a mix of the following legal and technological solutions are required.

Data Governance Frameworks: Putting in place complete data governance frameworks that include policies and processes for data collecting, consent management, anonymization, and data minimization. These frameworks should ensure that the data used to train AI models is handled ethically and lawfully.

Privacy-Enhancing Technologies (PETs): Using privacy-enhancing technologies such as differential privacy, federated learning, and homomorphic encryption can help safeguard personal data while also allowing AI models to be trained effectively. These technologies can lower the danger of data breaches and re-identification.

Regular Audits and Assessments: Regular privacy impact studies and audits are conducted to examine and mitigate the privacy hazards associated with generative AI systems. These audits can help to verify continuing compliance with data protection rules and suggest areas for improvement.

Transparent Practices: Maintaining transparency in the collection, usage, and protection of data in generative AI systems. Individuals' trust and compliance with data protection standards can be increased by providing them with clear and accessible information about their rights and how their data is handled.

V. Liability and Accountability for GAI-Generated Content

Determining accountability for GAI-generated content is still another big difficulty. If an AI system generates defamatory content, disinformation, or damaging outputs, it is critical to determine who is to blame (Dogru et al., 2023, p. 1089). Current legal frameworks fail to explicitly specify the accountability of AI developers, deployers, and consumers. Legal changes are required to define obligations and ensure that the relevant parties can be held accountable for the conduct of generative AI systems.

GAI systems, while strong and inventive, present substantial liability and accountability concerns. These difficulties must be addressed in

order to ensure that AI technology is used and deployed responsibly and ethically. The key difficulties in this field are determining who is liable for AI-generated content and addressing the legal ramifications when such content causes harm or violates laws.

V.1. Establishing Who Is Responsible for the Content Generated by AI

One of GAI's primary issues is identifying culpability for the content it generates. Unlike traditional software, which relies on explicit instructions from human programmers, GAI systems generate content on their own using patterns acquired from training data (Yang et al., 2024, p. 7). This poses various questions.

Developer Responsibility: Should the AI system's designers be held responsible for the results produced by their technology? Developers manage the AI's design and training, but not its specific outputs once deployed.

User Responsibility: Should users that interact with the AI and provide input prompts be held liable for the created content? Users can alter the material by providing inputs, but they may not fully comprehend the AI's underlying operations.

Joint Responsibility: Could there be a joint duty between developers and users? This approach acknowledges both parties' roles in the creation and usage of AI-generated material. For example, if an AI-generated artwork is discovered to infringe on existing copyrights, it is unclear whether the guilt should be placed on the AI developer, who developed and taught the system, or the user, who gave the precise input that resulted in the infringing output. This ambiguity hampers the process of determining liability and needs explicit legal definitions and frameworks.

V.2. Addressing Legal Consequences when AI-Generated Content Causes Harm or Violates Laws

When AI-generated content causes harm or violates laws, finding the proper legal repercussions is another difficult task. Harm can take many forms, including defamation, disinformation, or the creation of

harmful or unlawful content (Ling, 2023, p. 105). The legal system must change to adequately deal with these new forms of injury.

***Defamation and Misinformation*:** If an AI system creates content that defames someone or spreads incorrect information, it is critical to determine who is legally responsible. This is especially problematic when material is developed by an autonomous machine rather than a human.

Illegal and Harmful Content: AI systems have the potential to generate illegal or harmful content, such as explicit material, hate speech, or encouragement to violence, either accidentally or on purpose. Addressing the legal implications of such content necessitates new legislation that can hold responsible parties accountable.

Consider the scenario in which an AI chatbot produces damaging or offensive speech. Should the platform hosting the chatbot be held accountable, or should the burden fall on the developers who designed the chatbot's algorithms? Furthermore, if an AI-generated deepfake is used to deceive or hurt people, identifying culpability is critical for ensuring justice and preventing such instances.

V.3. Legal and Regulatory Implications

To effectively handle the difficulties of liability and accountability in GAI, numerous legal and regulatory approaches can be considered.

Clear Liability Frameworks: Creating explicit liability frameworks outlining the roles of developers, users, and other stakeholders engaged in the deployment and usage of GAI systems. These frameworks should specify the situations under which each party may be held accountable.

***Compliance and Oversight Mechanisms*:** Putting in place measures to monitor and regulate the use of GAI systems. This might include frequent audits, certification processes, and the creation of regulatory agencies to monitor AI systems.

***Robust Legal Recourse*:** Offering strong legal remedies to individuals and entities affected by AI-generated content. This involves ensuring that there are clear legal channels for seeking restitution and justice in cases of harm or infringement.

Ethical Guidelines and Best Practices: Government and associated relevant regulatory bodies should encourage the application of ethical guidelines and best practices in the creation and implementation of GAI systems. This can help to reduce harm and guarantee that AI technologies are used responsibly and ethically.

Addressing the responsibility and accountability issues raised by Generative AI necessitates a multidimensional approach that includes clear legal frameworks, strong oversight, and ethical principles. We can make the AI ecosystem safer and more accountable by determining who is liable for AI-generated material and dealing with the legal ramifications of damaging outputs. This will assist to increase trust in AI technologies and ensure that their benefits are realised without jeopardising legal and ethical standards.

VI. Cases of Deepfakes

After the evolution of GAI, deepfake cases have increased (Shoaib et al., 2023, p. 4). Few political deepfake, deepfake cases of celebrities, video fraud calls, cases of social media information, corporate espionage and financial scam cases are discussed below.

VI.1. Political Deepfakes

In 2018, director Jordan Peele worked with Buzzfeed to create a deepfake video depicting former US President Barack Obama. The video, titled "Obama Deepfake," utilises Peele's voice and facial manipulation technologies to resemble Obama giving a public service statement. This video received a lot of attention and highlighted how deepfakes can trick viewers by successfully imitating popular people (Cuthbertson, 2018). In 2018, researchers made a deepfake video of former US President Barack Obama to demonstrate how readily disinformation may spread. The video depicted Obama saying statements he never said, emphasising the potential for deepfakes to sway public perception and electoral outcomes.

In 2019, the Belgian political party Socialistische Partij Anders launched a series of deepfake videos starring several Belgian politicians, including the Prime Minister. These movies were produced as part of

a campaign to raise awareness about the risks of deepfake technology and its possible impact on political discourse and public confidence.[1]

Deepfake technology was reportedly used to make fake remarks by Gabonese politicians in 2020. These edited videos were shared on social media platforms, raising concerns about their ability to influence public opinion and cause unrest in the country.[2]

During the 2019 Indian general election campaign, deepfake videos of political leaders were shared on social media platforms. These videos were modified to show politicians making provocative statements or acting unethically, raising worries about the use of deepfakes for political propaganda and misinformation (Chaturvedi and Kumar, 2019).

These incidents show the increasing prevalence of political deepfakes, as well as the need for more awareness, legislation, and countermeasures to address the hazards connected with synthetic media manipulation in political contexts.

VI.2. Celebrity Deepfakes

Deepfake videos of actress Scarlett Johansson appeared online in 2019, showing her in uncomfortable settings. These fully produced videos demonstrated the potential for deepfakes to ruin individuals' reputations and invade their privacy.

In 2021, a deepfake video of Tom Cruise went viral on TikTok. Chris Ume, a visual effects specialist, made the film, which convincingly depicted Cruise performing magic tricks and chatting golf, sparking widespread doubt about its validity.[3]

---

[1] Mast, J., (2019). Prime Minister appears in deepfake video about Facebook. *The Brussels Times*. Available at: https://www.brusselstimes.com/all-news/belgium-all-news/education/70836/prime-minister-appears-in-deepfake-video-about-facebook/ [Accessed 12.05.2024].

[2] BBC News. (2020). Gabon government "using deepfakes to create fake speech." *BBC News*. Available at: https://www.bbc.com/news/technology-51219120 [Accessed 10.05.2024].

[3] ABC News. (2021). Viral deepfake video of Tom Cruise on TikTok heightens concerns about manipulated media. *ABC News*. Available at: https://abcnews.go.com/US/viral-deepfake-video-tom-cruise-tiktok-heightens-concerns/story?id=76249861 [Accessed 11.05.2024].

In 2020, a deepfake video surfaced online in which creator Steve Buscemi's face was digitally transplanted onto Jennifer Lawrence's body. The film, which went viral on social media, demonstrated how deepfake technology can generate misleading and fraudulent information.[4]

These incidents emphasise the ethical and privacy concerns surrounding celebrity deepfakes, emphasising the importance of improved awareness, regulation, and technological remedies to address the hazards posed by synthetic media manipulation.

VI.3. Fraudulent Video Calls

In 2020, a UK-based energy company was duped out of $ 243,000 with a deepfake audio call. The crooks employed artificial intelligence to impersonate the CEO's voice and direct an employee to transfer funds to a fake account. This example highlighted the risks connected with AI-generated voice impersonation in corporate security. In 2019, a UK-based energy company fell victim to a deepfake audio fraud that resembled the CEO's voice. The fraudsters impersonated the CEO using AI-generated voice technology and convinced an employee to transfer € 220,000 to a Hungarian supplier. This event exposed the ability of deepfake technology to support sophisticated financial fraud schemes.[5]

In 2020, a European energy company was targeted with a deepfake video conferencing hoax. During a video conference call with a senior executive, the fraudsters impersonated the CEO of the company using AI-generated footage. The deepfake video convinced the CEO to authorise a fraudulent money transfer, resulting in significant financial losses for the company.[6]

[4] Ridder, K., (2020). Steve Buscemi Replaces Jennifer Lawrence in Deepfake Video and It's So Confusing. *Newsweek*. Available at: https://www.newsweek.com/steve-buscemi-jennifer-lawrence-deepfake-video-1482503 [Accessed 12.06.2024].

[5] BBC News. (2019). UK energy firm probes "deepfake" video of boss. *BBC News*. Available at: https://www.bbc.com/news/technology-49574808 [Accessed 11.05.2024].

[6] Bloomberg. (2020). A European Energy Firm Pays Up After Cyberattack, Deepfake. *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2020-10-30/a-european-energy-firm-pays-up-after-cyberattack-deepfake [Accessed 09.05.2024].

In 2021, criminals targeted a German corporation by impersonating its CEO with AI-generated voice technology. The fraudsters employed a deepfake voice to ask an employee to send € 220,000 to a Hungarian supplier. Despite the company's verification measures, the deepfake voice's convincing nature allowed the fraudulent transaction to be carried out successfully.[7]

In 2020, fraudsters attempted to scam a UK-based energy corporation by impersonating a British CEO using deepfake technology. The deepfake video chat was convincing enough to trick the company's finance controller into sending € 220,000 to the criminals' account. The event demonstrated the vulnerability of organisations to deepfake-based impersonation frauds.[8]

These examples highlight the real-world consequences of fraudulent video calls enabled by deepfake technology. They emphasise the importance of organisations using strong authentication and verification mechanisms to detect and avoid deepfake-related scams. They also emphasise the significance of raising awareness about the risks connected with synthetic media manipulation in financial transactions and corporate communications.

VI.4. Social Media Misinformation

Deepfake technology was used during the 2020 US elections to generate videos of politicians making incendiary statements. These videos propagated on social media channels, confusing voters and propagating misleading information.

In 2019, a doctored video of US House Speaker Nancy Pelosi became popular on social media platforms. The video was slowed to make Pelosi appear intoxicated or incapacitated, causing considerable outrage and

[7] DW News. (2021). German energy firm becomes victim of deepfake cyberattack. *DW News*. Available at: https://www.dw.com/en/german-energy-firm-becomes-victim-of-deepfake-cyberattack/a-57192482 [Accessed 11.05.2024].

[8] IT Governance. (2020). Deepfake scams: UK CEO loses € 220,000 in latest attack. *IT Governance*. Available at: https://www.itgovernance.co.uk/blog/deepfake-scams-uk-ceo-loses-220000-in-latest-attack [Accessed 10.05.2024].

underlining the potential for deepfakes to propagate misinformation and political propaganda.[9]

Throughout the Covid-19 outbreak, multiple deepfake videos circulated on social media platforms, spreading falsehoods about the virus and its origin. These videos contained false remarks from health authorities, conspiracy theories, and incorrect information about viable therapies, all of which contributed to confusion and public mistrust.[10]

During elections and political campaigns, deepfake videos have been used to propagate misinformation and political propaganda on social media sites. For example, in the run-up to the 2020 presidential election in the United States, deepfake videos including falsified claims from political candidates circulated online, with the goal of manipulating public perception and influencing voter behaviour. Deepfake videos of celebrities have been used to promote disinformation and false tales on social media platforms. For example, falsified videos of celebrities making controversial words or engaging in illegal actions have spread online, confusing viewers and feeding rumours.[11]

These examples demonstrate the various ways deepfake technology has been used to propagate misinformation and disinformation on social media sites. They emphasise the significance of critical media literacy and strong fact-checking processes in combating the spread of false content online.

VI.5. Corporate Espionage

A bad creator might utilise deepfake technology to construct a convincing video or audio clip of a company's CEO or another high-ranking executive. Deepfakes could be used to broadcast misleading

[9] BBC News. (2019). Pelosi "drunk" video: Faked footage shows House speaker slurring. *BBC News*. Available at: https://www.bbc.com/news/world-us-canada-48348059 [Accessed 11.05.2024].

[10] The Guardian. (2020). "We're in a Petri Dish": How a Covid-19 Office Outbreak Unfolded — and Was Covered Up. *The Guardian*. Available at: https://www.theguardian.com/world/2020/aug/15/covid-19-petri-dish-how-a-coronavirus-outbreak-unfolded [Accessed 11.05.2024].

[11] NBC News. (2020, January 13). Deepfake videos are getting better, but they're still easy to spot. *NBC News*. Available at: https://www.nbcnews.com/tech/security/deepfake-videos-are-getting-better-they-re-still-easy-spot-n1116181 [Accessed 29.05.2024].

information, issue fraudulent directions, or deceive personnel or stakeholders, causing reputational damage or financial losses to the targeted organization (George and George, 2023). Deepfake technology might be used to create realistic video footage of boardroom meetings or private discussions inside a firm. Competitors or adversaries could use the faked content to obtain access to strategic plans, sensitive information, or trade secrets, undermining the targeted organization's competitive advantage. Deepfake videos or audio recordings could be used to construct false financial reports or earnings calls that misrepresent a company's financial status or prognosis. Attackers who disseminate false financial information may manipulate stock prices, disrupt financial markets, or erode investor trust in the targeted organisation. Deepfake technology may enable sophisticated phishing assaults or social engineering techniques aimed at a company's employees or business partners. Malicious creators could create convincing deepfake videos or audio messages that impersonate trusted individuals within the organisation, such as colleagues, supervisors, or IT administrators, in order to trick targets into disclosing sensitive information, granting unauthorised access, or conducting fraudulent transactions.

The deepfake cases cited above highlight areas of concern for the corporate world. Need of the hour for corporates is to be aware about bad usage of the GAI in the industry. Corporates must put a system in place to detect deepfakes and resolve any issues arising of it in minimum possible times.

VI.6. Financial Scams

In 2022, deepfake movies and audio samples were utilised in a series of scams aimed at individuals and businesses. Fraudsters exploited AI-generated material to imitate bank officials and get personal information, causing considerable financial losses for the victims (De Rancourt-Raymond and Smaili, 2023). A bad creator could utilise deepfake technology to imitate a company's CEO or another senior executive in video or audio recordings. The deepfake might be used to tell staff to transfer funds to fake accounts under the pretence of essential business activities, causing financial loss for the

targeted organisation. Deepfake technology might be used to generate fake video testimonials or endorsements from well-known figures or financial experts, thereby promoting fraudulent investment schemes or possibilities. The persuasive nature of the deepfakes may fool potential investors into making financial contributions or investments that result in losses. Malicious creators might utilise deepfake technology to make fake movies or audio recordings with misleading information about publicly traded firms, economic indicators, or geopolitical events. By releasing false information, attackers can manipulate stock prices, commodity markets, or cryptocurrency values for personal benefit or to cause financial harm to others. Deepfake videos or audio messages could be used in phishing or social engineering attacks on individuals or financial institutions. For example, attackers could construct convincing deepfake recordings imitating bank personnel, government authorities, or trusted associates in order to fool victims into providing critical financial information, such as account credentials or payment authorization codes.

While these instances demonstrate potential concerns related with deepfake technology in the context of financial frauds, it is crucial to remember that documented cases may be limited or unknown due to the secretive nature of fraudulent activity. Furthermore, breakthroughs in deepfake detection and verification systems are being developed to reduce the hazards associated with synthetic media manipulation in financial transactions and communications.

VII. Discussion

Generative AI holds immense promise for driving innovation, creativity, and advancements across various industries. However, its potential uses and misuses necessitate a careful examination of existing laws and regulations. As generative AI systems become more autonomous and capable of independent decision-making, determining accountability and liability becomes challenging. Legal amendments should establish clear frameworks to attribute responsibility in cases of AI-generated content causing harm or infringing legal rights. By amending legal frameworks, and addressing concerns surrounding

intellectual property rights, privacy, and ethics, society can foster the responsible and beneficial deployment of generative AI. Legislation must be revised to establish legal frameworks that address the creation, distribution, and detection of fake content, ensuring accountability and protecting individuals and organizations from the harmful effects of misinformation. Generative AI relies on vast amounts of data, raising concerns about data privacy and security. Legal amendments should address these concerns by ensuring transparent data usage, informed consent, and robust security measures to protect sensitive information. Striking the right balance between enabling innovation and protecting individual rights is crucial to ensure that this transformative technology benefits humanity. To address the unique challenges posed by generative AI, it is imperative to amend existing laws and regulations.

Existing intellectual property frameworks may not adequately address the challenges posed by generative AI. Amendments are necessary to clarify ownership, attribution, and licensing rights concerning content generated by AI systems, protecting the rights of both creators and consumers. Intellectual property laws should be revised to account for the generation of original content by AI systems. This may involve establishing clear guidelines for ownership, attribution, and licensing of generative AI-generated content, ensuring that creators are appropriately recognized and protected. The privacy laws need to be strengthened to tackle the potential harms arising from the misuse of generative AI. Generative AI raises concerns about privacy and data protection. Amendments in legislation should focus on regulating the collection, storage, and use of personal data in generative AI systems to safeguard individual privacy rights. Stricter regulations can be implemented to deter the creation and distribution of maliciously generated content, safeguarding individuals' privacy and preventing the spread of misinformation. Existing copyright laws need to be amended to account for the challenges posed by generative AI. New regulations should address issues of ownership, attribution, and fair use of content generated by AI systems.

Ethical considerations should be at the forefront of legal amendments concerning generative AI. Transparency requirements could be imposed to ensure that generated content is distinguishable from human-created content, reducing the potential for deception.

Additionally, guidelines for the responsible development and deployment of generative AI systems should be established, promoting accountability and mitigating potential risks. Laws and regulations should encourage the development and adoption of ethical guidelines for generative AI research and applications. Furthermore, mechanisms for accountability, transparency, and auditing of AI systems must be established.

Given the potential uses and misuse of generative AI, it is crucial to update existing laws and regulations to address the associated ethical and societal challenges. Legal amendments should focus on three key aspects: accountability, consent, and transparency. Accountability measures should be established to ensure that the creators and users of generative AI technologies bear responsibility for the content generated. This can involve holding individuals or organizations accountable for the misuse of generative AI, especially in cases of malicious deepfakes or other harmful manipulations. Consent frameworks need to be strengthened to protect individuals' rights and privacy. Clear guidelines should be established regarding the generation and dissemination of synthetic content involving real individuals, ensuring that consent is obtained and that there are strict limitations on the use of personal data. Transparency regulations should be enacted to enhance the explainability and traceability of generative AI systems. This includes requiring clear identification of generated content and implementing mechanisms that allow users to verify the authenticity of media. By promoting transparency, users can make informed decisions and distinguish between genuine and manipulated content.

VIII. Implications

The implications of this research can shape future discussions on copyright laws, licensing agreements, and attribution practices in the context of AI-generated content. The implications of this study are divided into two sections i.e., theoretical and practical implications. Theoretical implications reflect the current study's contribution into the literature while practical implications show how this study contributes to the field of legal policies and procedures.

VIII.1. Theoretical Implications

The study on generative AI has significant theoretical implications for ethical and legal frameworks, particularly in terms of liability, accountability, and bias mitigation. It contributes to the ongoing debate on legal frameworks attributing liability to developers, users, or AI systems themselves. Moreover, it addresses bias in AI systems and aids in the development of fair and unbiased algorithms that prioritize fairness, transparency, and diversity for equitable outcomes. This research proposes measures that specifically target the risks created by AI applications. It advocates for the identification of high-risk applications and the establishment of clear requirements for generated AI systems used in such applications. Furthermore, it emphasizes the need for defining specific obligations for both AI users and providers of high-risk applications. To ensure safety and compliance, the research recommends the implementation of a conformity assessment before the AI system is deployed or made available in the market. This study proposes the enforcement of regulations and policies once an AI system is placed in the market.

Fair and Transformative Use: Fair use is a US legal doctrine (as recently upheld by the US Supreme Court) that allows limited use of copyrighted material without permission under certain circumstances (King, 2023, p. 124). To determine whether an AI-generated work qualifies for fair use, factors such as the purpose, nature, extent, and effect of its use are needed to be considered. Transformative use is often considered an important factor in fair use analysis, which involves adding new meaning or expression to the copyrighted work.

Obligations and Responsibilities: Determining liability for copyright infringement in AI-generated works can be complex, involving questions regarding the role of AI developers, users, and artificial intelligence itself. The responsibility for ensuring compliance with copyright law lies with both the creator and the user of AI-generated works. Determining the rightful copyright owner becomes challenging if the AI system operates without human intervention.

The Indian Copyright Act, 1957[12] and the Patents Act, 1970[13] make specific provisions for fair treatment and enumerated exceptions for copyright infringement. The use of copyrighted material for training AI models is kept on the legal gray list. As such copyright laws do not protect any creation generated solely by AI, even if it stems from a human-generated text indicator. Observations and decisions of international courts and other jurisdictions, such as the recent US Supreme Court decision on copyright and AI, may influence the interpretation of fairness in Indian copyright law.[14]

Indian copyright law and fair use provisions will need to be adapted to address the challenges posed by AI-generated content. The purpose of the use is crucial, whether the AI-generated content is intended for commercial gain or non-profit educational purposes. The nature of the copyrighted work should be evaluated, along with the amount and substantiality of the portion used in relation to the entire copyrighted work. Another crucial consideration is the effect of AI-generated content on the potential market or the value and importance of the original copyrighted work. It is essential to update intellectual property laws to keep pace with advancements in AI technology, ensuring they encompass the intricacies of AI-generated content. The implementation of data use and governance policies, along with oversight and compliance mechanisms, is necessary to regulate AI projects effectively. To protect copyright, it would be prudent to mandate AI firms to appoint compliance officers who are responsible for copyright protection, conducting audits, and performing assessments. These measures collectively aim to strike a balance between innovation and the preservation of intellectual property rights in the realm of AI-generated content in India. The intersection between copyright infringement and AI may impact the development of AI technology and

[12] The Indian Copyright Act No. 14 of 1957, enacted by the Parliament of India on 4 June 1957.

[13] The Patents Act No. 39 of 1970, enacted by the Parliament of India on 19 September 1970.

[14] AI and Copyright Law: Understanding the Challenges, 2023. Available at: https://www.wileyconnect.com/AI-and-Copyright-Law-Understanding-the-Challenges [Accessed 15.05.2024].

its potential applications. Establishing a balance between protecting the rights of copyright owners and promoting innovation in the field of AI is essential for the development and progress of this field.

VIII.2. Practical implications

This research study has the potential to contribute to the development of legislation concerning copyright, attribution, and licensing issues regarding AI-generated content. It can aid in the establishment of laws that set up clear guidelines for assigning liability and holding accountable the individuals or organizations involved in the creation and implementation of AI systems.

The study's findings on generative AI can also contribute to the formulation of ethical guidelines for its development and deployment. These guidelines can serve as a fundamental framework for formulating legislation aimed at governing the application of AI within sensitive domains, including healthcare, finance, criminal justice, and autonomous vehicles.

By establishing clear boundaries and prescribing acceptable principles and procedures, these norms would facilitate the conscientious and morally upright utilization of AI technology, promoting responsible conduct and ethical practices. The research emphasizes the significance of promoting public awareness and education about AI technologies, including their capabilities and potential impact on society. It suggests the collaboration of policymakers and stakeholders in the promotion of AI literacy, ensuring that individuals possess a comprehensive understanding of the implications and risks associated with generative AI.

IX. Conclusion

This research study highlights the pressing need and significance of establishing comprehensive legal frameworks tailored specifically for the field of generative artificial intelligence. Through addressing key areas such as intellectual property, ethics, privacy, and collaboration, policymakers can cultivate responsible and innovative AI development, all while protecting the rights and welfare of individuals and society at

large. The study highlights the crucial importance of comprehensive laws and regulations that encompass various facets such as intellectual property rights, privacy concerns, accountability, and liability about AI-generated content. Moreover, it emphasizes the significance of interdisciplinary collaboration among technologists, policymakers, legal experts, and other stakeholders.

A unified and concerted effort involving all relevant parties is imperative to navigate the intricate legal implications of generative AI and to develop robust and adaptable regulatory frameworks. Furthermore, this study offers invaluable insights into the legal implications and challenges associated with the emergence of generative AI. By addressing these challenges through the implementation of updated legal frameworks, ethical guidelines, and interdisciplinary collaboration, we can fully harness the immense potential offered by generative AI while concurrently safeguarding the rights, privacy, and overall well-being of individuals and society at large.

This study focuses attention on the urgent need to reform the current laws and regulations to effectively address the generative AI's legal complications. The research study recommends modifications in legal framework to distinctly ensure the responsibility of the AI generated content. Furthermore, this study stresses to chart out clear ethical guidelines for the development and responsible deployment of generative artificial intelligence. The need of the hour is to inculcate ethics related content in the curriculum of primary and secondary education in schools. A clear-cut set of punishments need to be specified by the respective governments in the IT Acts / Cyber laws of their countries to tackle misuse of generative artificial intelligence.

However, this research study on generative AI and laws faces a significant limitation, namely the potential presence of data bias. The study is done in the context of Indian laws, future studies could be carried out on other countries' laws. This issue necessitates future research endeavors aimed at advancing the development of legal and policy frameworks that effectively tackle the legal challenges posed by generative AI. Several critical aspects require attention, including liability, intellectual property, data handling, privacy, and accountability. To make substantial progress, future investigations on

generative AI and laws should strive to overcome various limitations, encompassing but not limited to data bias, ethical considerations, legal interpretation, adversarial attacks, human-AI collaboration, regulatory frameworks, and user experience. By systematically addressing these areas, researchers can significantly contribute to the establishment of robust, equitable, and reliable generative AI systems within the legal domain.

References

Anderljung, M. and Hazell, J., (2023). Protecting Society from AI Misuse: When are Restrictions on Capabilities Warranted? *arXiv preprint arXiv:2303.09377,* doi: 10.48550/arXiv.2303.09377.

Aydın, Ö. and Karaarslan, E., (2023). Is ChatGPT leading generative AI? What is beyond expectations? *Academic Platform Journal of Engineering and Smart Systems*, 11(3), pp. 118–134, doi: 10.21541/apjess.1293702.

Bontridder, N. and Poullet, Y., (2021). The role of artificial intelligence in disinformation. *Data & Policy*, 3, p. e32, doi: 10.1017/dap.2021.20.

Campbell, C., Plangger, K., Sands, S. and Kietzmann, J., (2022). Preparing for an era of deepfakes and AI-generated ads: A framework for understanding responses to manipulated advertising. *Journal of Advertising*, 51(1), pp. 22–38, doi: 10.1080/00913367.2021.1909515.

Chan, A., (2023). GPT-3 and InstructGPT: Technological dystopianism, utopianism, and "Contextual" perspectives in AI ethics and industry. *AI and Ethics*, 3(1), pp. 53–64, doi: 10.1007/s43681-022-00148-6.

Chaturvedi, S. and Kumar, H., (2019). Deepfakes and beyond: The new landscape of political propaganda. *The Hindu*. Available at: https://www.thehindu.com/elections/lok-sabha/from-it-bots-to-ai-deepfakes-the-evolution-of-election-related-misinformation-in-india/article68015342.ece [Accessed 15.05.2024].

Cuthbertson, A., (2018). Obama deepfake warns of "terrifying" future for fake news. *The Independent*. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/obama-deepfake-jordan-peele-video-fake-news-a8313901.html [Accessed 11.05.2024].

De Angelis, L., Baglivo, F., Arzilli, G., Privitera, G.P., Ferragina, P., Tozzi, A.E. and Rizzo, C., (2023). ChatGPT and the rise of large language models: the new AI-driven infodemic threat in public health. *Frontiers in Public Health*, 11, pp. 1–8, doi: 10.3389/fpubh.2023.1166120.

De Rancourt-Raymond, A. and Smaili, N., (2023). The unethical use of deepfakes. *Journal of Financial Crime*, 30(4), pp. 1066–1077, doi: 10.1108/JFC-04-2022-0090.

Dogru, T., Line, N., Hanks, L., Acikgoz, F., Abbott, J.A., Bakir, S., Berbekova, A., Bilgihan, A., Iskender, A., Kizildag, M. and Lee, M., (2023). The implications of generative artificial intelligence in academic research and higher education in tourism and hospitality. *Tourism Economics*, pp. 1083–1094, doi: 10.1177/13548166231204065.

Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A. and Galanos, V., (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, pp. 1–47, doi: 10.1016/j.ijinfomgt.2019.08.002.

Dwivedi, Y.K., Kshetri, N., Hughes, L., Slade, E.L., Jeyaraj, A., Kar, A.K., Baabdullah, A.M., Koohang, A., Raghavan, V., Ahuja, M. and Albanna, H., (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, pp. 1–63, doi: 10.1016/j.ijinfomgt.2023.102642.

Ferrara, E., (2023). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. *Sci*, 6(1), pp. 1–15, doi: 10.3390/sci6010003.

Fiske, A., Henningsen, P. and Buyx, A., (2019). Your robot therapist will see you now: ethical implications of embodied artificial intelligence in psychiatry, psychology, and psychotherapy. *Journal of medical Internet research*, 21(5), p. e13216, doi: 10.2196/13216.

George, A.S. and George, A.H., (2023). Deepfakes: The Evolution of Hyper Realistic Media Manipulation. *Partners Universal Innovative Research Publication*, 1(2), pp. 58–74, doi: 10.5281/zenodo.10148558.

Haluza, D. and Jungwirth, D., (2023). Artificial Intelligence and Ten Societal Megatrends: An Exploratory Study Using GPT-3. *Systems*, 11(3), pp. 1–18, doi: 10.3390/systems11030120.

He, T., (2019). The sentimental fools and the fictitious authors: rethinking the copyright issues of AI-generated contents in China. *Asia Pacific Law Review*, 27(2), pp. 218–238, doi: 10.1080/10192557.2019.1703520.

Illia, L., Colleoni, E. and Zyglidopoulos, S., (2023). Ethical implications of text generation in the age of artificial intelligence. *Business Ethics, the Environment & Responsibility*, 32(1), pp. 201–210, doi: 10.1111/beer.12479.

Jobin, A., Ienca, M. and Vayena, E., (2019). The global landscape of AI ethics guidelines. *Nature machine intelligence*, 1(9), pp. 389–399, doi: 10.1038/s42256-019-0088-2.

Kar, A.K., Varsha, P.S. and Rajan, S., (2023). Unravelling the impact of generative artificial intelligence (GAI) in industrial applications: A review of scientific and grey literature. *Global Journal of Flexible Systems Management*, 24(4), pp. 659–689, doi: 10.1007/s40171-023-00356-x.

Khowaja, S.A., Khuwaja, P., Dev, K., Wang, W. and Nkenyereye, L., (2024). Chatgpt needs spade (sustainability, privacy, digital divide, and ethics) evaluation: A review. *Cognitive Computation*, pp. 1–23, doi: 10.1007/s12559-024-10285-1.

Kietzmann, J., Lee, L.W., McCarthy, I.P. and Kietzmann, T.C., (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), pp. 135–146, doi: 10.1016/j.bushor.2019.11.006.

King, Y.M., (2023). Written Statement: Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith. *Chicago-Kent Journal of Intellectual Property*, 23 (1), pp. 124–126.

Ling, D., (2023). Analysis on Tort Liability of Generative Artificial Intelligence. *Science of Law Journal*, 2(12), pp. 102–107, doi: 10.23977/law.2023.021215.

Lucaj, L., van der Smagt, P. and Benbouzid, D., (2023). AI Regulation Is (not) All You Need. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency,* pp. 1267–1279, doi: 10.1145/3593013.3594079.

Maras, M.H. and Alexandrou, A., (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof*, 23(3), pp. 255–262, doi: 10.1177/1365712718807226.

Meskys, E., Kalpokiene, J., Jurcys, P. and Liaudanskas, A., (2020). Regulating deep fakes: legal and ethical considerations. *Journal of Intellectual Property Law & Practice*, 15(1), pp. 24–31.

Mittelstadt, B., (2019). Principles alone cannot guarantee ethical AI. *Nature machine intelligence*, 1(11), pp. 501–507, doi: 10.1038/s42256-019-0114-4.

Mondal, S., Das, S. and Vrana, V.G., (2023). How to bell the cat? A theoretical review of generative artificial intelligence towards digital disruption in all walks of life. *Technologies*, 11(2), pp. 1–17, doi: 10.3390/technologies11020044.

Montasari, R., (2024). Responding to Deepfake Challenges in the United Kingdom: Legal and Technical Insights with Recommendations. In: *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses*. Cham: Springer International Publishing, pp. 241–258, doi: 10.1007/978-3-031-50454-9_12.

Moulaei, K., Yadegari, A., Baharestani, M., Farzanbakhsh, S., Sabet, B. and Afrash, M.R., (2024). Generative artificial intelligence in healthcare: A scoping review on benefits, challenges and applications. *International Journal of Medical Informatics*, p. 105474, doi: 10.1016/j.ijmedinf.2024.105474.

Pérez, J., Castro, M. and López, G., (2023). Serious Games and AI: Challenges and Opportunities for Computational Social Science. *IEEE Access,* doi: 10.1109/ACCESS.2023.3286695.

Porsdam Mann, S., Earp, B.D., Nyholm, S., Danaher, J., Møller, N., Bowman-Smart, H., Hatherley, J., Koplin, J., Plozza, M., Rodger, D. and Treit, P.V., (2023). Generative AI entails a credit — blame asymmetry. *Nature Machine Intelligence*, pp. 1–4, doi: 10.1038/s42256-023-00653-1.

Romero Moreno, F., (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. International Review of Law. *Computers & Technology*, pp. 1–30, doi: 10.1080/13600869.2024.2324540.

Shoaib, M.R., Wang, Z., Ahvanooey, M.T. and Zhao, J., (2023). Deepfakes, misinformation, and disinformation in the era of frontier ai, generative ai, and large ai models. *2023 International Conference on Computer and Applications (ICCA)*, pp. 1–7, doi: 10.1109/ICCA59364.2023.10401723.

Thongmeensuk, S., (2024). Rethinking copyright exceptions in the era of generative AI: Balancing innovation and intellectual property protection. *The Journal of World Intellectual Property*, pp. 1–15, doi: 10.1111/jwip.12301.

Uzun, L., (2023). ChatGPT and academic integrity concerns: Detecting artificial intelligence generated content. *Language Education and Technology*, *3*(1), pp. 45–54. Available at: http://www.langedutech.com/letjournal/index.php/let/article/view/49/36 [Accessed 11.05.2024].

Yang, Z., Wu, J.G. and Xie, H., (2024). Taming Frankenstein's monster: Ethical considerations relating to generative artificial intelligence in education. *Asia Pacific Journal of Education*, pp. 1–14, doi: 10.1080/02188791.2023.2300137.

Information about the Authors

Animesh Kumar Sharma, PhD in Marketing, Research Scholar, Mittal School of Business, Lovely Professional University, Phagwara, Punjab, India
mr.animesh@gmail.com
ORCID: 0000-0002-6673-319X

Dr. Rahul Sharma, PhD in Marketing, Professor, Mittal School of Business, Lovely Professional University, Phagwara, Punjab, India
rahul.12234@lpu.co.in
ORCID: 0000-0001-8880-7527

Article

DOI: 10.17803/2713-0533.2024.3.29.452-490

Cyber-Threat Landscape in Healthcare Industry and Legal Framework Governing Personal Health Information in India

Niharika Raizada[1], **Pranjal Srivastava**[2]

[1] *CHRIST University, Bengaluru, India*

[2] *Rashtriya Raksha University, Gandhinagar, India*

Abstract: 2021 and 2022 have been the years of frequent cyber-attacks. India remains in the top 25 countries severely affected by the continuous cyber-attacks and tops the list. The healthcare department is amongst the most affected area. In 2020, the healthcare department suffered a severe impact with around 348K cyber-attacks alone on Indian healthcare infrastructure. The recent occurrence of cyber-attack on AIIMS hospital in December 2022 followed by several other incidences of data breaches have made the concerned authorities pro-active on exercising vigilance and reforming the legal and technical system to protect the health infrastructure. This paper has been developed on extensive literature and focuses on describing the nature of electronic health records, the risks they are exposed to along with as to why they are so susceptible to these cyber-risks. Furthermore, the paper also deals with different kinds of threats affecting the privacy and security of electronic health records specifically. The paper analyzes Indian legal framework, briefly compares it with international legal framework (specifically US & EU) and highlights the shortcomings in Indian legislative framework followed by laying down certain recommendations primarily highlighting the possible changes required in Indian legal framework and practices that can be adopted at organizational level to overcome and mitigate such risks.

Keywords*:* cybersecurity; electronic health records (EHR); healthcare; personal health information; cyber-threats

Cite as: Raizada, N. and Srivastava, P., (2024). Cyber-Threat Landscape in Healthcare Industry and Legal Framework Governing Personal Health Information in India. *Kutafin Law Review*, 11(3), pp. 452–490, doi: 10.17803/2713-0533.2024.3.29.452-490

Contents

I. Introduction

With the gradual development of technology and its impact on different kinds of infrastructure in various departments and services, the risks have also gradually increased. The technological progress has led to a constant redefining of daily life. The healthcare department is no exception to this. A dramatic shift from paper records to electronic health records has undoubtedly reduced the workload of the front-line

workers, but it has nevertheless increased the risk of unlawful access to such records. Electronic health records are electronic versions of the medical records stored and organized by the healthcare service providers like hospitals, clinics and the internet of medical things (IoMT). They are the patients' history that can be referred to or interoperate between hospitals (Keshta and Odeh, 2021, p. 177). These include essential administrative as well as the clinical data that basically include the care and services given to an individual by a health provider. These are inclusive of details such as demographics, progress reports, problems, medications, important signs, MRI and CTC scans, medical history, immunization reports, laboratory data, radiology reports, etc. (Keshta and Odeh, 2021, p. 178). These electronic medical records are prone to risks and threats of a number of cybersecurity issues. The report published by QuickHeal Report in 2021[1] highlighted that India has suffered most cyber-attacks along with 24 other countries. The most of the attacks were targeted at hospitals, government and defense bodies. Most of them were malware and ransomware attacks. The malware, often also called as malicious software like Advanced Persistent Threats (APT), often targeted the departments and led to data theft.[2] One of such malware is APT10 that targeted at food processing industries, hospitals, banks, automobile industries. APT10 misled the security community in believing that this was a Transparent Tribe.

Ransomware is a variant of malware itself (Reshmi, 2021). Ransomwares attacks are generally financially motivated (Alder, 2021). This malware gives threat actors a large payout in a matter of days after conducting an attack and ransoms are often paid to allow files to be restored or to prevent the release or sale of stolen sensitive data. Ransomware usually either aims encodes the important file or prevent the users from using the devices by locking them and further demanding the organization to pay ransom in order to retrieve the access (Tully et al., 2020).

The cyber-attacks shot up during the Covid-19 period with several number of cyber-incidents covering areas like spyware attacks (Hakak

[1] Seqrite Annual Threat Report 2021. Available at: https://www.seqrite.com/seqrite-annual-threat-report-2021#dflip-df_book_full/1/ [Accessed 23.03.2024].

[2] Seqrite Annual Threat Report 2021.

et al., 2020), DDOS, ransomware (Muthuppalaniappan and Stevenson, 2021), digital fraud (Škiljić, 2020, p. 52), panic, disinformation, etc. The cyber-incidents levered an approximate cost around in millions and exposing the critical data to the illegal assessors. The data of patients and users of various medical services were accessed without consent and sold to various third parties. However, primary questions here are why would they target the medical data that happens to be a sensitive data (Blessing et al., 2022) and what would hackers do with our data?[3] The answer in brief is the medical infrastructure has an issue of weak cybersecurity and it makes it easier for hackers to commit data theft (Pal et al., 2024). Also, the stolen data is either sold on the deep dark online market which can enable the buyer on the market commit felony cases like tax evasion, identity theft, etc. The importance and the utter necessity of cybersecurity comes into play when the very fact is highlighted that the patient's data stored and compiled as EHRs are often stolen and utilized in identity thefts or more serious offences like tax evasion (Coventry and Branley, 2018, pp. 48–52). There are thousands of malware attacks infecting the databases of the hospitals, laboratories, devices, etc. and gaining the access to our personal data stored, illegally.[4]

This particular research article provides for a detailed explanation on the nature and importance of storing and utilization of health data; highlights the major reasons as to why EHRs serve as honeypot for cybercriminals; explores the different elements involved in cybersecurity and underlying explanations for developing a resilient cybersecurity framework for EHRs; provides thorough analyses of the literature available identifying various forms of cyber-threats that severely affect the privacy and security of the EHRs; encompasses the present cybersecurity measures or laws in India protecting the EHRs succeeded by recommendations that can help in strengthening the overall cyber-infrastructure of the system of healthcare.

[3] Once Stolen, What Do Hackers Do with Your Data? *Secplicity — Security Simplified*. May 18. Available at: https://www.secplicity.org/2017/05/18/stolen-hackers-data/ [Accessed 21.09.2024].

[4] BBC News, (2016). Wiggins and Froome Medical Records Released by "Russian Hackers." *BBC News*. 2016. September 15. Available at: //www.bbc.com/news/world-37369705 [Accessed 23.03.2024].

II. Nature of Electronic Health Records

An EHR can be defined as the electronic version of a medical data of a patient that is stored and maintained by a particular health care provider for a certain period. It includes all the essential administrative and clinical data of the treatment, care and facilities given to an individual, e.g., demographics, progress reports, problems, medications, important signs, medical history, immunization reports, laboratory data and radiology reports. In simpler language, an EHR is an enhanced database prepared with respect to health and healthcare of a patient where all data and essential information is kept on electronic media (Negro-Calduch et al., 2021). EHR has capability of storing sensitive personal data relating to our health and care.

The medical records of a person comprise of the simple demographic records, the chronology of the ailments, any type of medical images, problems, medications, etc. The records of a patient stored in hospitals are essential for the purpose of quick reference and finding remedies for the ailments. The paper records cannot sometimes extensively trace data related to a particular person (Keshta and Odeh, 2021, p. 179), which has led most of the organizations shift their policies of preparing, storing and maintaining of paper medical records to electronic health records. An EHR is an electronic version of a medical data of a patient stored and maintained by a particular health care provider for a certain period. It includes all the essential administrative and clinical data regarding the treatment, care and facilities given to an individual. An EHR is an enhanced database prepared with respect to health and healthcare of a patient where all data and essential information is kept on electronic media (Negro-Calduch et al., 2021). It has a peculiar capability of storing sensitive personal data relating to the patient's health and care.

The EHR was introduced in 1960 (Gajwani, 2020) and it is defined as an electronic record keeping system which not only maintains the records but also enables interoperability and various secondary uses as well. For the first time, the guidelines were introduced in 2013 by Ministry of Health and Family Welfare. The guidelines were amended and developed further in 2016. The document set for EHR Guidelines

was stated to be a *"living document"* on account of reason that *"...These standards cannot be considered either in isolation or as 'etched in stone for all eternity.' These will need to undergo periodic review and update as necessary*."[5]

EHRs have played significant role in making access and sharing of health information easier and accessible. The EHR system is apparently providing better benefits, enhanced productivity in contrast to the traditional paper-based record storing system. The EHR is not limited to the electronic records maintained by the hospitals comprising information only regarding ailment along with the demographic and financial details of the patient; it also extends its area over health records obtained via Internet of medical things, wearable body area network, telemedicine, etc., which makes it easier for the general practitioners to derive a specific conclusion with the help of all relevant information at one place. The digitization of the personal health information has also played a significant role in making the records interoperable, i.e., the records are easily accessible to other departments as well. Interoperability is essential to attain better patient care, better prediction for health of populations and lower costs for healthcare services.

The EHR has a peculiar characteristic as it creates a paradox; health records cannot be shared due to their sensitive nature and it is also required to be shared to enable better results and cheaper costs.[6] Lack of interoperability might lead to restricted comprehension of patient and also collective health of population and will consequently result in higher costs and poor outcomes (Kawu et al., 2023). Interoperability is not just limited to records from the hospitals and clinics. With the advancement of The Internet of medical things and wearable body area network are also connected with the primary EHR/EMR to monitor diseases like hypertension, blood sugar, etc. However, there are certain issues on account of which interoperability of electronic records is not a trend. The records of a patient stored in hospitals are essential for

[5] Electronic Health Records (HER) Standards for India, (2016). Available at: https://bahmni.atlassian.net/wiki/spaces/BAH/pages/2983165963/EHR+Standards+across+various+countries [Accessed 21/09/2024].

[6] What is Interoperability in Healthcare? IBM Report. Available at: https://www.ibm.com/topics/interoperability-in-healthcare [Accessed 23.03.2024].

the purpose of quick reference and finding remedies for the ailments. However, the paper records stored have led to an extensive trail of the data related to particular person (Keshta and Odeh, 2021, p. 180), which has led most of the organizations shift their policies of preparing, storing and maintaining paper medical records to electronic health records.

III. Why Electronic Health Records are being Targeted?

With the enhanced use and advantages of EHR, they are now primary targets for advanced cyber-attacks. Besides, financial institutions and healthcare institutions are now the primary focus for data extortion and theft. Lack of stringent legislation and weak healthcare infrastructure are two chief reasons why healthcare institutions have been lately targeted to launch a cyber-attack. There is no set legal framework to govern compliance with the above-mentioned standards. However, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, were enacted under Information Technology Act, 2000. The rules apply to every "body corporate" concerned with holding and maintaining sensitive records. Besides the above stated rules, there have been several attempts at framing laws that primarily deal with sensitive personal data;[7] however, the solid framework for governing the digital personal and sensitive data is yet to come in force.

The lack of a concrete law makes the electronic health records vulnerable and prone to several issues relating to cyber security like data extortion, identity theft, malware attacks, selling of sensitive records in black market, etc.

The vital question in focus, however, is why anyone would want to steal any health record and what is the significance of a mere record comprising of demographic and health information. Indian healthcare institutions have been subject to nearly 1.9 million cyber-attacks in

[7] Several bills precede the current bill in motion in the Parliament. Bills like Personal Data Protection Bill, 2018; Digital Information in Healthcare Security Act, 2018 and Data Protection Bill, 2019 were prior attempt at making flawless framework for governing of digital health data specifically.

year of 2022 (Ang, 2022) and around millions of records comprising of extremely sensitive information of patients were leaked. The primary motivation behind these cyber-attacks can be outlined around financial gain, political or military advantage (Coventry and Branley, 2018, p. 48). Politically motivated cyber-threats amount to approximately 26 % of the global cyber-attacks (Desjardins, 2018) and such motivation preceded by initiation of any form of threat for spreading propaganda or posing serious threat to national security (Han and Dongre, 2014), e.g., NHS website's control was taken over by cyber-terrorists and pictures of gruesome ongoing civil war in Syria were posted (Sengupta, 2017).

Each electronic health record is sold on dark web for around 1,000 $ USD (Sudhanshu, 2022). A social security number is worth $ 3, while credit card details are worth 15–20 $ (Ibarra et al., 2019, pp. 115–137). On a rough estimate, a particular EHR is sold for over hundreds of dollars over dark web. The electronic records can apparently be (mis) used to either extort money from the victim whose record has been sold illicitly or expose it to public embarrassment and/or political assassination (Ibarra et al., 2019, pp. 115–137). In other scenario, there are also several secondary uses of EHRs; they are also generated and developed in a clinical trial.

A clinical data is generated in the form of in-effect patient diagnostics and consists of extremely private information. It is used for purposes other than medical treatment like medical research, preventive campaigns, establishing national and international statistics, allocation of resources, study epistemological trends (Richter and Thielscher, 2023; Shah and Khan, 2020). Earlier, the diagnosis from any particular clinical trial were stored and maintained in paper records but to enable accessibility and promote better maintenance of all the records, the EHR system was adopted.

Induction of health records into EHR system enables medical researchers to keep track after a drug has been introduced in a drug trial (Shah and Khan, 2020; Adebayo and AbdulAziz, 2014) for the purpose of scientific discovery, for the purpose of conducting observational studies (Hoffman and Podgurski, 2013), to track the effects and focus on quality improvement with the aim of rendering better treatments, (Hoffman and Podgurski, 2013) and also in cases where, if any sensitive or de-

anonymized information of a patient(s) gets public, the EHRs can prove to be rather a fatal legal injury against the person/entity/organization responsible for storing such health records (Howden, 2023, p. 23).

IV. Cybersecurity for Electronic Health Records

Cybersecurity guarantees safety of computer systems and networks against data breach, data theft, information leak or any form of harm to the hardware, software or any form of electronic data and any form of disruption of services. Cybersecurity is one of the most persistent challenges that every corporation working with digital information encounters. Unfortunately, healthcare industry faces several kinds of cyber-threats leading to disruption in functioning of health delivery services. There are several factors in play for such threats like lack of cybersecurity policy, lack of management of proper record, minimal training, education and awareness of staff and personnel about the procedures, etc. (Paliwal et al., 2023, p. 388).

Because of these factors, healthcare cybersecurity is threatened (Pears and Konstantinidis, 2021, p. 1675). Healthcare industry functions as a supply-chain network involving different stakeholders interconnected and exchange data amongst themselves. This data is in form of electronic health record (EHRs) that consists of tons of valuable information of a patient. Any particular EHR comprises of following information:

— Personal information (Name, contact details, details of relatives).

— Demographic details of the patient (residential, permanent address and office address).

— Social security number of the individual (like AADHAR, driving license number).

— Financial details (credit card, bank account details, ATM numbers).

— Medical history or details of ailments or information related to diseases suffered by the individual.

Cybersecurity revolves around three pillars of information security: confidentiality, integrity and availability also known as CIA

Triad (Langer, 2017, pp. 117–125). However, this model of information security (CIA Triad) has been extended to include Accountability as a non-repudiated pillar (Warkentin and Orgeron, 2020). Electronic health records (EHRs) are vulnerable to various cyber-risks that can compromise the confidentiality, integrity, and availability of patient information. Confidentiality refers to protecting the privacy of patient data, ensuring that only authorized individuals have access to it. Integrity involves maintaining the accuracy and trustworthiness of the data, preventing unauthorized modifications or tampering. Availability ensures that the data is accessible to authorized users when needed (Almaghrabi and Bugis, 2022, pp. 126–128). One significant cyber risk to EHRs is the potential for unauthorized access and data breaches. The importance of confidentiality is one of the key security requirements for IoT-based healthcare systems (Nasiri et al., 2019, pp. 253–258). They emphasize the need for measures such as authentication and authorization to ensure that only authorized individuals can access patient data. They also emphasize the importance of confidentiality as one of the ultimate security objectives for healthcare systems (Kawu et al., 2023). They discuss the risks associated with data breaches and the potential harm data breaches can cause to individuals.

Another cyber risk is the threat to the integrity of EHRs that discusses the lack of robust cybersecurity in healthcare, since it can lead to the lack of integrity and security of electronic health records (Yusuf and Ayinde, 2023). It is necessary to prepare a security framework for EHR systems that considers the integrity of health records (Ganiga et al., 2020, p. 455). Enough focus has been laid on the risks posed by ransomware attacks in the healthcare industry (Farringer, 2019, p. 91). The rapid transition from paper records to electronic platforms has increased the risk to patient data integrity. Ransomware attacks can render medical records inaccessible, compromising patient care and privacy. Farringer (2019, p. 91) emphasizes the need for coordinated efforts to address cybersecurity risks in the healthcare industry. The researcher highlighted that concern over cyber-attacks targeting medical information systems is growing. The illegal market for electronic health records has led to an increase in virtual attacks,

posing a threat to the reputation and financial stability of medical institutions. Protecting the network infrastructure that supports healthcare systems is crucial to mitigating these cyber risks (Angel, 2022, p. 3455).

Phishing and ransomware attacks are specific cyber risks that can compromise the integrity and availability of EHRs. Health care organizations are ideal targets for these attacks due to outdated cybersecurity systems and limited staff training on safety practices (Croke, 2020). These attacks can lead to the disclosure of patient health information, identity theft, and medical fraud, highlighting the wide-ranging consequences of cyberattacks in the healthcare sector (Croke, 2020). Availability is also a critical aspect of EHR security. It highlights the need for maintaining the availability of healthcare technology and the confidentiality of health records (Lekshmi, 2022). The unauthorized availability of EHR systems can be compromised and disrupt the functioning of the systems or cause downtime. In the extended version, accountability refers to ensuring traceability of performed activities or processes to specific individual or a group and such processes that cannot be repudiated. Non-repudiation is ensuring that a person cannot deny due to the authenticity of their credentials or any act like sending a message (Anderson, 2003, pp. 308–313).

It is essential to frame a flexible EHR system that ensures availability, confidentiality, and integrity by integrating different hospital information systems (Nielsen et al., 2019, p. 5). One of the key concerns is the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities (Coventry and Branley, 2018, p. 48). These vulnerabilities can be exploited by cyber attackers to disrupt the availability of EHRs and compromise patient care.

Remote access to EHRs is another cyber risk that can impact availability. With the increasing use of telemedicine, the remote access to electronic medical records of patients has become more widespread, making it a potential target for cyber-attacks (Sardi et al., 2020). Unauthorized access or manipulation of EHRs can lead to disruptions in healthcare services and compromise patient care.

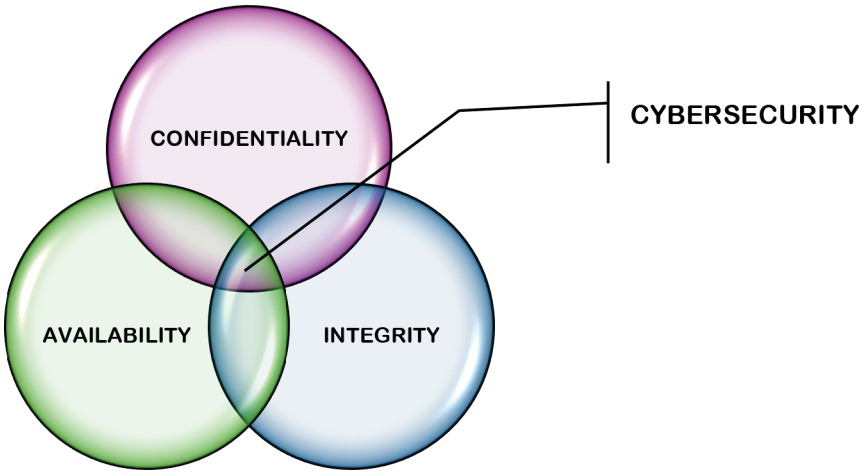

Figure 1. C-I-A Triad

The essence of cybersecurity underlies in the context of understanding what are the risks and vulnerabilities in the network. The cyber-risk has a wide meaning, it has been defined differently by different scholars. To understand what are the kinds of underlying threats to healthcare industry, it is also important to understand what cyber-risks and cyber-vulnerabilities are in healthcare industry.

IV.1. Vulnerability

Vulnerability with respect to cyber-infrastructure refers to internal component of the risk and specifies weakness in a digital system of organization. It refers to circumstances related to fact, processes, people or any phenomenon that can reduce the capacity of the organization to respond, recover and act against a risk or any event which is likely to occur because of such risk (Zodian, 2024, p. 20). Vulnerability refers to a weakness in an asset or in any infrastructure or implementation or operation that can be severely exploited by an adversary (Cox, 2008, p. 1749). Vulnerability can exist in software, hardware or in network (Savin and Anysz, 2021).

IV.2. Cyber Threats

A cyber-threat relates to occurrence of any incident with the capacity to result in loss or damage to asset or individual (Škiljić, 2020, p. 51). A threat can be anything ranging from cyber-attack to sophisticated forms of espionage, data breaches, identity theft, financial fraud, disruption of critical infrastructure. Threat is usually the exploitation of an existing weakness in the organization's infrastructure. The list of sources of threats is not exhaustive; this may include unsanctioned access, lack of cybersecurity policy, lack of awareness and training, information security breach, etc. A threat can emanate from frivolous motive or any act or omission of the perpetrator, which can be intentional or accidental in nature or can be altogether demonstrate perpetrator's incompetence. The origin of a threat can be external or within the organization. A threat does not necessarily should lead to a cyber-incident, if mitigated at an early stage. To analyze risk, threat is based on evaluating the intention and potential of the adverse party to perform a detrimental activity (Strupczewski, 2021, p. 105).

IV.3. Impact/Likelihood

It is significant to estimate potential damage that can be caused by a particular cyber-incident. One needs to take into consideration certain characteristics that are related to information security to ensure and maintain the three angles in CIA Triad. Therefore, careful analysis and evaluation of the organization's information security system should be done with respect to the loss of integrity, availability and confidentiality. The impact/likelihood/probability of occurrence should be analyzed as:

— High: Severely affects the goals and working of the organization.

— Medium: Leads to financial damage and may cause challenges for human resources.

— Low: Causes minor financial losses.

IV.4. Cyber-Risks

Risk is associated with the threat and likelihood of an uninvited incident and its adverse impact. It is a potential incident that can be discovered and quantified; likelihood and impact can be assessed. It

is estimated as the combination of probability and consequence of any hostile event like a threat. When numerical values represent the probability and consequences (impact), the anticipated risk is calculated by multiplying these values, taking uncertainty into account. In the realm of security, risk assessment involves analyzing and aggregating three well-established factors: threat, vulnerability, and consequence. When probability and consequences are quantified, the expected risk is determined by multiplying these numerical values, incorporating considerations for uncertainty. In the context of security, the evaluation of risk involves analyzing and consolidating three widely acknowledged factors: threat, vulnerability, and consequence. This approach provides a comprehensive understanding of potential risks and aids in effective risk management. Risk can be managed by implementation of appropriate controls and different response and recovery strategies that may reduce the likelihood and impact of a threat or an unwanted event (Zahid et al., 2021). Thus, the following equation can be provided for cyber-risks assessment:

Vulnerability × Threat × Impact = Risk

V. Kinds of Cyber-Threats to Healthcare Industry

It is significant to note that although there is an upside to digitization of healthcare industry, the complexity of computing environment makes it easier for cybercriminals to exploit vulnerabilities. Information security incidents that include sensitive health information and different malware attacks on critical services pose incredible danger (Cremer et al., 2022, p. 698). Medical staff can easily access patient information. Offenders can abuse illegally obtained information in several ways, e.g., commission of identity theft, initiate unlawful transactions or even blackmail victims (Martin et al., 2017).

Another possible scenario is installation of a malicious code or committing sensitive credentials. Consequently, the entire network suffers. One of the most frequently occurring incidents is stealing information through genuinely looking websites or emails. The primary element to gain patient confidence is safeguarding the privacy and security of the EHR and personal health information during medical

visits. Healthcare organizations face several cybersecurity issues every year. In the USA approximately 88 % of healthcare organizations have faced some form of cyber-attack usually performed in the form of ransomware attacks, cloud compromise, phishing emails and supply chain attacks (Bhatia, 2022, p. 103). Such cyber-incidents have caused healthcare organizations to suffer losses for more than 100 million $ USD and have also affected the patients or the end-users availing the services. Such incidents have in different ways have also affected confidentiality, integrity and availability of medical information. Some common but severe form of cyber-threats are discussed below in Table 1.

Table 1: Different kinds of cyber-threats

Types of Cyber-Threats	Description
Phishing Attacks (Coventry and Branley, 2018)	Phishing e-mail is the way to gain access to valuable credentials like passwords, medical information, and financial data using targeted communication methods like email or text messages where the prospective victim clicks the link and is directed to malicious code or malware
Remote Desktop Protocol (Thamer and Alubady, 2021)	Remote desktop protocol is copyrighted protocol that provides ability to users to connect to their respective workspace. RDP allows access to managers and employees to their systems from any location. Such remote access is followed by severe vulnerability and can be exploited using brute force attacks to gain valuable credentials like username and passwords
Removable Media and Universal Serial Bus (Thamer and Alubady, 2021)	Removable media and Universal Serial Bus (USB) is a way of externally infiltrating the targeted devices and it is different from attacks based on internet-based
Ransomware (Nusairat et al., 2023, p. 238)	Ransomware is the form of malware that encrypts the recorded information and decryption is only possible after ransom is paid to the perpetrator

DDOS (Argaw et al., 2020, p. 146)	Distributed denial of service attacks floods a particular server with false connection permission to interfere with its working. This coordination utilizes several end-points and IoT devices that by force affects through malware infection through botnet
Internal Threats (Javaid et al., 2023)	Insider threats are security risks arising from individuals within an organization exploiting privileged access to compromise information security intentionally or inadvertently
Breach of Data (Javaid et al., 2023)	Data breach incidents are no usually the result of form risk however they can be consequence of any malware, insider attacks or compromised emails

VI. Legal and Regulatory Framework for Protection of Electronic Health Records

The peculiar sensitive nature of digital health information is known internationally in order to ensure that data is protected specifically (Kaplan, 2014). It is essential to prevent privacy from being infringed in order to utilize for better prospects like patient care, progressive public health and research purposes (Price et al., 2019, p. 448). The present legal framework and regulatory measures in India do neither. These legal instruments were not brought in force for the purpose to promote the progressive research and improve public health. Instead, they are established for obsolete and redundant technologies (Kaplan, 2020). As the technology upgrades, data gathered for certain purpose may become interdependent with other kind of data and the basic notion of privacy may also evolve gradually with time, which may render a particular law that may be not completely obsolete but definitely inadequate and having several loopholes.

Furthermore, we know little about how data are collected, generated, combined, used, and protected, as well as about the specific algorithms that collect, process, and use it. For example, communication companies track users' locations and personal contact data, which can inadvertently reveal sensitive health information. In the United States, as in many other countries, privacy regulation often relies on de-identification to

preserve privacy, particularly under laws like HIPAA and the Common Rule. However, this approach only covers certain types of data. With advancements in data analysis, re-identifying de-identified data has become increasingly feasible, rendering de-identification an inadequate legal protection in many cases.

This part of the article will highlight legal and regulatory issues in the existing legal framework.

Issues in Legal and Regulatory Framework. The threats and risks as provided in 5th section of this paper have not been discussed or mentioned precisely in the Indian legal framework that comprises legislations, policies and guidelines. Information Technology Act, 2000, is the primary Indian legislation that governs protection of data and individual's privacy relating to their health data and medical records.

VI.1. Primary Legislations and Policies

VI.1.1. Information Technology Act, 2000

Information Technology Act, 2000[8], is a comprehensive legislation focused on governance of several different electronic transactions and interchange electronic data. The Act came into force on 9 June 2000 and specified in its Preamble that it is "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies." IT Act provides for several offences (20021 § 43A). Under Chapter IX, however, the Act does not specifically deal with data breach or cyber-attack. The Act provides for compensation on part of the body corporate on account of failure to protect sensitive data from being stolen or unlawfully accessed (Information Technology Act, 2000, 21 § 43A) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, is one of the corresponding rules that aim at explicit protection of sensitive personal

[8] Available at: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf [Accessed 21.09.2024].

data and information and these Rules are supposed to be read with Section 43A (Information Technology, 200021 21 § 43A).

Rule 3 of the IT Rules, 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, Part II-Sec. 3(i) § Rule 3, 2011) defines Sensitive Personal Data and information comprising of information relating to:

i. password;

ii. financial information such as Bank account or credit card or debit card or

iii. other payment instrument details;

iv. physical, physiological and mental health condition;

v. sexual orientation;

vi. medical records and history;

vii. Biometric information;

viii. any detail relating to the above clauses as provided to body corporate for providing service; and

ix. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

The Rules, although provide for umbrella provisions for protection of sensitive data and information, do not provide for specific provisions and classification of health and medical data and kinds of data constituting health data. Furthermore, the Rules have major application to body corporate only and not to other organizations or individuals. Consequently, there will not be any imposition of compensation on individuals or other organizations that are not within the ambit of "body corporate."[9]

VI.1.2. Electronic Health Records Standards, 2016

Electronic Health Records Standards, 2016[10] provides for extensive standards that specifically apply on healthcare institutions or anybody, which lead to creation of medical history and record. In a way, EHR

[9] Information Technology Act, 21 § 43A Explanation.

[10] Electronic Health Records Standard (Q-11011/3/2015-eGov). Available at: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf [Accessed 21.09.2024].

Standards, 2016, fill the gaps with respect to terminologies, protection, and prevention from unlawful access and in relation to health data primarily. The Standards, specify International Standards, are used not only for protection of sensitive data but also for maintenance, sharing or enhancing of interoperability of electronic health records as well. In addition to this, the Standards also lay down guidelines with respect to network connectivity, interoperability and data ownership. Most importantly, they define and differentiate in an elaborate manner between "Electronic Health Record (EHR)," "Electronic Medical Records" (EMR), "Electronic Personal Health Information" (E-PHI) and "Personal Health Record" (EPR).

a. Electronic Health Record

An EHR has been defined as "one or more repositories of information in computer processable form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users, represented according to a standardized or commonly agreed logical information model."[11]

b. Electronic Medical Record

An EMR has been defined as a varied form of EHR "restricted in scope to the medical domain or at least very much medically focused."[12]

c. Electronic Personal Health Information

E-PHI has been defined as any protected health information that has been "created, stored, transmitted, or received electronically" (Savin and Anysz, 2021). The data created, recorded, sent, transmitted or received through any electronic medium is covered under this term.

d. Personal Health Record

A PHR has been defined as documentation of any form of patient information including medical history, vaccinations or even medicines prescribed and purchased.[13]

The EHR Standards, 2016 is a comprehensive document but lacks enforceable character due to unavailability of such provision. Subsequently, due to lack of enforceability, the application and the

[11] Electronic Health Records Standard (Q-11011/3/2015-eGov).

[12] Electronic Health Records Standard (Q-11011/3/2015-eGov).

[13] Electronic Health Records Standard (Q-11011/3/2015-eGov).

norms so provided within the same, act as mere recommendations or guidelines for health service providers and hence there is no imposition of penalty or fine on lack of implementation of such standards by the service providers.

VI.1.3. The Digital Data Protection Act, 2023

The Digital Data Protection Act, 2023 (DPDA) is a comprehensive proposed legislation for the governance of the personal digital data. It states, "The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto."[14] The consent of an individual is supposed to be "free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose."[15] The consent sought should be followed by conveying all the relevant information describing the purpose of processing such data.[16] Section 7 stipulates that data so processed is "for legitimate purposes" along with the condition that Data Principal has willingly provided the personal data and "has not indicated to the Data Fiduciary that she does not consent to its use." Besides, data fiduciary can also process medical data of data principal in two other scenarios:

a. for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;[17]

b. for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health.[18]

[14] DPDA, 2023, CG-DL-E-12082023-248045 22 of 2023. § Preamble, 2023.
[15] DPDA, 2023, § 6, 2023.
[16] DPDA, 2023, § 5, 2023.
[17] DPDA, 2023, § 7 (f), 2023.
[18] DPDA, 2023, § 7(g), 2023.

Section 2(s) of DPDPA provides additional provision for "Significant Data Fiduciary."[19] A significant data fiduciary is a "Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under Section 10."[20] A significant data fiduciary is appointed by Central Government on the basis of different factors including:

a. the volume and sensitivity of personal data processed;
b. risk to the rights of Data Principal;
c. potential impact on the sovereignty and integrity of India;
d. risk to electoral democracy;
e. security of the State; and
f. public order.[21]

The relevant provisions do not provide for privacy, security and confidentiality of health data specifically and most importantly, it does not define sensitive personal data nor differentiate between sensitive and non-sensitive personal data. Consequently, there are no provisions for regulation of the same. The Digital Personal Data Protection Act, 2023 ensures that personal data is processed only after consent and for legitimate uses.[22]

VI.2. Regulatory Framework

VI.2.1. National Digital Health Ecosystem, 2019

National Digital Health Ecosystem, 2019 (NDHE) is a framework developed for easier interchange of health data between health service providers and stakeholders. NDHE developed overtime since 2019 to National Digital Health Blueprint (NDHB) in 2020 and finally rolled out as Ayushman Bharat Digital Mission (ABDM) in 2020 in 6 Union territories on 15 August (National Heath Mission, 2022). ABDM has 5 major components: ABHA Number, UHI interface, Health Professional Registry, Health Facility Registry and ABHA Mobile App (PHR app). ABDM provides for data exchange between all of these components for it primary objective of enhancing interoperability and reducing

[19] DPDA, 2023, § 2, 2023.
[20] DPDA, 2023, § 2, 2023.
[21] DPDA, 2023, § 10(1), 2023.
[22] DPDA, 2023, § 4 Preamble, 2023.

paper health records. Such interchange is governed by guidelines and policies brought out in public with ABDM framework, of which the most relevant here is Health Data Management Policy (HDMP) that provides for several aspects of data exchange along with how health data is supposed to be exchanged in a safe and confidential manner only after explicit consent of the patient.

However, it is noteworthy that such a policy document is not rolled out as an obligation thereby limiting the benefits. Furthermore, the ABDM is defined as a framework and does not possess mandatory force over private hospitals, clinics or laboratories. The framework requires an enforcing Act or provision.

VI.2.2. National Cybersecurity Policy, 2013

National Cybersecurity Policy, 2013 (NCP) is a comprehensive document that enables different businesses, citizens and government bodies to establish a resilient and secure cyber ecosystem. The NCP 2013 aims to achieve the following objectives:

1. To establish a resilient cyber-ecosystem and develop trust and confidence in IT systems and transactions which take place in a cyberspace.

2. To formulate framework to design security policies and promote and enable global security compliant standards and practices.

3. To establish a stringent regulatory framework to ensure a protected cyber ecosystem.

4. To establish and develop machinery to obtain significant information with reference to risks to ICT infrastructure, creation of solutions for response, risk management and assessment procedures by way of "predictive, preventive, protective, response and recovery actions."

5. To enhance protection of critical infrastructure and establish a 24 × 7 National Critical Information Infrastructure Protection Centre and mandate security and privacy practices.

6. To introduce and develop technologies for purposes of National Security.

7. To improve transparency and integrity of different technologically connected products and services by developing systems for testing and validation of security.

8. To upscale the number of professionals in cybersecurity.

9. To ensure fiscal benefits for organizations adopting security standards and practices.

10. To reduce economic losses due to cybercrimes and data theft by protecting information.

11. To enact an efficient prosecution and investigation of cybercrimes through legislative intervention.

12. To enable cybersecurity culture and privacy enabled responsible behavior.

13. To develop public-private partnerships.

14. To promote and develop global cooperation towards furthering the cause of security in cyberspace.

15. To establish such mechanisms which provide for early warnings, risk and response management.

16. To formulate a framework for assessment for conformance and compliance certification to best cyber practices and policies.

17. To reduce of supply chain risks in cyber infrastructure.

It is relevant here to know that National Cybersecurity Policy, 2013 is a comprehensive document but it does not introduce provisions mandating organizations and corporations to establish an internal policy in compliance with the NCP, 2013. Besides this, the policy is more like a guiding stick in the dark and developing room of technology that will turn obsolete in coming time. Moreover, the policy does not introduce any rights and/or obligations for a data owner or consent. Even though it is a holistic framework having preventive characteristics, it does not cover enough area to protect sensitive data.

VII. Indian Judiciary and Digital Privacy

In India, a definition of privacy has been framed by both Indian Judiciary and the Legislature. After a review of literature discussing different aspects of privacy, it can be laid down that in Indian Scenario privacy can be subjectively categorized into four aspects: a. privacy and

press freedom; b. privacy and surveillance; c. privacy and decisional autonomy; and d. informational privacy. However, we will be discussing all of them briefly but our primary focus is laid upon information privacy. Freedom of expression has been enshrined as a constitutional and fundamental right in India under Art. 19 of the *grundnorm*. The right to privacy has also been given a status of a fundamental right under Art. 21(15).

The conflict situation was laid rest by the Supreme Court in case *R. Rajagopala v. State of Tamil Nadu* (1994).[23] The Honorable Supreme Court highlighted that only private and confidential information related to national security shall remain out of the ambit of right to information.

The second aspect of privacy — surveillance — has been lately the most discussed part of privacy. With recent upsurge in technology and public policies, surveillance especially by the state has been in focus because it leads to gross violation of digital and manual privacy.

In India, privacy has been claimed in two aspects, in property and in communications. However, in earlier times, the notion of privacy did not hold a significant status in the eyes of law. The concept of privacy was denied the status of fundamental right in *M.P. Sharma v. Satish Chandra* (1954)[24] and *Kharak Singh v. State of Punjab* (1977).[25]

In Kharak Singh case (1977), surveillance related constitutional claim of privacy was challenged, and the concept of privacy was acknowledged. In: Kharak Singh (1977), the court was not concerned with the concept of privacy for a while; however, in the next case *R.M. Malkani v. State of Maharashtra* (1972) the Apex Court held that attaching a recording device to a telephone line did not violate Section 25 of the Telegraph Act. Even though the judicial pronouncement was related to admissibility of evidence but the Honorable Supreme Court denied the privacy claim based on Art. 21. Subsequently, case *Gobind v. State of Madhya*

[23] R. Rajagopal v. State of Tamil Nadu (no date) Global Freedom of Expression. Available at: https://globalfreedomofexpression.columbia.edu/cases/r-rajagopal-v-state-of-t-n/ [Accessed 21.07.2024].

[24] M.P. Sharma vs Satish Chandra (1954). Available at: https://indiankanoon.org/doc/1306519/ [Accessed 21.09.2024].

[25] Kharak Singh vs The State Of, U.P. & Others (1962). Available at: https://indiankanoon.org/doc/619152/ [Accessed 21.09.2024].

Pradesh (1975), similar to case of Kharak Singh (1977), involved police visits at the personal property of a history-shelter. The court in this case inclined towards recognizing and determining the right to privacy as the constitutional and a fundamental right under Art. 21 but instead declared privacy, a right subject to "compelling state interest". The right to privacy was finally given the status of fundamental right in *K.S. Puttuswamy v. Union of India* (2018)[26] where it overruled both MP Sharma (1954) and Kharak Singh (1977).

The Puttuswamy case (2018) put forth a three-tier test to check whether a legislation infringes the right to privacy. The first tier is concerned with legality, the second is concerned with requirement, i.e., legitimate objective to enact that particular law and lastly, the third tier involves proportionality where the burden is on the state to highlight the legitimate aim supposed to be achieved. In addition to this, the Puttuswamy judgment also highlighted that "privacy is not surrendered just because an individual is in public sphere." The court asserted that privacy is an inherent part of living a life with dignity.

The right to privacy was given the status of fundamental right in *K.S. Puttuswamy v. Union of India* (2018) where it overruled both *MP Sharma* (1954) and *Kharak Singh* (1977). *The Puttuswamy case* (2018) put forth a three-tier test to check whether a legislation infringes the right to privacy. The first tier is concerned with legality, the second is concerned with requirement, i.e., legitimate objective to enact that particular law and lastly, the third tier of proportionality where the burden is on the state to highlight the legitimate aim supposed to be achieved. In addition to this, the Puttuswamy judgment also highlighted that "privacy is not surrendered just because an individual is in public sphere." The court asserted that privacy is an inherent part of living a life with dignity.

Regardless of this judgment, privacy does not have a status of an absolute right. In 2018, the Apex Court laid down in Puttuswamy (II) that AADHAR Act was not unconstitutional and and it was invalid since

[26] Justice, K.S. Puttaswamy (Retd) vs Union Of India (2018). Available at: https://indiankanoon.org/doc/127517806/ [Accessed 21.09.2024].

the intrusion of privacy is proportional to the objective of the legislation. The judgment laid down in 2018 was formed based on 2017 decision.

In Puttuswamy (II) (2018), Justice Sikri laid down a four-pronged test to confirm proportionality of the legislation. The first prong means ensuring that a provision restricting a right must be legitimate; secondly, such provision must be appropriate for furthering the concerned goal; thirdly, there must be another alternate remedy available; and lastly, the provision should not disproportionately affect the owner of the right. Upon analysis of constitutional validity of AADHAR Act on the above four parameters, the majority inclined towards upholding the constitutional validity of the Act and barred some of its provisions. The court held that AADHAR, being a unique and biometric identity system, is effective and meets with the conditions of necessity. Thus, they are constitutional.

The issue regarding privacy in healthcare was also brought up in *Mr. X v. Hospital Z* (1998) where Mr. X was diagnosed with HIV+ when donated blood. It was alleged that unauthorized disclosure of his positive result of his ailment by the hospital led to Mr. X's marriage and seeking legal course. The court held that doctors are obliged with the irrefutable duty to maintain confidentiality of their patients. However, the court asserted, "public interest would override the duty of confidentiality, specifically where there is an immediate or future health risk to others." In this situation, there was an inherent risk to the health of the woman Mr. X was going to marry.

It is important to note that, although the Right to Privacy has been given the status of a fundamental right under Art. 21, such a status is not absolute. On the contrary, it is a qualified right. It is subject to certain restrictions and such restrictions vary case to case. Furthermore, the concerns related to digital health information still remain unaddressed by Indian Judiciary. The AADHAR judgment (Puttuswamy (II) (2018)) though it addresses the concerns relating to biometric identity and upholds the protection of digital data privacy, the lack of consideration towards digital health information may lead to higher instances of violation of the confidentiality of health data.

VIII. Overview and Comparative Analysis of the Legal Systems in India, the European Union, and the United States

Upon analysis of Indian legal and regulatory framework, it can be stated that Indian legal framework suffers from several shortcomings. An assessment of legal framework implemented in International counterparts, primarily United States and European Union, will provide an overview of provisions that can also be incorporated in Indian legal regime. The comparative assessment of Health Insurance Portability and Accountability Act, 1996 enforced in the U.S. and General Data Protection Regulation applicable to member states of European Union with Digital Personal Data Protection Act, 2023 and Information Technology Act, 2000 currently in force in India will provide a comprehensive view of provisions primarily dedicated to protection of personal health information.

The landscape of health data protection and privacy regulations varies significantly across different jurisdictions, with notable differences between Health Insurance Portability and Accountability Act, 1996 (HIPAA — United States), General Data Protection Regulation (GDPR- European Union), the Information Technology Act, 2000 & Information Technology Rules, 2011 (India), and the Digital Personal Data Protection Act, 2023 (India). Each framework offers a distinct approach to handling health data, consent, data breach notifications, and the rights of data subjects.

HIPAA is a robust framework specifically addressing the protection of health information in the United States. It provides comprehensive definitions of health information, including requirements for safeguarding electronic protected health information (ePHI) and restrictions on its use and disclosure. These provisions ensure that health data remains confidential and secure, with specific guidelines on how such data can be used and shared. HIPAA's stringent rules highlight its focus on maintaining the privacy and security of health information, making it a cornerstone of health data protection in the U.S.

In contrast, the European Union's GDPR includes provisions for the protection of health data under its broader data protection framework. GDPR recognizes the sensitive nature of health information and provides

it with special protection, mandating that such data be processed only under stringent conditions. Explicit consent from the data subject is often required, and GDPR outlines detailed requirements for obtaining and managing this consent. This regulation ensures that individuals are fully aware of how their health data will be used and have the right to withdraw consent at any time, reflecting the EU's strong emphasis on individual privacy rights.

India's Information Technology Act and the Digital Personal Data Protection Act (DPDP Act) differ significantly from HIPAA and GDPR. These acts lack explicit provisions specifically tailored to the protection of health data. While they cover aspects of data protection more broadly, they do not offer the detailed and specialized regulations concerning health information found in HIPAA and GDPR. This gap indicates a less comprehensive approach to health data protection in India, where the focus is more on general data protection principles rather than specific health data regulations.

Consent is another critical area where these frameworks differ. GDPR and the DPDP Act emphasize obtaining explicit, informed, and unambiguous consent from data subjects for processing personal data. GDPR, in particular, outlines detailed requirements for consent, ensuring that data subjects are fully informed and have control over their data. The DPDP Act aligns with these principles, emphasizing clear and affirmative consent from individuals. HIPAA, while not focusing explicitly on consent in the same way, requires detailed authorizations for the use and disclosure of protected health information, particularly for uses beyond treatment, payment, or healthcare operations.

Data breach notification requirements also vary. Both GDPR and HIPAA mandate specific obligations for organizations to notify supervisory authorities and affected individuals in the event of a data breach. These requirements ensure transparency and accountability, providing clear guidelines on how to handle data breaches. In contrast, the Information Technology Act and the DPDP Act lack detailed provisions for breach notifications. While they include broader data security provisions, they do not have the specific and stringent requirements for notifying breaches comparable to GDPR and HIPAA.

The rights of data subjects form another area of divergence. GDPR and the DPDP Act grant extensive rights to data subjects, including the right to access, rectification, erasure, and the right to object to processing. These rights empower individuals to have significant control over their data. HIPAA provides certain rights related to accessing and amending health information but does not offer the same level of granularity as GDPR and the DPDP Act. The Information Technology Act does not specifically outline detailed rights for data subjects, lacking the specific procedures and protections found in GDPR and the DPDP Act.

IX. Conclusion and Suggestions

Health data privacy is an extremely important aspect of Electronic Health Records. EHRs carry vital medical information of an individual that may turn out to be dangerous if not recorded, stored and protected carefully. Currently, there are numerous risks and threats developing every day and the current legislation governing privacy of data of any kind in India are not specifically framed to deal with privacy, confidentiality and security of medical records, thereby rendering EHRs susceptible to high level risks and threats, one of which is a cyber-attack. A cyber-attack is not a merely fictitious event anymore; the incidences are occurring frequently and a legal machinery to handle such incidences is not properly equipped with requisite provisions.

If one takes a look at the IBM report, India has suffered the loss of 2.18 million USD in the year 2023 alone and 2.23 million USD in 2022 (Raizada and Biswal, 2024). Furthermore, an authorized government body responsible to deal with such occurrences is CERT-IN established under Section 73 of the Information Technology Act, 2000 in 2004 set up to prevent cyber-attacks, issue guidelines, advisories and enforce emergency measures as well. However, it is also important to note that guidelines, advisories issued by CERT-IN do not possess enforcing characteristics.

The legislative measures that have been introduced through the new Digital Data Protection Bill last year also do not consist of provisions directed at protection of health data specifically, nor it have been addressed in the current legislation, i.e., Information Technology Act,

2000 or succeeding Amendment in 2008. Recurring attacks, threats and risks are putting our health data at stake and lessons must be learnt not only from the recent cyber-attack on All India Institute of Medical Sciences hospital or Indian Council for Medical Research database but subsequent incidences occurring internationally as well.

Another step can be taken towards bringing in the private practitioners, clinics, laboratories and health service providers within the ambit of regulatory frameworks like Ayushman Bharat Digital Mission (India's own digital health architecture). Furthermore, the country's policies require not just punitive but a preventive legislation as well, which can be attained through making provisions of Electronic Health Records Standards, 2016 mandatory for all health service providers including private sector. Besides legal machinery, there is also an utmost necessity of training among clinicians and law enforcement personnel to be aware of issues concerning cybersecurity and procedure thereby required to be complied with in case of occurrence of such event.

The absence of provisions of sensitive records database management has made it only harder to achieve the primary objective of protecting privacy individual's data. To address different types of cyber-risks, various approaches can be taken. They can emphasize the need for security, privacy, and confidentiality in electronic health information systems (Jayawardena, 2013).

They may help in highlighting the vulnerability of EHRs to unauthorized access and misuse of sensitive information and suggest investing time and resources in maintaining cybersecurity and ensuring the confidentiality of health records (Iasiello, 2013).

The blockchain technology is also proposed as a solution to enhance the security of EHRs. The use of blockchain-enabled EHRs provides patients with traceable, trustworthy, and secure ownership over their medical data (Rai, 2022). Cyber-risks to electronic health records pose significant threats to the confidentiality, integrity, and availability of patient information. Measures such as authentication, authorization, encryption, and the use of technologies like blockchain can help mitigate these risks and ensure the security of EHRs. Technology is now undergoing rapid upgrades and is developing every single minute. Threats are inevitable, so at the very least the entities

responsible for recording, storing and protecting data should be well equipped and properly made aware of the technicalities in order to avoid such encounters. Furthermore, cybersecurity is not a destination or a milestone; it is a continuous process that requires constant development and evolution to keep up with the changing dynamics of digital health.

Now with the healthcare organizations outsourcing most of their services, cybersecurity needs to be considered as another important aspect of security for healthcare organizations. Several steps are required to be adopted and practiced in consonance with other significant activities. Healthcare organizations can adopt different initiatives to minimize numerous forms of cyber-risks and threats. The list of steps is not exhaustive but can be a rewarding initiative towards protection of patient privacy.

1. Establishing Cybersecurity Policies

In the aspect of health data, cybersecurity policies and regulations differ for each organization. Policies are supposed to be flexible and constantly adapt the changing circumstances. This should include protocols related to data encryption, access controls, functions related to communication, leadership and organizational commitments, and other risk management frameworks it adopts.

2. Proper Allocation of Resources

Proper allocation of resources is critical for maintenance of a robust cybersecurity in health information management system. It includes proper investment in innovative technologies and solutions, constant updating of software and ensuring skilled personnel. Furthermore, funding plays a significant role in adoption of security measures, establishing firewalls, detection systems, etc.

3. Education and Awareness

Education and awareness plays a significant role in forming an indispensable fortress for patient privacy. It is crucial to communicate employees about sensitivity of health information and potential risks associated with it. Various education and informative sessions should be organized by the organizations and employee enrollment should be compulsory. Such sessions will develop a culture for cybersecurity awareness and reduce likelihood of different events that could harm the digital infrastructure.

4. Training of Personnel

Proper training and skill development of employees working with the digital health system is necessary. Training of individuals who regularly deal with patient data should be trained to recognise and mitigate different threats like phishing attacks, ransomwares, etc. Employees should understand the significance of password hygiene and established protocols. It is an ongoing process and staff should be updated on evolving threats and practices.

5. Maintenance of Employee Records

Employee records support in maintaining track of personnel authorized to access sensitive information. A proper account for employees with their authorized access rights should be formed and continuously maintained. It is essential for ensuring cyber-resilience in health data management.

6. Adherence to Related Laws

Strict compliance to respective laws actually aids organizations to mitigate accountability issues in case of a breach. European Union's General Data Protection Regulation (GDPR) and US' Health Insurance Portability and Accountability Act lay down crucial aspects of patient privacy and security practices to be mandatorily adopted by the healthcare organizations. Similar obligations should be obligated under relevant laws of the jurisdiction in which healthcare organizations lie.

References

Adebayo, O.S. and AbdulAziz, N., (2014). An Intelligence Based Model for the Prevention of Advanced Cyber-Attacks. *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, pp. 1–5, doi: 10.1109/ICT4M.2014.7020648.

Alder, S., (2021). Healthcare Industry Cyberattacks Increase by 45 %. *The HIPAA Journal*. January 6. Available at: https://www.hipaajournal.com/healthcare-industry-cyberattacks-increase-by-45/ [Accessed 23.03.2024].

Almaghrabi, N.S, and Bugis, B.A., (2022). Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature.

Dr. Sulaiman Al Habib Medical Journal, 4(3), pp. 126–135, doi: 10.1007/s44229-022-00016-9.

Anderson, J.M., (2003). Why We Need a New Definition of Information Security. *Computers & Security*, 22(4), pp. 308-313, doi: 10.1016/S0167-4048(03)00407-3.

Ang, A., (2022). 1.9 Million Cyberattacks against Indian Healthcare Recorded in 2022. *Healthcare IT News*. December 5. Available at: https://www.healthcareitnews.com/news/asia/19-million-cyberattacks-against-indian-healthcare-recorded-2022 [Accessed 21.09.2023].

Angel, D., (2022). Protection of Medical Information Systems against Cyber Attacks: A Graph Theoretical Approach. *Wireless Personal Communications*, 126(4), pp. 3455–3464, doi: 10.1007/s11277-022-09873-x.

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., et al., (2020). Cybersecurity of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks. *BMC Medical Informatics and Decision Making*, 20(1), p. 146, doi: 10.1186/s12911-020-01161-7.

Bhatia, D., (2022). A Comprehensive Review on the Cyber Security Methods in Indian Organisation. *International Journal of Advances in Soft Computing and Its Applications,* 14(1), pp. 103–124, doi: 10.15849/IJASCA.220328.08.

Blessing, G., Azeta, A., Misra, S., Osamor, V.Ch., Fernandez-Sanz, L. and Pospelova, V., (2022). The Emerging Threat of Ai-Driven Cyber Attacks: A Review. *Applied Artificial Intelligence,* 36(1), pp. 1–34, doi: 10.1080/08839514.2022.2037254.

Coventry, L. and Branley, D., (2018). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. *Maturitas*, 113, pp. 48–52, doi: 10.1016/j.maturitas.2018.04.008.

Cox, Jr, L.A., (2008). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28(6), pp. 1749–1761, doi: 10.1111/j.1539-6924.2008.01142.x.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Stefan Materne, S., (2022). Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. *The Geneva Papers on Risk*

and Insurance — Issues and Practice, 47(3), pp. 698–736, doi: 10.1057/s41288-022-00266-6.

Croke, L., (2020). Protecting Your Organization from E-mail Phishing and Ransomware Attacks. *AORN Journal*, 112(4), doi: 10.1002/aorn.13229.

Desjardins, J., (2018). Why Hackers Hack: Motives Behind Cyberattacks. *Visual Capitalist*. January 3. Available at: https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/#google_vignette [Accessed 21.09.2024].

Farringer, D.R., (2019). Maybe if We Turn it off and then Turn it back on again? Exploring Health Care Reform as a Means to Curb Cyber Attacks. *Journal of Law, Medicine & Ethics*, 47(S4), pp. 91–102, doi: 10.1177/1073110519898046.

Gajwani, A., (2020). Electronic Health Records and Data Privacy Regimes in India. *iPleaders*. November 28. Available at: http://blog.ipleaders.in/electronic-health-records-data-privacy-regimes-india/ [Accessed 21.09.2024].

Ganiga, R., Pai, R.M., Manohara Pai, M.M. and Sinha, R.K., (2020). Security Framework for Cloud Based Electronic Health Record (Ehr) System. *International Journal of Electrical and Computer Engineering (IJECE),* 10(1), pp. 455–466, doi: 10.11591/ijece.v10i1.pp455-466.

Hakak, S., Khan, W.Z., Imran, M., Choo, K-K.R. and Shoaib, M., (2020). Have You Been a Victim of Covid-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *IEEE Access*, 8, pp. 124134–124144, doi: 10.1109/ACCESS.2020.3006172.

Han, Ch. and Dongre, R., (2014). Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, 4(10), pp. 40–42, doi: 10.22215/timreview/838.

Hoffman, Sh. and Podgurski, A., (2013). The Use and Misuse of Biomedical Data: Is Bigger Really Better? Faculty Publications, January, pp. 497–538. Available at: https://scholarlycommons.law.case.edu/faculty_publications/606 [Accessed 21.09.2024].

Howden, E., (2023). Retaining and Destroying Patient Records. *BDJ Team,* 10(1), p. 23, doi: 10.1038/s41407-023-1712-x.

Iasiello, E., (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*,

pp. 1–18. Available at: https://ieeexplore.ieee.org/document/6568392 [Accessed 21.09.2024].

Ibarra, J., Jahankhani, H. and Kendzierskyj, S., (2019). Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. In: Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G. and Al-Khateeb, H., eds, (2019). *Blockchain and Clinical Trial: Securing Patient Data*. Cham: Springer International Publishing, doi: 10.1007/978-3-030-11289-9_5.

Javaid, M., Haleem, A., Singh, R.P. and Suman, R., (2023). Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends. *Cyber Security and Applications,* 1, 100016, doi: 10.1016/j.csa.2023.100016.

Jayawardena, A.S., (2013). A Systematic Literature Review of Security, Privacy and Confidentiality of Patient Information in Electronic Health Information Systems. *Sri Lanka Journal of Bio-Medical Informatics*, 4(2), p. 25, doi: 10.4038/sljbmi.v4i2.5740.

Kaplan, B., (2014). How Should Health Data Be Used? Privacy, Secondary Use, and Big data Sales. *Yale University Institute for Social and Policy Studies Working Paper No. 14-025, Cambridge Quarterly of Healthcare Ethics,* 25(2), 312–329, doi: 10.2139/ssrn.2510013.

Kaplan, B., (2020). Seeing through Health Information Technology: The Need for Transparency in Software, Algorithms, Data Privacy, and Regulation. *Journal of Law and the Biosciences*, 7(1), lsaa062, doi: 10.1093/jlb/lsaa062.

Kawu, A.A., Hederman, L., Doyle, J. and O'Sullivan, D., (2023). Patient Generated Health Data and Electronic Health Record Integration, Governance and Socio-Technical Issues: A Narrative Review. *Informatics in Medicine Unlocked*, 37, 101153, doi: 10.1016/j.imu.2022.101153.

Keshta, I. and Odeh, A., (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal,* 22(2), pp. 177–183, doi: 10.1016/j.eij.2020.07.003.

Langer, S.G., (2017). Cyber-Security Issues in Healthcare Information Technology. *Journal of Digital Imaging*. 30(1), pp. 117–125, doi: 10.1007/s10278-016-9913-x.

Lekshmi, A.S., (2022). Growing Concern on Healthcare Cyberattacks & Need for Cybersecurity. Preprint. Available at: https://

www.researchgate.net/publication/357753537_Growing_Concern_on_Healthcare_Cyberattacks_Need_for_Cybersecurity [Accessed 21.09.2024].

Martin, G., Kinross, J. and Hankin, Ch., (2017). Effective Cybersecurity Is Fundamental to Patient Safety. *The British Medical Journal*, 357, j2375, doi: 10.1136/bmj.j2375.

Muthuppalaniappan, M. and Stevenson, K., (2021). Healthcare Cyber-Attacks and the Covid-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Health Care: Journal of the International Society for Quality in Health Care,* 33(1), mzaa117, doi: 10.1093/intqhc/mzaa117.

Nasiri, S., Farahnaz, S., Tadayon, M. and Dehnad, A., (2019). Security Requirements of Internet of Things-Based Healthcare System: A Survey Study. *Acta Informatica Medica*, 27(4), pp. 253–258, doi: 10.5455/aim.2019.27.253-258.

Negro-Calduch, E., Azzopardi-Muscat, N., Krishnamurthy, R.S. and Novillo-Ortiz, D., (2021). Technological Progress in Electronic Health Record System Optimization: Systematic Review of Systematic Literature Reviews. *International Journal of Medical Informatics*, 152, 104507, doi: 10.1016/j.ijmedinf.2021.104507.

Nielsen, M., Saavedra, A., Villarreal, V., Muñoz, L. and Castillo, Y., (2019). Flexehr: Proposal of a Platform for Interoperability between Information Systems Based on Electronic Medical Records in Panama. *Proceedings of the 13th International Conference on Ubiquitous Computing and Ambient Intelligence UCAmI 2019*, 31(1), 5, doi: 10.3390/proceedings2019031013.

Nusairat, T., Saudi, M.M. and Ahmad, A.B., (2023). A Recent Assessment for the Ransomware Attacks against the Internet of Medical Things (Iomt): A Review. *2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE)*, pp. 238–242, doi: 10.1109/ICCSCE58721.2023.10237161.

Pal, P., Sahana, B.C. and Poray, J., (2024). Secure electronics medical infrastructure for healthcare 4.0: a voice identity management-based approach. *Procedia Computer Science*, 235, pp. 468–477, doi: 10.1016/j.procs.2024.04.046.

Paliwal, S., Parveen, S., Singh, O., Alam, A. and Ahmed, J., (2023). The Role of Ayushman Bharat Health Account (Abha) in Telehealth: A New Frontier of Smart Healthcare Delivery in India. In: Kohei Arai, ed., (2023). *Proceedings of the Future Technologies Conference (FTC)*. Vol. 2, pp. 388–406. Cham: Springer Nature Switzerland; doi: 10.1007/978-3-031-47451-4_28.

Pears, M. and Konstantinidis, S.T., (2021). Cybersecurity Training in the Healthcare Workforce — Utilization of the Addie Model. *2021 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1674–1681, doi: 10.1109/EDUCON46332.2021.9454062.

Price, W.N., Kaminski, M.E., Minssen, T. and Spector-Bagdady, K., (2019). Shadow Health Records Meet New Data Privacy Laws. *Science (New York, N. Y.)*, 363(6426), pp. 448–450, doi: 10.1126/science.aav5133.

Rai, B.K., (2022). Blockchain-Enabled Electronic Health Records for Healthcare 4.0. *International Journal of E-Health and Medical Communications (IJEHMC)*, 13(4), pp. 1–13, doi: 10.4018/IJEHMC.309438.

Raizada, N. and Biswal, M., (2024). An evidence-based investigation of cert-in's reporting on cyber-threats in healthcare sector. *Conhecimento & Diversidade*, 16(42), pp. 219–246, doi: 10.18316/rcd.v16i42.11694.

Reshmi, T.R., (2021). Information Security Breaches Due to Ransomware Attacks — a Systematic Literature Review. *International Journal of Information Management Data Insights*, 1(2), 100013, doi: 10.1016/j.jjimei.2021.100013.

Richter, J.G. and Thielscher, Ch., (2023). New Developments in Electronic Health Record Analysis. *Nature Reviews Rheumatology*, 19(2), pp. 74–75, doi: 10.1038/s41584-022-00894-1.

Sardi, A., Rizzi, A., Sorano, E. and Guerrieri, A., (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, 12(17), 7002, doi: 10.3390/su12177002.

Savin, V.D. and Anysz, R.N., (2021). Cybersecurity Threats and Vulnerabilities of Critical Infrastructures. *American Research Journal of Humanities Social Science,* 04(07), pp. 90–96. Available at: https://www.arjhss.com/wp-content/uploads/2021/07/L479096.pdf [Accessed 21.09.2024].

Sengupta, K., (2017). Isis-Linked Hackers Attack NHS Websites to Show Gruesome Syrian Civil War Images. *The Independent*. February 8. Available at: https://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html [Accessed 21.09.2024].

Shah, Sh.M. and Khan, R.M., (2020). Secondary Use of Electronic Health Record: Opportunities and Challenges. *IEEE Access*, 8, pp. 136947–136965, doi: 10.1109/ACCESS.2020.3011099.

Škiljić, A., (2020). Cybersecurity and Remote Working: Croatia's (Non-)Response to Increased Cyber Threats. *International Cybersecurity Law Review,* 1(1), pp. 51–61, doi: 10.1365/s43439-020-00014-3.

Strupczewski, G., (2021). Defining Cyber Risk. *Safety Science*, 135, pp. 105–143, doi: 10.1016/j.ssci.2020.105143.

Sudhanshu, N., (2022). Indian Healthcare: Attack Surfaces, Personal Digital Data Protection, and Cyber Resiliency. *Observer Research Foundation*. December 28. Available at: https://www.orfonline.org/expert-speak/indian-healthcare-attack-surfaces-personal-digital-data-protection-and-cyber-resiliency/ [Accessed 21.09.2024].

Thamer, N. and Alubady, R., (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. *2021 1st Babylon International Conference on Information Technology and Science (BICITS),* pp. 210–216, doi: 10.1109/BICITS51482.2021.9509877.

Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, Ch., (2020). Healthcare Challenges in the Era of Cybersecurity. *Health Security*, 18(3), pp. 228–231, doi: 10.1089/hs.2019.0123.

Warkentin, M. and Orgeron, C., (2020). Using the Security Triad to Assess Blockchain Technology in Public Sector Applications. *International Journal of Information Management*, 52, 102090, doi: 10.1016/j.ijinfomgt.2020.102090.

Yusuf, A. and Ayinde A., (2023). Cybersecurity Plan for a Healthcare Cloud-Based Solutions. *Journal of Cyber Security,* 4(3), pp. 185–188, doi: 10.32604/jcs.2022.035446.

Zahid, M., Inayat, I., Daneva, M. and Mehmood, Z., (2021). Security Risks in Cyber Physical Systems — A Systematic Mapping Study. *Journal*

of Software: Evolution and Process, 33(9), e2346, doi: 10.1002/smr.2346.

Zodian, M., (2024). Recourse Allocation and Capabilities Generation in Security Studies. In: Anton, S., Tutuianu, I.S., editors (2024). *The Complex and Dynamic Nature of the Security Environment. Proceedings of the International Scientific Conference "Strategies XXI."* Vol. 2, pp. 19–26. Available at: https://www.academia.edu/103421710/THE_COMPLEX_AND_DYNAMIC_NATURE_OF_THE_SECURITY_ENVIRONMENT_Volume_2 [Accessed 23.03.2024].

Information about the Authors

Niharika Raizada, Assistant Professor, CHRIST University, Bengaluru, India
niharika95raizada@gmail.com
ORCID: Orcid ID: 0000-0002-6919-104X

Pranjal Srivastava, Research Scholar, Rashtriya Raksha University, Gandhinagar, India
niharika95raizada@gmail.com
ORCID: 0009-0007-2298-3510

Article

DOI: 10.17803/2713-0533.2024.3.29.491-513

Digital Profiling and the Legal Regime of Derived Personal Data

Artur N. Mochalov

Ural State Law University named after V.F. Yakovlev, Yekaterinburg, Russian Federation

Abstract: The paper discusses some aspects of the legal regulation of personal data profiling in various jurisdictions. It focuses on derived personal data, also known as inferences, which are the outputs of digital profiling and automated decision-making. Although the extraction of new knowledge about individuals based on the processing of personal data has become common practice in both the commercial and public sectors, there have been only a few attempts to establish specific legal frameworks for derived personal data. These include the European Union, California (USA), and Singapore. Using a comparative legal approach, the author analyzes the characteristics of derived personal data and how the rights of individuals are protected in relation to derived personal information in these jurisdictions and in Russia as well. After examining the relevant laws and regulations, the author concludes that these attempts to regulate derived personal data are an effort to adapt traditional legal frameworks to the challenges posed by Big data. At the same time, the protection of personal data when using Big data technologies and artificial intelligence requires advanced regulatory approaches. Today, data extraction processes are often hidden from data subjects and not under their control. The author believes that the automated processing of personal information, including digital profiling and the extraction of new personal data, should be made more transparent and allow users to opt out.

Keywords: personal data; derived personal data; inferences; profiling; data mining; privacy

Acknowledgements: The reported study was funded by Russian Science Foundation, project number 24-28-01378

Cite as: Mochalov, A.N., (2024). Digital Profiling and the Legal Regime of Derived Personal Data. *Kutafin Law Review*, 11(3), pp. 491–513, doi: 10.17803/2713-0533.2024.3.29.491-513

Contents

I. Introduction

The term "profiling" in relation to personal data means a set of practices of creating, discovering or constructing knowledge about a person from large sets of data from a variety of sources (Niševic, 2020, p. 104).

By analyzing personal information, computer algorithms allow to obtain new knowledge about people, which was not initially known to the controller. For example, processing data about a user's social network behavior, it is possible to get reliable information about their age, education level, interests, hobbies, beliefs, and even political preferences. A few years ago, in the USA there was a public outcry due to the actions of Cambridge Analytica Company. They processed data from users' accounts in a popular social network to identify potential

Republican Party supporters and target them with a campaign for Donald Trump (Day, 2020).

Today, digital profiling of internet users is a common practice in data-driven business models. News services and marketplaces, for example, use profiling to generate personalized recommendations, while advertising operators use it to create targeted ads. The material for profiling comes from digital footprints left by Internet users on various sites, including "likes" on social networks, search queries, or the delivery time of goods purchased on marketplaces. In recent years, information transmitted by smart devices has also been actively used by controllers for profiling the users (Wiedemann, 2022). In all cases, profiling produces new knowledge about individuals by deriving hidden and non-obvious information from a primary data set. This information can be used for evaluating individuals (social scoring systems) and predicting their behavior. In this regard, the results of profiling are widely used, particularly by banks to assess the solvency of customers, employers to select candidates for vacant positions, and law enforcement agencies to identify persons prone to illegal behavior (Westerlund et al., 2021, p. 34). The social rating system has been most developed in the People's Republic of China (Vinogradova et al., 2021, pp. 9–10).

Despite the widespread use of profiling in the processing of personal data by computers, there is relatively little special regulation regarding derived personal information about an individual. The article will focus on three jurisdictions where such regulation exists — the European Union, Singapore, and the State of California (USA). It will be shown that there are still many controversial issues in establishing the legal regime for derived personal data, which the legislator approaches differently in each case. The article will discuss some features of derived personal data that distinguish them from "classical" (primary) personal data. Then, the specifics of the implementation by data subjects of individual rights in relation to derived data will be analyzed, considering their characteristics. In particular, the right to access derivative data about themselves, the right of rectification of derivative data and the right to delete them ("right to be forgotten") will be considered.

II. Conceptual and Legal Framework

Profiling is based, first, on social and psychological patterns of people's behavior and, second, on the statistical correlations, which allow to "calculate" certain characteristics of a person based on information about his or her previous activity, to determine his or her interests and predict likely actions in the future (Day, 2020, pp. 596–599). Classifying people according to their psychological types and understanding their behavior is nothing new in science. However, with the advent of Big data technologies and machine learning, it has become possible to process information about a large number of people at once, identify previously unknown patterns, and quickly obtain accurate results (Adjerid and Kelley, 2018). This has led to the development of a new economy based on data, where personal information has become a valuable digital asset.[1]

In computer science, the term "data profiling" has a narrower meaning and refers to the process of preparing and technically analyzing data for subsequent use. Profiling is aimed at improving the quality of data, eliminating errors, contradictions, and duplications. In the process of profiling, it is possible to identify patterns, rules, and trends in data, and determine dependencies between different data elements. The extraction of new non-obvious knowledge by computer processing of existing information is called data mining (Naumann, 2014).

The use of data mining to process information about a person has raised difficult questions, since statistical correlations, as it turned out, completely ignore the requirements of personal data legislation (Roig, 2017, p. 6). From the data on a user's behavior in a social media platform, it is possible to extract information that infringes their privacy, such as their philosophical convictions or political opinions. These inferences about a person's characteristics may be biased (Chander, 2017). There are cases where computer algorithms have denied employment opportunities to all female candidates or have considered individuals with common Afro-American names to be potential criminals. Therefore,

[1] *See* Personal Data: The Emergence of a New Asset Class. An initiative of the World Economic Forum January 2011. Available at: https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf [Accessed 06.04.2024].

the rights of individuals in relation to profiling and the use of extracted personal information cannot be effectively safeguarded solely through traditional protections provided by personal data legislation. Instead, specific regulatory measures are necessary.

The European Union has taken the lead in the legislative framework for data profiling. Enacted in 2016, the General Data Protection Regulation, commonly known as GDPR,[2] establishes a framework for automated processing of personal data that involves using personal data to evaluate or predict specific aspects of an individual's personal life, such as their work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. From the definition of profiling in Art. 4(4) of GDPR, two features of profiling are seen: (a) it is always automated processing of personal data; (b) the special purpose of processing is the assessment of "certain personal aspects relating to a natural person," including the analysis or prediction of his or her behavior. The GDPR does not clearly distinguish between the process of creating a person's profile and making a decision based on the created profile. Some contributions suggest that profiling does not include the automated decision-making stage (Wiedemann, 2022).

The GDPR is silent about the legal nature of estimated or inferred knowledge about a person obtained during profiling or decision-making based on a digital profile, and does not use the term "derived data." In particular, it avoids the question of whether such knowledge relates to personal data or is a separate type of information. However, Art. 4(1) of the Regulation does not link the assignment of information to personal data with the method of obtaining it. On this basis, it can be concluded that even if information about a person is not *collected*, but *created* on the basis of primary data, this is not a reason not to consider it personal data (Wachter and Mittelstadt, 2019, p. 518). The Article 29

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 06.04.2024].

Data Protection Working Party[3] (hereinafter Art. 29 Working Party), in its Guidelines on automated individual decision-making and profiling within the framework of the General Data Protection Regulation (GDPR), acknowledged the existence of inferred or derived data about individuals. These data were described as "new personal information that has not been directly provided by the data subjects themselves."[4]

Unlike the GDPR, the California Consumer Privacy Act (CCPA),[5] adopted in this American State in 2018, explicitly refers to personal information "inferences drawn from any of the information identified in this subdivision [definition of personal information] to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." "Inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data. The scope of CCPA is narrower than the GDPR. This Act applies only to the processing of data about consumers who are citizens of the State of California by commercial corporations. It does not regulate profiling carried out by law enforcement bodies and other government agencies.

The third example of legal regulation of derived data can be found in the Singapore Personal Data Protection Act (PDPA) following the amendments made to it in 2020.[6] Derived data is defined under the PDPA to refer to new data elements that are created by an organization in the course of business from other personal data about the individual (or another individual), in the possession or under the control of the organization. Like the CCPA, the PPDA treats derived data as personal data.

[3] The Working Party was set up under Art. 29 of Directive 95/46/EC as an independent European advisory body on data protection and privacy.

[4] Art. 29 Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Adopted on 3 October 2017 WP251rev.01. Available at: https://ec.europa.eu/newsroom/article29/items/612053 [Accessed 06.04.2024].

[5] The California Consumer Privacy Act of 2018. Available at: https://theccpa.org [Accessed 06.04.2024].

[6] Available at: https://sso.agc.gov.sg/Act/PDPA2012 [Accessed 06.04.2024].

Despite the widespread use of profiling, special regulation of derived data is currently rare. For example, it is not included in the Chinese Personal Information Protection Law 2021 (hereinafter PIPL)[7] or in the Russian Federal Law "On Personal Data" No. 152-FZ.

III. The Two Key Features of Derived Personal Data

There are at least two important features of derived personal data that distinguish them from "classic" personal data. The first feature is that derived data is not "collected" in the usual sense (i.e., received directly from the data subject or from third parties), but is created (or "calculated") as a result of automated processing of other (primary) personal data. The second feature is the probabilistic or inferred nature of derived personal data. These features will be discussed in more detail later.

III.1. Derived Data as Non-Collected Data

Unlike ordinary personal data that is collected from the data subject or from third parties, derived data does not have a collection stage. The process of obtaining derived personal data is most often hidden from the subject, and the subject may not even know that the controller has become aware of personal information that he or she did not provide. Accordingly, with respect to derived personal data, there is most likely no explicit consent of the data subject to their processing.

As noted above, the assignment of information to personal data does not depend on the method of its receipt. The Article 29 Working Party pointed out that there are three types of personal data based on their origin:

— "actively and knowingly" provided by the data subject;

— "observed" data that characterizes the subject's activity (for example, the history of search queries or information transmitted by trackers of devices such as fitness bracelets);

[7] Personal Information Protection Law of the People's Republic of China (Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on 20 August 2021). Available at: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm [Accessed 06.04.2024].

— inferred or derived data, which are created by the controllers themselves on the basis of data provided by the subjects and are the result of computer algorithms.[8]

From the perspective of the Art. 29 Working Party, derived data, although not explicitly provided by the data subject, should nevertheless be treated as personal data within the scope of the GDPR. However, certain legal safeguards granted to data subjects under the GDPR, such as the right to portability of data, are restricted to collected and observed personal data and do not extend to derived data.

In California, the State Attorney General's Office issued Opinion No. 20-303, dated 10 March 2022, explaining certain aspects of the CCPA in relation to derived personal data.[9] The document effectively equates derived data with collected data, since inferences constitute a part of the consumer's unique identity and become part of the information that the business has "collected about" the consumer.

The logic of these explanations suggests that the restrictions imposed by law for the collection of personal data should also apply to computer generating new derived data. In particular, this applies to the rule that the amount of personal data should be the minimum necessary to achieve the purpose of their processing. The purposes of processing derived personal data, in turn, must be legitimate, pre-defined and clearly formulated. Derived personal data should not be obtained and used for purposes incompatible with the purposes of primary data collection.

The difficulty, however, lies in the fact that the process of profiling and subsequent decision-making can involve personal information obtained from different sources and collected by various controllers for different purposes. The primary data for creating digital profiles is provided by the subject at different times and in different circumstances. Moreover, when forming a digital profile and discovering new knowledge about a subject, data is used that relates both to this subject and to other

[8] Art. 29 Working Party. Guidelines on the right to data portability Adopted on 13 December 2016. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf [Accessed 06.04.2024].

[9] Available at: https://www.dwt.com/-/media/files/2022/03/20-303.pdf [Accessed 06.04.2024].

persons with similar characteristics (for example, to predict the subject's consumer preferences or the probability of non-repayment of a loan). During processing, personal data can be combined with information that is not personal data. Based on some derived personal data, other derived personal data may be created. Therefore, in practice, it is almost impossible to correlate derived personal data and the purposes of their use with the purposes of collecting primary personal data. Traditional guarantees of a subject's control over the use of their data, such as the principle of consent of the subject, limitation of the amount of data processed and limitation of purposes, become illusory when it comes to Big data technologies (Gonçalves, 2017, p. 98; Savelyev, 2015).

III.2. Inferred Nature of Derived Data

The second characteristic of derived data is its inherently probabilistic nature. Despite the advancements in Big data processing techniques that allow for relatively accurate assumptions, these data are still the product of computer calculations based on statistical correlations. For instance, a social media user's age group can be inferred with a high degree of probability based on their membership in certain communities, their likes, emojis, and comments. Likewise, gender, citizenship, nationality, religious affiliation, and political views can also be "calculated" to some extent. However, these predictions remain approximations and may not always hold true.

The outcome of profiling may also result in the generation of sensitive data that falls under specific categories necessitating the individual's explicit consent for processing. In numerous jurisdictions, this encompasses, for instance, data pertaining to an individual's medical condition or beliefs. As mentioned previously, derived data is not obtained directly from the subject, and its creation is typically not accompanied by the acquisition of the subject's consent. However, what if the automated analysis of personal information reveals sensitive data about an individual? Some may argue that the probabilistic nature of these conclusions (for instance, regarding an estimation of a person's health based on their purchases) exempts the entity that obtained this data from seeking the individual's permission.

In literature, there is a suggestion to employ the term "quasi-health data," which refers to inferred data about an individual's condition (just "indirectly related to health"), particularly based on information obtained from smart devices. Such data may be confidential, but in a legal context, it should not be construed as health information. (Malgieri and Comandé, 2017). However, this approach does not answer the question of the legal conditions for processing sensitive derivative data designated as "*quasi-*" (Fischer, 2020, p. 39). The presumed nature or even inaccuracy of inferred information does not mean that such information is not personal data or does not relate to a specific person. However, if new data related to specific categories is calculated during the analysis of data (including those that do not belong to special categories), its processing will require the consent of the subject. The same position is shared by European commentators.[10]

Certain types of derived personal data may constitute an opinion or evaluation, such as inferences regarding an individual's preferences, trustworthiness, financial capacity, or projected future conduct. The distinctive aspect of this information is its unverifiability.

Among the compared legal acts, the CCPA most clearly refers assumptions and conclusions to the personal information that falls into the scope of this Act. The GDPR is silent on whether personal data includes information about a person that is an estimate, prediction, or analytical conclusion. The Article 29 Working Party assumes that non-verifiability of information about a person is not an obstacle to considering it as personal data[11] (Wachter and Mittelstadt, 2019, p. 520). At the same time, in the law enforcement practice of the European Court of Justice, this question has not received a clearness. In its decision of 17 July 2014, it concluded that the legal analysis of immigrants' applications may contain personal data but cannot be classified itself as personal data within the meaning of Directive

[10] Art. 29 Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

[11] Art. 29 Data Protection Working Party. Opinion 4/2007 on the Concept of Personal Data on 20 June 2007. Available at: https://www.europarl.europa.eu/cmsdata/183970/20080130ATT20135EN.pdf [Accessed 06.04.2024].

95/46/EC, which was in force prior to the adoption of the GDPR.[12] In a subsequent decision on 20 December 2017, the court expanded the definition of "personal data" to include written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers.[13] However, such an extension of the scope of the personal data legislation was limited by the Court to specific circumstances. Following the logic of these decisions made in non-digital contexts, there is no reason to state unequivocally that the conclusions drawn as a result of profiling are personal data within the meaning of the GDPR.

IV. Rights of Data Subjects with Respect to Derived Personal Data

Considering the features of derived personal data, a number of controversial issues arise regarding the implementation of the rights of subjects — in particular, the right to access data, the right of rectification and the right to delete or to demand erasure of data ("right to be forgotten").

IV.1. Right to Access

In the context *of the right of access to personal data*, the question of who owns the derived personal data is important. In theory, the model of "ownership" of personal data, which means that the data subject is regarded as owner of information about himself or herself, has become widespread. This doctrinal model is resulted in general rule of the need for the subject's consent to the processing of personal data, which is enshrined in the legislation of most countries, or the right of

[12] CJEU — C-141/12 and C-372/12 — YS v. Minister voor Immigratie, Integratie en Asiel. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=155114&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=671001 [Accessed 06.04.2024].

[13] CJEU — C-434/16 — Peter Nowak. Available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=BC736E3C6C1250DFC36D8A676A461F8C?text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=798290 [Accessed 06.04.2024].

data portability, which is guaranteed, for example, in Art. 20 of the GDPR (Bouchagiar and Bottis, 2018, pp. 226–227). However, derived personal data, as noted above, is not received from the data subject or from a third party. From this standpoint, is it reasonable to regard them as information that continues to belong to the data subject, or does such information, from the moment of its creation, become the sole "property" of the controller?

Assuming that it is the controller who derived the personal data that owns them, then, then the controller may refuse the subject access to them, referring, for example, to the fact that this information is a trade secret. Indeed, derived personal data may have the characteristics of a trade secret: they are created in the course of the activities of a holder, are not known to third parties, and have commercial value for the holder (Bottis and Bouchagiar, 2018, p. 208).

In the abovementioned Opinion the Attorney General of California emphasized, that according to the CCPA, "if the business holds personal information about a consumer, the business must disclose it to the consumer on request." Without explicitly addressing the question of ownership of information that is generated internally, the CCPA guarantees the right to access personal data in any situation. "The plain language of the statute, as well as the legislative history, persuade us that the CCPA purposefully gives consumers a right to receive inferences, regardless of whether the inferences were generated internally by the responding business or obtained by the responding business from another source," the Opinion says.

Similarly, Article 15 of the GDPR refers to the right of a data subject to request confirmation from the controller, that "personal data *concerning* him or her" (not "*collected*" *from* him or her) are being processed. It is obvious that the scope of Art. 15 extends beyond only "collected" personal data. However, it is not clear how far it extends (Custers and Vrabec, 2024). Recital 63 of the GDPR indicates restrictions on the right to access personal data, in particular if this violates the rights and freedoms of others, including the right to trade secrets and intellectual property results. The definition of trade secret

in the EU Trade Secret Directive[14] is so broad as to include nearly any data handled by a commercial entity, in particular information about consumers' behavior (Wachter and Mittelstadt, 2019, p. 607). This means that trade secret protection considerations significantly limit the access of subjects to derived personal data.

Unlike the right of access to data, *the right to data portability* provided for in the GDPR does not apply to derived data. According to Art. 20 of the GDPR, the data subject has the right to receive from the controller the personal data related to him in a machine-readable format, which he *provided* to this controller, and transfer them to another controller — if the processing of such data is carried out in automated systems *based on the consent of the data subject*.

This approach is likely aimed at protecting the economic interests of data controllers who have invested resources in data mining to extract valuable personal information. Unlike primary data, which can be collected multiple times from a subject or third parties, derived data are a unique product of a controller's efforts (the result of computer algorithm processing) and have greater economic value. Therefore, freely transferring such data in a machine-readable format from the controller that created it to other controllers that did not invest resources in obtaining it would disproportionately limit their economic interests.

IV.2. Right to Rectification

The specific features of derived personal data are manifested in the exercise of the *right of the data subject to rectification* of inaccurate or irrelevant information.

In various jurisdictions, accuracy and adequacy are usually proclaimed among the fundamental principles of personal data processing. At the same time, derived personal data, as mentioned above, are inferred. This means that there is a possibility of error

[14] 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. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943 [Accessed 06.04.2024].

in identifying certain characteristics of a person based on statistical correlations identified in the primary data. Does this mean that if an error is detected, the derived data must be updated at the request of the subject? Article 16 of the GDPR refers to the right of the subject to require the controller immediately rectification of inaccurate personal data concerning him or her. From this wording, it can be concluded that such a right should apply to both collected and derived personal data. However, if the procedure for clarifying the verifiable data is clear, then the probabilistic or estimated characteristics of a person may not always be changed at the request of the subject. For example, a data subject may say that their music preferences and individual recommendations for a playlist on a music listening service are defined incorrectly and do not correspond to their wishes. In turn, the service administration can claim that the selection of music was performed correctly, as a result of computer calculations based on data about tracks previously listened to by the user, as well as information about the music preferences of other users of the service with similar characteristics and interests (Custers and Vrabec, 2024, p. 55).

PDPA (after the changes made in 2020) demonstrates another approach. Article 22 of the PDPA, like the GDPR, establishes the data subjects' right to send requests to controllers for correction of data about themselves. However, Article 22(6) contains a number of exceptions from this rule, including derived personal data and "opinion data kept solely for an evaluative purpose." The term "evaluative purpose" is defined in Art. 2(1) of the PDPA. This includes, in particular, "the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates" in such fields as employment or education.[15]

The Singapore legislator likely assumes that derived and opinion data do not belong to the individual who is the subject of the data, but rather to the entity that created the information. From the perspective

[15] *See* Advisory Guidelines on Key Concepts in The Personal Data Protection Act (Revised 1 October 2021). Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.ashx?la=en. P. 107 [Accessed 06.04.2024].

of the Personal Data Protection Commission of Singapore, accuracy in derived personal data shall be achieved through accurate categorization and selection criteria (i.e., adequate business rules) at the data processing stage.[16]

IV.3. "Right to be Forgotten"

The rights of a personal data subject usually include the right to request the termination of processing of their personal data and their deletion (if there are no other legal grounds for their storage and processing by the controller) — the so-called "*right to be forgotten*." The subject may be interested in prohibiting the processing of derived personal data not only if they are incorrect or irrelevant, but also if such data is sensitive information for the subject that he would not have provided to the controller at his own will, including if the processing of such information requires the individual's mandatory consent in accordance with the law. The acquisition of such knowledge about the subject without their consent may be regarded as a disproportionate invasion of their privacy. The subject may also wish to stop processing and delete conclusions and assessments based on the analysis of the primary data, if the use of this information by the controller or other parties poses a risk of discrimination to them.

At the same time, the CCPA guarantees the consumer's right to request the deletion of only the personal information that was collected from this consumer. It can be concluded that in California, the consumers' right to delete the data does not apply to inferences. A similar conclusion can be drawn from the analysis of the Singapore PDPA, which does not provide for the "right to be forgotten," but only speaks about the possibility of the subject to withdraw consent to the processing of personal data. At the same time, it seems that if the derived data belongs to special categories of data, the processing of which can only be carried out with the consent of the subject, then the subject will

[16] Advisory Guidelines on Key Concepts in The Personal Data Protection Act (Revised 1 October 2021). Para. 16.9.

have the right to demand that the processing of data about him or her be stopped on the grounds that this data is being processed illegally.

The GDPR rules differ significantly from the CCPA and PDPA. Article 17(1) of the GDPR assigns the subject "right to obtain from the controller the erasure of personal data concerning him or her" regardless of the way, in which this data was obtained. However, right to be forgotten is not absolute and can only be implemented if certain conditions are met. In particular, the subject may request the deletion of data about them if such data is processed illegally or are processed for direct marketing purposes, including profiling. In addition, Article 21 of the GDPR establishes the right of the subject to object to the processing of data about him or her, including profiling, if the data is processed in the public interest or for the purpose of ensuring the legitimate interests of the controller or a third party. In the event of an objection, if there are no legally binding legal grounds for processing, the personal data must also be deleted.

The subject's interests during automated processing of personal data (including profiling) are also protected by special guarantees, provided by Art. 22 of the GDPR, among which the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." This provision is criticized in the literature due to its limited practical application (Davis and Schwemer, 2023). First, it applies only to the cases where automated processing, including profiling, leads to legally significant consequences. Conclusions or assessments derived from personal data through their computer processing may have serious consequences for the subject, including long-term ones, but may not always be described in terms of "legal effects." Secondly, Article 22(1) only deals with cases where a legally relevant decision is based solely on automated processing and, therefore, does not apply to semi-automated procedures, when part of the data processing operations is performed with the participation of a person. Moreover, Article 22(2) of the GDPR sets out a number of significant restrictions in the implementation of the right.

IV.4. Other Rights and Special Guarantees

The new EU Artificial Intelligence Act,[17] adopted by the European Parliament on 13 March 2024, consolidates guarantees of the rights of individuals against unfair derivation and use of specific types of personal data. In light of the fact that data mining often involves machine learning and the outputs generated by AI algorithms are often unpredictable and difficult to explain (Fischer, 2020), Article 5 of the Act prohibits placing such AI systems on the market and using them, in particular, for the evaluation or classification of natural persons or groups of persons based on their social behavior or known, inferred or predicted personal or personality characteristics, with the social score leading to discriminatory or unfavorable treatment of certain natural persons or groups in social contexts that are unrelated to the contexts in which the data was originally generated or collected, or of such treatment is unjustified or disproportionate to their social behavior or its gravity. The prohibition will come into effect on 1 January 2025. It will also be illegal to use AI to assess or predict the risk that a natural person will commit a criminal offense, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; to infer emotions of a natural person in the areas of workplace and education institutions; to categorize individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. Should any data regarding an individual be obtained through the use of AI technologies in contravention of this prohibition, it shall be deemed subject to erasure in accordance with Art. 17(1d) of the General Data Protection Regulation (GDPR). Nonetheless, these restrictions do not impede the employment of AI for purposes related to security and law enforcement, nor do they apply in certain other situations.

Special guarantees of subjects' rights related to the processing of derived data may also be provided for cases where such data is processed for marketing purposes, including in recommendation services. In

[17] The EU Artificial Intelligence Act. Available at: https://artificialintelligenceact.eu [Accessed 06.04.2024].

China, for instance, the PIPL does not explicitly regulate profiling or the use of derived personal data. However, it does provide in Art. 24 that commercial marketing targeting individuals based on automated decisions must be accompanied by options that are not specific to their personal characteristics, and individuals must have convenient means to opt out. In March 2022, the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services came into force in China.[18] Article 17 of the document obliges the algorithmic recommendation service providers "to provide users with a choice to not target their individual characteristics, or provide users with a convenient option to switch off algorithmic recommendation services." Moreover, algorithmic recommendation service providers shall provide users with functions to choose or delete user tags used for algorithmic recommendation services aimed at their personal characteristics. Such regulation allows subjects to avoid derivation of inferences for marketing purposes on the stage of providing the primary data.

V. Legal Regime of Derived Personal Data in Russia

The Russian Federal Law "On Personal Data" dated 27 July 2007 No. 152-FZ (hereinafter FLPD), like the Chinese PIPL, does not contain special rules concerning profiling or the derived personal data.

In 2019, by Decree of the Government of the Russian Federation No. 710, the concept of "digital profile" was introduced into official circulation.[19] However, the term "digital profile" in this document is used in a different sense than in the GDPR or CCPA. Digital profile in

[18] The Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services: Order of the Cyberspace Administration of China, the Ministry of Industry and Information Technology of the People's Republic of China, the Ministry of Public Security of the People's Republic of China, and the State Administration for Market Regulation No. 9. Adopted 31 December 2021. Available at: https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm [Accessed 06.04.2024].

[19] Decree of the Government of the Russian Federation No. 710 dated 3 June 2019 "On conducting an experiment to improve the quality and connectivity of data contained in State information resources."

the context of the Decree means a set of up-to-date and reliable data and other information about individuals or legal entities generated in the Unified Identification and Authentication System or other information systems of state and local government bodies, as well as organizations subordinate to them, in order to provide such information with the consent of the subjects to the entities who have requested access to it (Vinogradova et al., 2021, p. 8). Creating a digital profile, therefore, is limited to the information that is used in the public sector, does not involve the use of inferred data, and does not aim to discover or evaluate personal qualities or predict person's behavior. Profiling in the sense that it is used in the GDPR or CCPA is regulated in Russia only by the general provisions of personal data legislation.

Article 16 of the FLPD outlines the rights of individuals in relation to automated processing of their personal data. However, the provisions of this article only apply to situations where decisions are made based solely on automated processing, which have legal consequences for the individual or significantly impact their rights and legitimate interests. Such decisions can only be taken with the explicit consent of the individual, and they have the right to object to such decisions.

The right of objection provided for in Art. 16(4) of the FLPD cannot be exercised in situations where automated processing of personal data is undertaken for marketing or other purposes that do not have direct legal effect on the individual. Moreover, this provision does not apply when the processing of data is not exclusively automated. Consequently, a significant portion of digital profiling activities falls outside the scope of Art. 16 of the FLPD.

The Law does not prohibit the extraction of new knowledge from processed personal data about individuals. At the same time, conditions for the processing of personal data in accordance with Art. 6 of the FLPD may include not only the explicit consent of the individual, but also other circumstances, such as the fulfillment of contractual obligations by the data controller (or "operator") to the individual or the exercise of rights and legitimate interests by the operator or third parties. In practical terms, this latter circumstance can be interpreted broadly to include rights and interests of the operator related to economic activities.

Derived data, within the scope of the FLPD, remains personal data as defined by the Law as "any information that relates directly or indirectly to a specific or an identifiable natural person." The Law does not tie the subject's right to access, clarify, block, or delete personal data to the method of obtaining such data, as stipulated in Art. 14(1) of the FLPD. This implies that these rights can be exercised with respect to derived data as well, provided that the data is incomplete, obsolete, inaccurate, obtained illegally, or unnecessary for the specified purpose of processing. The FLPD acknowledges certain exceptions, primarily related to security concerns and the conduct of law enforcement operations. Additionally, the individual's exercise of their right to access personal data might be denied if it results in a violation of the rights or legitimate interests of other parties.

Starting from 1 October 2023, Art. 10.2-2 of the Federal Law "On Information, Information Technologies and Information Protection" No. 149-FZ also applies in Russia, which provides for the specifics of submitting information using recommendation technologies based on the collection, systematization and analysis of information related to the preferences of Internet users. This Article obliges providers of recommendation services to disclose information about user preferences that are used to generate recommendations, as well as not to violate the rights and legitimate interests of citizens and organizations. At the same time, unlike the Chinese PIPL, the Russian Law does not provide for the right of users to refuse using the recommendation technologies in relation to them or to prohibit processing of certain information about their preferences. It is also debatable whether the Russian legislator considers information about user preferences as personal data. The current regulation provides a significant degree of flexibility for operators who process personal data from Russian internet users for marketing purposes. This includes the use of neural network technologies that may lead to potential violations of the rights of individuals whose data is processed (Minbaleev and Storozhakova, 2023, pp. 76–78).

VI. Conclusions

The timid efforts of legislators to regulate the use of derived personal data represent their desire to adapt traditional legal mechanisms to processes of digital profiling that rely on Big data and artificial

intelligence technologies. At the same time, existing approaches to personal data regulation do not work in the context of Big data (Bottis and Bouchagiar, 2018; Gonçalves, 2017; Savelyev, 2015).

The legal framework for personal data protection remains highly conservative, continuing to view personal data as information originating from an individual, belonging to them, and typically requiring their consent for use. However, valuable personal information is increasingly extracted through computational processes, often without the consent of the data subjects. The processes of discovering non-obvious personal data during profiling and its subsequent use by controllers for estimation and prediction subject's behavior are typically hidden from the data subjects and beyond their control. In light of these developments, there is a need for alternative regulatory paths in personal data protection, shifting the emphasis from merely how data is collected to how it evolves (Wachter and Mittelstadt, 2019, p. 615). The new approaches require increased transparency in automated decision making and the expansion of mechanisms allowing data subject to opt out. (Gonçalves, 2017). Ultimately, the regulation should proceed from the need for a fair and reasonable balance between the interests of data subjects and the controllers, based on mutual confidence and accountability.

References

Adjerid, I. and Kelley, K., (2018). Big data in Psychology: A Framework for Research Advancement. *American Psychologist*. 73(7), pp. 899–917, doi: 10.1037/amp0000190.

Bottis, M. and Bouchagiar, G., (2018). Personal Data v. Big data: Challenges of Commodification of Personal Data. *Open Journal of Philosophy*, 8, pp. 206–215, doi: 10.4236/ojpp.2018.83015.

Bouchagiar, G. and Bottis, M., (2018). Personal Data Protection Models: Aspects of Ownership. *16th International Conference e-Society 2018*. Available at: https://ssrn.com/abstract=3167011 [Accessed 06.04.2024].

Chander, A., (2017). The Racist Algorithm? *Michigan Law Review*, 115, pp. 1023–1045.

Custers, B. and Vrabec, H., (2024). Tell me something new: data subject rights applied to inferred data and profiles. *Computer Law & Security Review*, 52, 105956, doi: 10.1016/j.clsr.2024.105956.

Davis, P. and Schwemer, S.F., (2023). Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making. *Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2023)*. Available at: https://ssrn.com/abstract=4478107, doi: 10.2139/ssrn.4478107 [Accessed 06.04.2024].

Day, P., (2020). Cambridge Analytica and Voter Privacy. *Georgetown Law Technology Review*, 4.2, pp. 583–607.

Fischer, C., (2020). The legal protection against inferences drawn by AI under the GDPR. July 2020. Available at: https://arno.uvt.nl/show.cgi?fid=151926 [Accessed 06.04.2024].

Gonçalves, M.E., (2017). The EU Data Protection Reform and the Challenges of Big data: Remaining Uncertainties and Ways Forward. *Information & Communication Technology Law*. 26(2), pp. 90–115, doi: 10.1080/13600834.2017.1295838.

Malgieri, G. and Comandé, G., (2017). Sensitive-by-distance: quasi-health data in the algorithmic era. *Information & Communications Technology Law*, 26(3), pp. 229–249, doi: 10.1080/13600834.2017.1335468.

Minbaleev, A.V. and Storozhakova, E.E., (2023). Problems of legal protection of personal data in the process of using neural networks. *Courier of Kutafin Moscow State Law University (MSAL)*, 2, pp. 71–79, doi: 10.17803/2311-5998.2023.102.2.071-079. (In Russ.).

Naumann, F., (2014). Data Profiling Revisited. *ACM SIGMOD Record*, February 2014, doi: 10.1145/2590989.2590995.

Niševic, M., (2020). Profiling Consumers Through Big data Analytics: Strengths and Weaknesses of Article 22 GDPR. *Global Privacy Law Review*, 1(2), pp. 104–115.

Roig, A., (2017). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*, 8(3).

Savelyev, A.I., (2015). The Issues of Implementing Legislation on Personal Data in the Era of Big data. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, 1, pp. 43–66. (In Russ.).

Vinogradova, E.V., Polyakova, T.A. and Minbaleev, A.V., (2021). Digital profile: the concept, regulatory mechanisms and enforcement problems. *Law Enforcement Review,* 5(4), pp. 5–19, doi: 10.52468/2542-1514.2021.5(4).5-19. (In Russ.).

Wachter, S. and Mittelstadt, B., (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big data and AI. *Columbia Business Law Review*, 2, pp. 494–620.

Westerlund, M., Isabelle, D.A. and Leminen, S., (2021). The Acceptance of Digital Surveillance in an Age of Big data. *Technology Innovation Management Review*, 11(3), pp. 32–44.

Wiedemann, K., (2022). Profiling and (automated) decision-making under the GDPR: A two-step approach. *Computer Law & Security Review*, 45, 105662, doi: 10.1016/j.clsr.2022.105662.

Information about the Author

Artur N. Mochalov, Cand. Sci. (Law), Associate Professor, Department of Constitutional Law, Ural State Law University named after V.F. Yakovlev, Yekaterinburg, Russian Federation
artur.mochalov@usla.ru
ORCID: 0000-0003-2502-559X

Article

DOI: 10.17803/2713-0533.2024.3.29.514-533

Criminal Prohibitions when Using Mobile Applications

Arseniy A. Bimbinov

Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

Abstract: The article summarizes interim results of a research performed under the project of the Russian Science Foundation focusing on criminal law risks of using mobile applications. These risks can be of two types: the risk of being held criminally liable and the risk of being victimized by the criminal activities of others. The second type of risk is better defined because it is addressed in the context of preventing crimes committed using information and telecommunications networks or in the field of computer information in general. The first one implies not only situations when a user intentionally causes harm through a mobile application, but also cases where people do things, the public danger and wrongfulness of which is not obvious to them. Such persons usually have no desire to violate criminal law but do so failing to understand the unlawfulness of their actions due to the specific environment and technological features. Therefore, the ultimate goal of this project (at the next step) is to ensure safety of mobile application users, including inadmissibility of their unjustified criminal liability, through the development of recommendations on the rules of behavior when using relevant technologies. The purpose of the work within the framework of the presented scientific article is to determine the state of use of mobile applications (characteristics of mobile Internet culture) and those criminal law regulations that may be consciously or unconsciously violated by users of mobile applications. To achieve this goal two sociological surveys were conducted among users of mobile applications to determine how they use their mobile devices. The provisions of the criminal law and the materials of criminal cases were analyzed in order to understand what crimes can be committed by users of mobile

applications who actually did not want and did not understand that they were violating the criminal law.

Keywords: messengers; social networks; dating apps; Mamba; wrongfulness; criminal law; crime

Acknowledgements: The reported study was funded by Russian Science Foundation, project number 22-78-00180

Cite as: Bimbinov, A.A., (2020). Criminal Prohibitions when Using Mobile Applications. *Kutafin Law Review*, 11(3), pp. 514–533, doi: 10.17803/2713-0533.2024.3.29.514-533

Contents

I. Introduction

Individuals aged twenty-five to thirty years old and older may look back at their daily routine fifteen years ago. They would wake up, prepare breakfast using the food stored in the fridge, perhaps they would turn on a personal computer, access a browser and check e-mail, then, remembering by heart their bus time table, they would get ready and leave for the office or college. During the day, they would have some small talks with colleagues or classmates, read a newspaper or, pretending to be immersed in work, read news via the office computer. Later they would go for lunch at a cafeteria or some other fast food casual, and in the afternoon they would call friends on the cell phone or through an office landline and arrange a long-awaited meeting to kick around the latest happenings in each other's lives. They would try to call the clinic to reschedule tomorrow's appointment, as you would be "in poor shape," get through; write the new date in the diary. On the way home they would find the nearest ATM to withdraw some cash

remembering you had to replenish your bus pass or buy a new one. They would meet with friends in a cafe where they had already been before and enjoyed their nice food. They would learn that their friend had been on a fascinating trip viewing intriguing photo in the album he had specially brought. Then they might have been caught by surprise to hear that his ex-girlfriend met a new guy and even moved in with him a few weeks ago, but couldn't break the news to you because their new apartment block doesn't have landline service and hadn't yet been connected to the internet. After realizing that they need a romantic relationship, they would decide to head to a club or bar recommended by some friends to have the opportunity to meet someone on the dance floor or in the chillout. Having no time to go shopping for something posh, they would come home to put on some old but still trendy shirt. After finally reaching the place and having a drink, they suddenly feel tired as the day was long and full of fuss and order a cab home by dialing the number of the taxi company they found in the advertising leaflets near the checkroom. When finally at home, they would set the bedside alarm clock so that they could drop by the office in the morning, despite the day off, just to print out some important documents received by the corporate e-mail, which can only be accessed from the office computer, and to pick up the day planner you forgot on the desk.

For many, this routine has not changed much, but for many others it looks very different these days. People of all ages and in all regions often order home delivery of food and groceries, clothes and other goods, work remotely, receiving and responding to work-related emails, including while traveling, find best traveling routes in automatic mode, receive services through virtual personal accounts, communicate with colleagues, classmates, friends, parents, spouses and children through instant messengers, audio, video or conference calls from anywhere. They are up to date of all events in the life of their loved ones and not only them through social networks. They keep track of social and political news and commentaries reading posts in various online communities, do most publicly available financial transactions in one click, and find best free time options, including dating, without distracting from other activities, and using geolocation for convenience. More and more people choose to organize their lives in this way, especially since all of the

above can be easily accomplished with the help of just one device that is nowadays, without exaggeration, a companion of almost every person — a mobile phone (smartphone).

According to one of the most authoritative data and statistics portals in Russia (Statista), the number of smartphone users in 2022 amounted to 120.14 million people, which is more than 82 % of the country's total population. The number of smartphone users in Russia is forecast to increase steadily between 2023 and 2028, adding 5.6 million new users (+4.57 %). According to this forecast, smartphone user base will hit 128.29 million people by 2028 (Degenhard, 2023). And this is a global trend. Back in 2016, the number of smartphone users worldwide was 3.67 billion or 45 % of the Earth's population (Turner, 2023) at that time, and according to some reports, it reached 86 % in 2022.

It has to be noted that mobile technology penetration figures need some adjustment to make allowance for smartphone sharing and Internet restrictions in effect in some regions of the world (e.g., Iran, DPRK), but as far as Russia is concerned, a definite year-on-year growth is obvious. According to a research performed in the U.S on mobile device usage trends, Russia, along with India, Indonesia, and Turkey, are absolute leaders in terms of growth of smartphone (Flynn, 2023) use time per capita. DataReportal analysts estimated smartphone use time of an average Russian at 3 hours and 39 minutes a day[1] in 2022. Along with that, the time spent daily in front of a desktop PC or laptop tends to decrease.[2] According to the Global Media Intelligence Report, prepared together with Publicis Media-Starcom and GWI,[3] the

[1] Digital 2022: Global overview report. Available at: https://datareportal.com/reports/digital-2022-global-overview-report?utm_source=Global_Digital_Reports&utm_medium=Article&utm_campaign=Digital_2022 [Accessed 11.06.2023].

[2] Statista. Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 4th quarter 2022. Available at: https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/#:~:text=Mobile%20accounts%20for%20approximately%20half,consistently%20surpassing%20it%20in%202020 [Accessed 11.06.2023].

[3] The Global Media Intelligence Report 2022. Available at: https://www.insiderintelligence.com/content/global-media-intelligence-report-2022 [Accessed 11.06.2023].

time spent by people using non-mobile internet-connected devices had reduced by 10 % during the period from 2019 to 2022.

This is confirmed by the International Telecommunication Union data indicating that the growth of stationary and mobile network traffic equaled 23.2 % and 163.6 %, respectively, in Russia over the recent few years. Faster than in Russia growth of mobile traffic is reported only in the United Arab Emirates, Montenegro and Thailand.[4]

The foregoing indicates that the number of mobile phone (smartphone) users in Russia will only be increasing. Users tend to spend more time using apps rather than browsers on their mobile devices. This is just because mobile apps are conveniently focused on personal needs and the use of personal data, thus allowing faster access to desired content. It has to be noted that distinction between browsers and apps on mobile devices has been blurring for years. Most of browser usage time is spent in web windows of relevant mobile applications, driven by marketing, organizational, and other interests of software and app developers and mobile device manufacturers.

Thanks to their variety and functionality, the use of mobile apps is beneficial in many ways, both the above mentioned and others. However, their regular use may also have negative consequences. Most researchers of mobile internet culture point out to such cons of mobile apps as workplace distraction, reduction of personal contacts and psychological addiction (Parasuraman et al., 2017). Signs of smartphone addiction include, for example, constantly checking your phone for no reason, feeling anxious or worried without your phone, waking up in the middle of the night to check for updates and new information, and reduced professional efficiency due to prolonged and sometimes unnecessary use of your phone and the apps on it (Chen, 2015).

Negative consequences also include legal risks, of which criminal risks are most dangerous for users. Criminal law risks can be of two types: the risk of being held criminally liable and the risk of being victimized by the criminal activities of others. The second type of risk is better defined because it is addressed in the context of preventing

[4] International Telecommunication Union: Database of world telecommunication indicators. Available at: https://ourworldindata.org/internet [Accessed 11.06.2023].

crimes committed using information and telecommunications networks or in the field of computer information in general. The first one implies not only situations when a user intentionally causes harm through a mobile application, but also cases where people do things, the public danger and wrongfulness of which is not obvious to them.

Such persons usually have no intent to violate criminal law but do so failing to understand the unlawfulness of their actions due to the specific environment and technological features that provoke a subconscious feeling of permissibility and blunt the perception of the limits of allowable behavior, rights and other legally protected interests of citizens, organizations, society, and state. Users of mobile applications may be prosecuted for lewd acts (Art. 135 of the Russian Federation Criminal Code) or even violent acts of a sexual nature (Art. 132 of the Russian Federation Criminal Code) when posting their own or other people's explicit photos, artistic or historical materials with similar images in online communities accessible to minors; for violation of privacy (Art. 137 of the Russian Federation Criminal Code) when sending to third parties their correspondence with a person who disclosed non-public information about their personal life; for illegal circulation of special technical means (Art. 138 of the Russian Federation Criminal Code) when purchasing spy equipment available on a marketplace as a gift for someone; for illegal use of means of individualization of goods (Art. 180 of the Russian Federation Criminal Code) when composing and filling out the page of one's online store in social network; for cashless counterfeiting (Art. 187 of the Russian Federation Criminal Code) when creating incorrect payment orders in a mobile business bank; for circulating unregistered medical products (Art. 238 of the Russian Federation Criminal Code) when ordering expensive foreign drugs; for the dissemination of pornography (Art. 242 of the Russian Federation Criminal Code) when sending intimate photos or links to relevant videos in personal correspondence, even with one's regular sexual partner, etc. At the same time, these people would probably never show explicit images to minors in real life or counterfeit cash currency, because in real life they realize the public danger of such acts. Therefore, the ultimate goal of the Russian Science Foundation (RSF) project, under which the development of this topic began, is to ensure

safety of mobile application users, including the inadmissibility of their unjustified prosecution, by informing them about the rules of behavior when using relevant technologies.

To achieve this goal, it is necessary to identify situation that has formed about the use of mobile applications (characteristics of mobile internet culture and behavior models of mobile application users) and those criminal law regulations that may be consciously or unconsciously violated by mobile application users. The foregoing is the purpose of this study.

II. Methods

In today's environment, a new world emerges almost every day, and even more frequently in the digital realm. The transformations that began during the Covid-19 pandemic, as well as current world events, are increasingly orienting mobile app developers toward a new paradigm. While previously the acronym VUCA (Volatility — Uncertainty — Complexity — Ambiguity) (Handy, 1995; Johansen, 2007, 2012) was used to describe an unpredictable, rapidly changing environment, now the term BANI has come up to describe the new reality. New times dictate the need to adapt working tools and behavior models to a Brittle, Anxious, Nonlinear and Incomprehensible world. The author of this term, futurist Jamais Cascio, suggests that when analyzing current situation the likely forecast for the near or even distant future (Cascio, 2020) should be taken into account, among other things.

So, it follows that it is impossible to determine the state of mobile apps use without forecasting the prospects of such usage in the foreseeable future. Therefore, this study was carried out without reference to any specific mobile applications but taking into account the demand for their functionality today and in the near future.

The study of publications on mobile Internet culture and materials of judicial and investigative practice allowed us to determine an approximate scope of social relations protected by criminal law, which are subject to the risk of being affected by the use of mobile applications. The most frequent targets of this impact are property rights as well as social relations supporting public health and morality and the procedure of handling legally protected information, including personal data.

To determine behavioral patterns of people when using mobile apps, it was decided to conduct a large-scale poll (survey) among mobile application users.

Survey parameters and procedures were designed based on current analytics in the field of mobile application development as well as specialized literature (in law, sociology, computer and information sciences): from journalism (Chereshnev, 2022) to seminal works (Dremlyuga, 2022). As it follows, most active users of mobile applications are students who, due to their age, involvement in modern, including technological, processes, and their social status, use mobile applications more and longer than other categories of the population and to the fullest extent of their functionality (Jeong and Lee, 2015; Roberts et al., 2014). Therefore, students were identified as the primary group of respondents. Taking into account existing professional affiliations, other groups of respondents were identified as research and teaching staff, criminal law practitioners and any acquaintances of them who, at the request of the former, would agree to participate in the poll and answering specially designed questions.

In order to establish constants and variables in the models of human behavior when using mobile apps, questions were formulated so that to allow, first, establishing socio-demographic characteristics of respondents (age, gender and education level); second, the type (in terms of functionality) of apps they use, frequency and reasons for using; third, the character of use and the experience of causing or suffering harm from using mobile apps; fourth, the level of perception of possible risk associated with the use of mobile apps; fifth, the level of perception that certain activities may constitute a crime; sixth, recent changes in mobile app usage behavior; and seventh, the reasons influencing the transformation of mobile app usage behavior. That was how a questionnaire[5] for the poll was compiled.

[5] For the purpose of greater coverage, in order to achieve a wider geography in Russia and in some foreign countries, and taking into account the topics of the poll, the questionnaire was converted into electronic form with the help of the Google Forms software. Available at: https://docs.google.com/forms/d/e/1FAIpQLSfY3X4sLbKogpmHUQkPx0fOQs_g0K9-J43cV-asNv7ymK7m2g/viewform [Accessed 11.06.2023].

This questionnaire was sent to students of 31 educational institutions in Russia, Kazakhstan, Belarus, and Kyrgyzstan, teachers from criminal and medical law departments of these universities, as well as to lawyers who regularly show up at the events held by the Scientific and Educational Center for Criminal Law Application at the Kutafin Moscow State Law University (MSAL) requesting them to voluntarily and anonymously take part in the poll.

Understanding that the poll mostly involved law professionals and students, who are likely to be much more aware of possible criminal law risks of using mobile applications than people who do not have such knowledge or such education, it was decided that it was necessary to conduct a poll using the same questionnaire among persons without legal education.

This survey was conducted by Analytical Sociology LLC under a relevant contract. According to the report presented by that organization, the poll involved 250 residents from Moscow and St. Petersburg over 23 years old, 50 % men and 50 % women.

As already indicated, some of the questions in the questionnaire concerned the directions of development and transformation of human behavior when using mobile applications, as well as reasons for the changing such behavior. In order to verify and analyze the obtained results, another poll was organized among experts (law and political scientists, sociologists, psychologists, economists, and practitioners in relevant fields with significant experience in assessing social and legal phenomena). They were asked questions about their field of work and work experience, changes in their mobile app usage behavior, their assessment of causes of such changes, and directions in which apps and their usage behaviors will in their opinion[6] be changing.

In addition, focus group discussions were regularly organized with Kutafin Moscow State Law University (MSAL) students to analyze potential criminal law risks of using mobile applications. Each participant kept a mobile app usage diary for four months (from December 2022 to March 2023), indicating which mobile apps he or she needed to use,

[6] Available at: https://docs.google.com/forms/d/e/1FAIpQLSepRsEGvVQgAlhvAL8PUO91yczx-bV1WpfBhXE8S-teZRchvw/viewform [Accessed 11.06.2023].

as well as any risks that may have occurred as a result of such activity. After identifying potential risks, study participants discussed prospects of materialization and management of such risks with their colleagues or classmates.

The results obtained in these studies were compared with each other and analyzed from the viewpoint of applicable criminal law as well as judicial and investigative practices.

III. Results and Discussion

Primary results of the study are data on human behavior patterns when using mobile applications (mobile internet culture) and the factors forming them in relation to criminal responsibility.

More than 1,100 people were polled (including 250 by Analytical Sociology LLC) using basic questionnaire and more than 50 people — using the questionnaire prepared for experts.

It was established that absolute majority of people use the same (in their basic functionality) mobile apps: messengers, social networks, mobile banking, apps to order goods or services and apps to create or watch video content. A third of respondents said that they use photo or video editing apps at least once a week and slightly more use health or fitness apps. In doing so, users are essentially performing the same actions available in their respective apps. For example, messengers and social networks are used for keeping in touch with friends, giving "likes," writing comments or reposting materials posted by friends or other people, posting other materials (texts, photos, videos, etc.) about their lives, communicating on educational, organizational or work-related matters, including offering goods or services. A fifth of respondents said they use mobile applications to find new people with common interests, for friendship or romantic relations, and about 12 % of respondents said they post materials on socially significant events, events related to various agencies or organizations, as well as the life of people they are not acquainted with personally. Half of respondents said they use popular messengers, as most universal and easy-to-use applications (Alonzo and Oo, 2023), to search for information and store data in addition to their main functionality.

The risks, mobile app users are exposed to, are often of similar nature. Thus, absolute majority of users in all age groups admit sending personal documents (passport photos, medical checkup results, etc.) through messengers or social networks. A significant percentage of users lost personal data because of hacked social networks accounts, as well as fell victim to extortionists or scammers.

A quarter of those polled admitted having access to content blocked in Russia through regular use of cryptography (encryption) in the form of special programs, such as VPN services. The majority of users believe that the use of these programs does not entail the risk of prosecution, much less criminal liability, and this belief is based on the rampant use of such services, admissions of their use by public persons and some publications (Vagantov, 2022) on the subject. Given the current state of digital communication, the types and means that enable it, the lineup of users and socioeconomic merits of the blocked IT products, we can only hope that the latter concept will not be unequivocally rejected. However, there are legal grounds for doing so, which can be seen in a number of recent court decisions. For example, Oktyabrsky District Court of Tomsk found Mr. B. guilty of committing a crime under Art. 273, Part 1 of the Russian Federation Criminal Code for using a malicious program. It was established that B., being aware of that the use of the Vipole program would neutralize computer information protection means, regularly launched this malicious computer program, thereby using it. As a result of the B.'s use of the Vipole malicious computer program, information protection means were neutralized so that B. and his activity on the Internet[7] could not be unambiguously identified. We did not find any subsequent cases of this sort but given the wording of the law and the applicable clarifications[8] made by the Russian Federation Supreme Court Plenum it cannot be ruled out that people using applications that affect information security by distorting their network activity may be held liable in the future.

[7] Court ruling of Oktyabrsky District Court of the city of Tomsk dated 21 October 2022. Case No. 1-981/2022.

[8] Russian Federation Supreme Court Plenum Resolution No. 37 dated 15 December 2022 "On Some Issues of Judicial Practice in Criminal Cases Related to Computer Information, as Well as Other Crimes Committed Through the Use of Electronic or Information and Telecommunication Networks, Including the Internet."

It is significant to note that the survey revealed serious distinctions in the attitudes of respondents belonging to different age and professional groups toward certain mobile app use behaviors, including those associated with the risk of criminal prosecution.

The survey we conducted on our own, was initially focused on students, so 88 % of respondents were 18 to 26 years old, university graduates or receiving higher education, usually in law (Group 1). In the survey performed by the contracted specialist organization, 72.4 % of respondents were people aged 27 to 65 years old, the absolute majority of whom had higher or unfinished higher education in disciplines other than law (Group 2). It seems that it was the difference in sociodemographic characteristics of these groups that influenced the choice of their answers. Thus, more than 16 % from Group 2 admitted placing materials (posts, photos, videos, etc.) in social networks and messengers related to socially significant events, activities of agencies or organizations, and other people who are not their family members, while only about 8 % of Group 1 respondents admitted doing that. Much older respondents (compared to students) admitted regular use of paid games and apps to create or watch video content.

33.1 % of Group 2 respondents admitted using dating apps on daily basis, while the figure was only 3.7 % among students. These values correlate with answers to the question "Have you ever sent out any materials (photos, videos) with naked intimate parts of your body on dating apps, dating chat rooms, groups or social networks to find a partner?" Among the older age group, 67.2 % responded negatively, while among students, 85.7 % indicated that they had never sent anything like this. These data show that a significant percentage of people allow themselves to send intimate photos and videos to other persons, believing, as it seems, that criminal liability in this case is excluded due to the private nature of sharing and non-relevance of these materials to pornography. Given marital, partnership, and other interpersonal near-sexual relationships, these arguments are well-reasoned from the social viewpoint. Moreover, subject-matter experts maintain that the exchange of erotic photos between sexual partners via cell phone has no criminal component (Soloviev, 2017). However, law enforcement practice, partly based on some ambiguity in the

law, confirms the opposite. For example, Marksovsky District Court of Saratov Region found Mr. L. guilty of committing a crime under Art. 242, Part 3, Para. "b" of the Russian Federation Criminal Code. It was established in the case that L., on the night of DD.MM.YYYY, being in <address>, using his Redmi cell phone, subscriber number N, the Internet, and WhatsApp messenger, sent a photo of male genital organ, which is a pornographic material, to the cellular communication device, being in use of the victim, who received the above mentioned pornographic material.[9]

It has to be noted that there is still no legal definition of pornography in the national law to date. The attributability of such products to pornography is determined by various non-profit organizations invited by court or investigative authorities. The approach of such organizations is often simple: they cite the same authors, many of whom once cited each other, and then conclude that such and such materials are attributable to pornography due to lack of historical, artistic or scientific value, as this indicative feature of pornography is perhaps the only one that is not questionable (Zazirnaya, 2014). Given that, it is easy to find oneself under pornography dissemination charges if you sent intimate images of yourself in a private message to another user, even if you are in a romantic relationship with him or her.

Under the Russian Federation criminal law, dissemination, public display or advertisement of pornographic materials or objects is a punishable crime, and a reserved warning of that could be formulated as a recommendation based on the results of the RSF project. App users should be aware that Art. 242 of the Russian Federation Criminal Code stipulates criminal liability for disseminating pornographic materials (even if sent to just one person), as well as for their public display. At the same time, demonstration of such materials in private does not entail liability. Therefore, it would be reasonable to use specialized dating applications that provide moderation of images posted by users in their accounts and do not allow users to send their photos during correspondence or allow their hidden placement on one's own personal

[9] Court ruling No. 1-18/2023 of Marksovsky District Court of Saratov Region dated 10 February 2023.

account (in the latter case, if another user is given access to such hidden images, that will be a private demonstration, not dissemination) or allow sending photos in the "self-destruct" mode, i.e., precluding their further use, which cannot be qualified as dissemination.[10]

It appears that these "digital law" nuances should be taken into account by developers of relevant domestic IT products, which are growing in number as popular foreign dating apps are limiting their functionality in Russia or withdraw completely. User guides for relevant applications, as well as software alerts, should warn users of the consequences of not only sending photos and videos, but also of disclosing their personal data and other information that can be used by criminals for committing mercenary and even violent crimes.[11]

Only 10 % of respondents in our poll expressed concern about their safety and the security of their personal data when using dating apps. 4.8 % of respondents from Group 2 and 2.6 % from Group 1 said that they were aware that some of their actions in such applications may constitute an offense.

Survey participants consider social networks and messengers to be the most risky applications. Half of respondents fear being harmed by third parties, and a quarter do not rule out the possibility of being held liable for their own actions when using these apps. For example, more than half of respondents in Group 2 mistakenly believe that they may be held criminally liable for clicking on a "like" under someone else's post in a social network with information about the belonging of certain territories of the Russian Federation to other states (70.2 %), or for indicating HIV-negative status in their profile when they are HIV-positive (50 %), or for ordering from abroad a drug containing potent substances for personal consumption (58.1 %), or for virtual (via video link) actions of a sexual nature for a fee (58.5 %), while the absolute

[10] Russian Federation Supreme Court Plenum Resolution No. 37 dated 15 December 2022 "On Some Issues of Judicial Practice in Criminal Cases Related to Computer Information, as Well as Other Crimes Committed Through the Use of Electronic or Information and Telecommunication Networks, Including the Internet."

[11] Court ruling of Solntsevsky District Court of Moscow dated 13 February 2023, Case No. 1-105/2023.

majority of respondents from Group 1 (mostly law students) know that these actions do not constitute criminal offence.

Representatives of the older age group are more aware than students that showing parts of one's naked body live (via video link) to another person in a private conversation is not a crime (Sharapov, 2021) (86.7 % vs. 77.7 %).

A higher percentage of Group 2 respondents (compared to those from Group 1) correctly indicated that criminal liability is possible for reading private messages addressed to another person[12] (37.1 % vs. 27.3 %), for running a video blog and receiving income from advertisers without proper registration and taxation (53.2 % vs. 40.7 %), and for administering a social network group whose members share information with each other on how to commit suicide (84.7 % vs. 56.9 %). If the first of the above situations is not very common and the second one depends on the amount of income received, the low awareness of the latter among students is a cause for concern.

The topic of responsibility for participation in so-called death groups has been widely discussed among broad public for several years now with lots of information and methodological materials for schoolchildren and their parents (Maslova, 2020) and scientific papers (Ustinova, 2020) published and numerous educational events and programs held in online communities and youth-oriented media. Despite the fact that provisions of Art. 110–110.2 of the Russian Federation Criminal Code, especially in respect of those who organize suicide promotion activities, do not clearly indicate prohibited actions in particular, the meaning of these norms is clear and should be communicated to broad public. Given the paramount importance of human life, any direct or indirect complicity (Bimbinov, 2023) in the suicide of another person, especially a minor, is absolutely unacceptable, without regard to motives. In its recent decision, the Russian Federation Constitutional Court pointed out that "taking into account the restrictions established for dissemination of certain types of information, Art. 110.2 of the Russian Federation Criminal Code does not imply prohibition of lawful behavior, but is

[12] Court ruling of Engelsky District Court of Saratov Region dated 5 May 2021, Case No. 1-1-392/2021.

aimed at protecting an indefinite circle of persons (which may include minors, who, due to the incomplete formation of their personality, are characterized by immaturity and suggestibility) from harmful (negative) influence on their psyche, which may, under unfavorable circumstances, provoke them into committing suicide or assist them in that act." Therefore, this provision is indirectly aimed at protecting human life as a supreme good and a special constitutional value, which corresponds to the constitutional duties of the state to ensure the rights and freedoms of citizens and to take adequate measures to protect them.[13]

As already indicated, the most popular software products include applications for ordering goods or services, including government services, as well as mobile banking. Only a small number of respondents (about 3 %) are concerned that any actions using these applications may constitute an offense or crime. This is probably due to the fact that the vast majority of users of such applications perform the same non-intrusive actions, such as calling a cab, ordering the delivery of goods, transferring money, and so on. However, some functions of these IT products and the operations performed using them are not without risk. For example, financial transactions should not be made if their characteristics, such as the payment addressee or its purpose, are unknown.

Sending money to an unknown recipient can lead to a variety of criminal cases, from drug trafficking to treason. Inadmissibility of falsifying the purpose of payment should be clear to all persons involved in economic activity, including self-employed and small businesses. Insufficiently responsible attitude to non-cash money circulation, the importance and legal protection of which is not inferior to cash, unfortunately leads to criminal prosecution. Thus, Arzamas City Court of Nizhny Novgorod Region found Ms. R. guilty of committing eighteen crimes under Art. 187, Part 1 of the Russian Federation Criminal Code. The investigation determined that the defendant, acting willfully and using the functionality of Sberbank Business Online, composed

[13] Decision No. 1104-O of the Russian Federation Constitutional Court dated 30 May 2023 "On refusal to accept for consideration the complaint of Polina Dmitrievna Yesipova about violation of her constitutional rights by the provisions of Art. 110.2 of the Russian Federation Criminal Code."

counterfeit payment orders relating to electronic means of payment, namely: payment order No. for RUB 20,000, payment order No. for RUB 5,000, payment order No. for RUB 4,000, and payment order No. for RUB 1,500, by entering false (made up by her) information about the purpose of payment, i.e., she generated counterfeit payment orders relating to electronic means of money transfer.[14]

The abovementioned situations and criminal cases initiated in connection with them clearly demonstrate that human behavior patterns when using mobile applications are subject not only to the risk of being harmed, but also to the risk of criminal liability, including in cases where unlawfulness of such actions is not obvious. Improving this state of affairs should be the task of the state, professional legal community and applied science.

IV. Conclusions

The results of this study indicate that people most readily use messengers, social networks, applications for ordering goods or commercial services, mobile banking and dating applications, the criminal law risks of using which have their specifics primarily due to their functionality. As the survey results indicate, this situation can change if relevant security measures are implemented, including the possibility of criminal prosecution; if people come to want to ensure their privacy; or if some apps we are used to cease to exist (be blocked or slowed down).

As things stand today, there are no prospects that the functionality of the most popular apps will cease to be in demand. User and expert polls and analytical data on current IT developments indicate that new applications (with full voice support; cloud-based (not tied to operating system or device model); specialized (allowing to receive professional consulting assistance); with the function of virtual and augmented reality; self-learning; ecosystem applications) will reproduce the functions of all currently popular applications. Criminal law risks will soon become common for all mobile apps, and, therefore, safe

[14] Court ruling of Arzamas City Court of Nizhny Novgorod Region dated 26 November 2021, Case No. 1-414/2021.

use guidelines should be universal. Such approach can, among other things, create prerequisites for the formation of new interdisciplinary research areas at the intersection of law and other sciences. Further clarification of the state of mobile culture and the scope of criminal law risks will allow balancing and improving the approach to ensuring legal protection of social relations by preventing criminal and near-criminal behavior. The poll results indicate that, unlike Group 2 respondents, young people would prefer the option of being warned about criminal responsibility with justification of its reasons. For example, a warning of criminal liability for drug purchase should be accompanied not only by the indication of possible prison terms or other punishment, but also by pointing to the public danger of such activity and other reasons for its criminalization.

References

Alonzo, D. and Oo, C.Z., (2023). The use of Messenger for research collaboration: An auto-ethnographic study. *Front Psychol.,* 10, 13, doi: 10.3389/fpsyg.2022.1076340.

Bimbinov, A.A., (2023). Criminal liability for virtual "complicity" in the suicide of minors. *Suicidology*, 14 (1), pp. 154–168, doi: 10.32878/suiciderus.23-14-01(50)-154-168. (In Russ.).

Cascio, J., (2020). *Facing the Age of Chaos*. Available at: https://medium.com/@cascio/facing-the-age-of-chaosb00687b1f51d [Accessed 11.06.2023].

Chen, H., (2015). Asia's Smartphone Addiction. *BBC*. Available at: http://www.bbc.com/news/world-asia-33130567 [Accessed 11.06.2023]

Chereshnev, E., (2022). *Form of life No. 4: How to stay human in the heyday of artificial intelligence*. Moscow: Alpina Publ. ISBN 978-5-9614-7366-7. (In Russ.).

Degenhard, J., (2023). Number of smartphone users in Russia from 2013 to 2028. *Statista*. Available at: https://www.statista.com/forecasts/1147055/smartphone-users-in-russia [Accessed 11.06.2023].

Dremlyuga, R.I., (2022). *Criminal law protection of the digital economy and information society from cybercrime attacks: doctrine,*

law, enforcement. Moscow: Yurlitinform. ISBN 978-5-4396-2368-6. (In Russ.).

Flynn, J., (2023). 20 Vital Smartphone Usage Statistics (2023): Facts, Data, and Trends On Mobile Use in The U.S. *Zippia.com*. Available at: https://www.zippia.com/advice/smartphone-usage-statistics/ [Accessed 11.06.2023].

Handy, C.B., (1995). *The Age of Unreason*. Arrow Business Books.

Jeong, H.S. and Lee, Y.S., (2015). Smartphone addiction and empathy among nursing students. *Adv Sci Technol Lett*, 88, pp. 224–228.

Johansen, R., (2007). *Get There Early: Sensing the future to compete in the present*. Oakland, CA, USA: Berrett-Koehler.

Johansen, R., (2012). *Leaders Make the Future: Ten New Leadership Skills for an Uncertain World*. Berrett-Koehler Publishers.

Maslova, E.V., (2020). *Cautiously: "death groups"!* Omsk. Available at: http://ou104.omsk.obr55.ru/files/2020/06/790546854.pdf [Accessed 11.06.2023]. (In Russ.).

Parasuraman, S., Sam, A.T., Yee, S.W.K., Chuon, B.L.C. and Ren, L.Y., (2017). Smartphone usage and increased risk of mobile phone addiction: A concurrent study. *Int J Pharm Investig,* 7 (3), pp. 125–131, doi: 10.4103/jphi.JPHI_56_17.

Roberts, J.A., Yaya, L.H. and Manolis, C., (2014). The invisible addiction: Cell-phone activities and addiction among male and female college students. *J Behav Addict*., 3, pp. 254–265, doi: 10.1556/JBA.3.2014.015.

Sharapov, R.D., (2021). Qualification of crimes related to illegal trafficking of pornographic materials and objects. *Legality*, 8, pp. 43–48. (In Russ.).

Soloviev, V.S., (2017). Revenge porn: the essence of the phenomenon and the problems of its criminal-legal assessment. *Criminal law*, 6, pp. 60–64. (In Russ.).

Turner, A., (2023). *How Many Smartphones Are in the World?* BankmyCell. Available at: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world [Accessed 11.06.2023].

Ustinova, T.D., (2020). Inducement to suicide or assistance to suicide: a critical analysis. *Lex Russica*, 3, pp. 151–159, doi: 10.17803/1729-5920.2020.160.3.151-159. (In Russ.).

Vagantov, V., (2022). How to return the "escaped" money. *Practical accounting*, 3, pp. 66–75. (In Russ.).

Zazirnaya, M.M., (2014). On the question of the definition of pornography. *Criminal law*, 6, pp. 15–21. (In Russ.).

Information about the Author

Arseniy A. Bimbinov, Cand. Sci. (Law), Associate Professor, Department of Criminal Law, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

bimbinov@yandex.ru

ORCID: 0000-0002-7440-293X

SHANGHAI COOPERATION ORGANIZATION

Article

DOI: 10.17803/2713-0533.2024.3.29.534-568

China and Shanghai Cooperation Organization: Reconsideration and Improvement of Multilateralizing Effect of Most Favored Nation Clause in BIT

Ren Yanyan,[1] **Zhao Zhixin**[2]

[1] *China National Institute for SCO International Exchange and Judicial Cooperation, Shanghai, China*

[2] *Shanghai University of Political Science and Law, Shanghai, China*

***Abstract*:** Since the *Maffezini* case, debates upon the application of the Most-Favored-Nation (MFN) clause have never stopped. Research from the perspective of the Shanghai Cooperation Organization (SCO) can test the way for further advancement of this issue. The analysis on the international investment arbitration cases involving the SCO states may shed some light on the crucial point on dispute. At present, the bilateral investment treaties (BIT) between China and other states of the SCO are in an urgent need of renewal in order to meet the interests of deepening investment cooperation. Problems of fragmentation of the interpretation method and of unpredictability of the interpretation conclusion of the MFN clauses manifested in international investment disputes involving SCO states will provide concrete preventative suggestions on the updating of the wording of MFN clauses. Under SCO framework, the multilateral effect of the MFN clause can play a model role for other regional integration organizations to build an integrated and multilateral investment treatment system in the fragmented and bilateralism-based framework of international investment law, and in fact promote investment facilitation for regional organizations.

***Keywords*:** bilateral investment treaty (BIT); Most-Favored-Nation (MFN) Treatment; Shanghai Cooperation Organization (SCO); Multilateralization

Acknowledgments: The article was prepared with the financial support of the Ministry of Justice of the People's Republic of China (project No. 22SFB1013)

Cite as: Yanyan, R. and Zhixin, Zh., (2024). China and Shanghai Cooperation Organization: Reconsideration and Improvement of Multilateralizing Effect of Most Favored Nation Clause in BIT. *Kutafin Law Review*, 11(3), pp. 534–568, doi: 10.17803/2713-0533.2024.3.29.534-568

Contents

I. Introduction

MFN in the context of international investment is an international law obligation arising from specific provisions in the International Investment Agreement (IIA). The application of MFN provisions is usually limited by the *ejusdem generis* principle. "The host state is obliged to grant no less favorable treatment to investors of the other contracting state to the BIT than that the host state grant to third-state's investors in the same or similar matters under like circumstances."[1] The BIT between the host state and the other contracting state is usually called a "basic treaty" and the BIT between the host state and the third party is usually called a "third-party treaty." The MFN clause is able to "make counterbalance between different negotiating powers, entitling the contracting party, which is in lower bargaining position, to the treatment that the party in higher position accords to its other investing partner."[2] The substantive legal effect of the MFN clause is that "once a state accords to investors of another state more favorable treatment, then all the investors of other states which have concluded the MFN clause with the state shall enjoy such favorable treatment."[3] The MFN clause, for its multilateral effect and potential in maintaining fair, liberal and facilitative international investment environment, has become an indispensable structural provision in the standard of treatment section in IIA. According to data released by the United Nations Commission on Trade and Development (UNCTAD), among 2,592 mapped IIAs, only 37 IIAs have no MFN clause. All the BITs concluded between China and other SCO states stipulated Most-Favored-Nation treatment.

Since SCO is a comprehensive international cooperation organization covering the fields of politics, economy, trade and humanities and the Charter of the SCO in 2001 put forward the vision of investment facilitation, the MFN clauses are expected to empower investment facilitation and multilateralization of the SCO. However, the current

[1] UNCTAD Investment PolicyHub. Available at: https://investmentpolicy.unctad.org/international-investment-agreements/iia-mapping. P. 13 [Accessed 13.03.2024].

[2] UNCTAD, World Investment Report 2023: Investing in Sustainable Energy for All. New York, United Nations. P. 377.

[3] UNCTAD Investment PolicyHub. P. 13.

MFN clauses in the China — SCO states BITs have obvious differences in wording, which may lead to different scope of application and exceptions, and MFN clauses themselves have a large room for improvement. At the same time, SCO states have constantly been parties to the international investment arbitration involving disputes over MFN clauses, and the respective arbitration tribunals have different opinions on the scope of application. This paper aims to analyze the scope of application of the MFN clause by taking the China — Shanghai Cooperation Organization BIT as an example, combined with the arbitration case of investment disputes involving SCO states, and put forward concrete suggestions, in the future negotiation and upgrading process, for the improvement and perfection of the MFN clauses of the China — SCO states BITs.

II. Evolution of Most-Favored-Nation Clause in BITs between China and Other SCO States

Since the conclusion of the China — Sweden BIT in the early 1980s, the degree of investment liberalization in China has been increasing, and China has become the state which has concluded the most BITs and is the second largest foreign direct investment importer.[4] BITs, which constitute the state's promise to protect the legitimate rights and interests of foreign investors and provide them with remedies, have become an indispensable prerequisite for attracting foreign investment and promoting investment facilitation, and can also provide an impetus for the development of investment facilitation within the SCO. As "one of the most effective state obligation of investor protection in the IIA" (Dolzer and Schreuer, 2012, p. 186), the MFN clause should become an important driving force to promote international investment cooperation among SCO states. At present, the SCO has nine member states, three observer states and 14 dialogue partners. China has concluded BIT with 22 other SCO member states. All of the 22 bilateral investment treaties contain MFN clauses, which establish the treaty obligations under the International Investment Law to build a level playing field for international investment between China and other SCO states and

[4] UNCTAD, World Investment Report 2023: Investing in Sustainable Energy for All. P. 8.

accelerate the implementation of the vision of investment facilitation and liberalization outlined in the Programme for Multilateral Economic and Trade Cooperation of the SCO.

II.1. The Differences of Generations in MFN Clauses in BITs between China and Other SCO States

By searching the MFN clauses stipulated in the BITs between China and other SCO states, it can be seen that the MFN clauses in the BITs between China and other SCO states have certain generational characteristics. In order to expand the effectiveness of the MFN clause in the protection of investors' rights and interests while maintaining the host state's sovereignty over regulating investors, the MFN clauses in "China — SCO states BITs" have undergone one adjustment and can be divided into two generations.

Scope of Application of MFN Clauses Stipulated in China — SCO states BITs

BIT and Time of Conclusion	Scope of Application stipulated
1986 China — Kuwait BIT	Treatment accorded to the investments of investors of either state and the investments' returns, management, maintenance, use, enjoyment or disposal in the territory and maritime zone of the host state
1987 China — Sri Lanka BIT	Treatment accorded to the investments of the investors of either contracting state and the investments' returns in the territory of the host state
1989 China — Pakistan BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1991 China — Mongolia BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state

1992 China — Kazakhstan BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1992 China — Kyrgyzstan BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1993 China — Belarus BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1993 China — Tajikistan BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1994 China — United Arab Emirates BIT	Treatment accorded to the investments of either contracting state in the territory of the host state and the investments' returns, management, maintenance, use, enjoyment, disposal and other activities associated
1994 China — Azerbaijan BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1995 China — Armenia BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1996 China — Egypt BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1997 China — Saudi Arabia BIT	Treatment accorded, subject to the host state's laws and regulations, to investments of investors of either contracting state and the investments' returns, management, maintenance, use, enjoyment or disposal or the means to assure their rights to such investments like transfers and indemnifications or with any other activities associated with the investments in the territory of the host state

1999 China — Bahrain BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1996 China — Cambodia BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
1999 China — Qatar BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
2000 China — Iran BIT	Full legal protection and fair treatment accorded, in accordance with the laws and regulations of the host state, to investments of investors of either contracting state effected within the territory of the other contracting party
2001 China — Myanmar BIT	Treatment accorded to the investments and activities associated with investors of either contracting state in the territory of the host state
2006 China — India BIT	Treatment accorded to the investments of investors of either contracting state, including in respect of returns of the investments
2006 China — Russia BIT	Treatment accorded to the investments and activities associated with investors of either contracting state
2011 China — Uzbekistan BIT	Treatment accorded, in like circumstances, to the investments of either contracting state with respect to the establishment, acquisition, expansion, management, maintenance, use, enjoyment, sale or disposal hereof
2015 China — Turkey BIT	Treatment regarding investment permission, within the host state's framework of laws and regulations, to the investments and activities associated with investors of either contracting state in the territory of the host state; Treatment is accorded to these investments once established

The first generation of MFN clauses in BITs concluded between China and other SCO states started with 1986 China — Kuwait BIT, ended with the conclusion of 2001 China — Myanmar BIT. This first generation's development was stagnant for 14 years and its main characteristic was that all of the BITS adopted the territorial principle, which meant that the investment stipulated in MFN clauses referred only to the investments established and effected within the territory of the host state. Although the wording of China — Kuwait BIT is a "territory and maritime zone" due to a large number of marine energy investment cooperation projects between China and Kuwait, most of the MFN clauses in first generation defined this principle as only referring to the land under the sovereignty of the host state.

In accordance with the Art. 31 of the *Vienna Convention on the Law of the Sea,* the interpretation of a treaty provision is obliged to start with finding out its ordinary and plain meaning. The ordinary meaning of the phrase "in the territory of the host state" indicates that the prerequisite of comparing the treatment accorded to a contracting party of the basic treaty and that accorded to a non-contracting party and then judging whether the MFN clause has been violated is that both the contracting state and the non-contracting state have made investments or started activities associated with the investments. "Treatment within the territory of the host state" or similar wording has been universally adopted by IIA (Perez-Aznar, 2017, pp. 777–806). The international investment arbitration tribunal, namely the Stockholm Chamber of Commerce (SCC), which is relevant to MFN treatment, made interpretations according to this wording's ordinary meaning and its purpose of contracting. In 2004, in *Berschader* case[5] the SCC clarified that the wording of "treatment within the territory of the host state" means that both the contracting parties intended to limit the scope of the MFN clause to the substantial treatment accorded to the investors of a contracting state in the territory of the host state. The tribunal further reasoned that the provisional obligation the host state undertakes in accordance with another BIT in respect of a contracting

[5] *See* Vladimir Berschader and Motse Berschader v. The Russian Federation (Berschader v. Russia). SCC, Case No. 080/2004, Award and Correction (21 April 2006). Para. 185.

state of that BIT is not the "treatment within the territory of the host state." Besides, in the previous international investment arbitration involving MFN treatment, the point at issue was usually that what kind of provisions can be introduced into a basic treaty from a third-party treaty by the MFN clause, and the *Maffezini v. Spain* case[6] resolved by the International Centre for Settlement of Investment Disputes (ICSID) shed some light on this dispute, clarifying that procedural provisions in a third-party treaty can be introduced into a basic treaty by the MFN clause. The *Berschader* case in 2004 furthered this dispute by reasoning why a more favorable provision in a third-party treaty cannot be introduced into a basic treaty because it is not the "treatment within the territory of the host state."

The second generation of MFN clauses in BITs between China and other states of the SCO began in the China — India BIT in 2006 and the China — Russia BIT in 2006. They were further refined in the China — Uzbekistan BIT in 2011. The MFN clauses of the 2020 China — Turkey BIT basically follow the model of the 2011 China — Turkey BIT. The main features of this generation of MFN clauses can be basically seen in two aspects: one is to dilute the principle of "treatment in territory," and the other is to explicitly incorporate the "like circumstances" rule in the scope of application of the MFN clauses.[7]

The dilution of the principle of "treatment in territory" has gone through several adjustments. In *Berschader* case, the arbitration tribunal denied the legality of importing a substantial provision from a third-party treaty into a basic treaty through the MFN clause. As a consequence, the BIT concluded between China and Russia abandoned the wording of "treatment within the territory of the host state" in

[6] Emilio Agustín Maffezini v. Kingdom of Spain. ICSID, Case No. ARB/97/7. Available at: https://investmentpolicy.unctad.org/investment-dispute-settlement/cases/19/maffezini-v-spain [Accessed 13.03.2024].

[7] *See* Art. 4(1) of the China — Uzbekistan BIT: Each Contracting Party shall accord to investors of the other Contracting Party and the investments thereof treatment no less favorable than that it accords, in like circumstances, to investors and the investments thereof of any third State with respect to the establishment, acquisition, expansion, management, maintenance, use, enjoyment, sale or disposal of investments.

the MFN clause and made the MFN clause extremely vague.[8] To some extent, this indicates that China and Russia, both founding states of the SCO, are trying to include the provisional obligations of the host state to the contracting party of the third-party treaty in the "treatment" of the MFN clause, so as to prevent the arbitral tribunal from completely denying the legitimacy of importing the contents of the third-party treaty into the basic treaty from the perspective of treaty interpretation in the future investment disputes. Compared with the China — Russia BIT, the subsequent China — Turkey BIT revises the dilution of the principle of "treatment within the territory" and uses the expression of "within the territory" again. However, this BIT deconstructs the "treatment" into two parts: the treatment at the pre-establishment stage and the treatment at the post-establishment stage. What is more, it reduces the wording of "within the territory" to the qualifier of treatment at the pre-establishment stage. From the perspective of text interpretation, there are two possible ways of interpreting: the first one is to avoid repetition of the text; the other one is to expand the scope of application of MFN treatment at the post-establishment stage and thereafter provide interpretative feasibility for the importation of third-party treaty provisions through MFN provisions.

The second generation of MFN clauses universally incorporates the "like circumstances" rule.[9] The "like circumstances" rule in the MFN clause has the function of clarifying the reference system needed when making the comparisons of treatment. To be specific, the MFN obligation with the "like circumstances" rule is that the treatment the host state accords to investors of a contracting state shall not be less favorable than the treatment the host state accords to investors of a non-contracting party who are in similar circumstances rather than all

[8] *See* Art. 3(3) of the China — Russia BIT: Neither Contracting Party shall subject investments and activities connected with such investments by the investors of the other Contracting Party to treatment less favorable than that accorded to the investments and activities in connection with such investments by the investors of any third State.

[9] *See* Art. 3(4) of the China — Turkey BIT: Within the framework of the hosting Contracting Party's laws and regulations, each Contracting Party shall admit in its territory investments on a basis no less favourable than that accorded in like circumstances to investments of investors of any third State.

the treatment accorded to all the investors of a non-contracting state. The incorporation of the "like circumstances" rule makes the MFN clause more in line with its purpose and the development trend of international investment agreements. MFN treatment is considered to ensure that investors of a negotiating party that is in a lower position can enjoy more preferential treatment granted by the other party that is in a higher position to investors of non-contracting states. On the other hand, MFN treatment also limits the autonomous will of the stronger party for it makes the stronger party to conclude BITs more carefully especially when negotiating on the content included in the treaty. It also impacts the principle of international law that "treaties do not create obligations for third states." The rule of "like circumstances" has a moderating effect on the conflict between the two values. Some scholars believe that this rule is an inherent constitutive element of MFN treatment and regardless of the exact wording of specific MFN clauses, they should be interpreted as they contained "like circumstance" rule (Perez-Aznar, 2017, p. 798). What is more, investment treaties that have come into force since 2010 have also generally incorporated "like circumstances" rules into MFN clauses.[10] However, there are still many BITs that do not include the "like circumstances" rule in MFN clauses, and it is worth considering whether the "like circumstances" rule has been the inherent constitutive element of MFN clauses.

II.2. The Comparison between the MFN Exception Clauses in China — SCO State BITs

A comparison between the exceptions set in MFN clauses of different China — other SCO states BIT would to some extent reveal the different attitudes SCO states hold to the scope of MFN. The MFN exception clauses in such BITs have listed only a small number of exceptions to which the MFN clause does not apply. Those exceptions listed in different BITs are similar and can therefore be divided into two types. The first type is the exception of a regional economic integration

[10] *See* 2017 the China — Hong Kong SAR BIT, the 2017 Japan — Israel BIT, the 2016 Rwanda — Turkey BIT, the 2016 Canada — Hong Kong SAR BIT, the 2016 Canada — Mongolia BIT.

agreement, that is the preference or treatment granted to a state by another state in accordance with a regional economic agreement such as a free trade agreement or a customs union agreement does not fall within the scope of application of the MFN clause. Such preferences or treatment cannot be spread among the parties to the basic treaty even if it is more favorable. The second is the exception of international agreements related to tariffs, that is one state waives or reduces taxes on investors from another state in accordance with international agreements on or partially on taxation. Since the relevant preferential treatment is granted to everyone among the parties based on the principle of equality and reciprocity, then the relevant tax preferential treatment cannot be unconditionally spread among the parties to the basic treaty.

In the MFN exception clauses in recent China — SCO states BITs, the dispute settlement mechanism has been a new exception. The China — Uzbekistan BIT and the China — Turkey BIT both expressly stipulated that MFN treatment does not apply to "dispute settlement mechanism stipulated in other IIA." What is also worth mentioning is that the 2001 China — Myanmar BIT does not list dispute settlement mechanism as a exception, but the 2009 *Agreement on Investment of the Framework Agreement on Comprehensive Economic Cooperation between the People's Republic of China and the Association of Southeast Asian Nations* has incorporated dispute settlement mechanism in the MFN exception clause,[11] which means that in the investment disputes between China and Myanmar, dispute settlement resolution set out in the other BIT cannot be applied to such disputes. Since *Maffezini v. Spain* in 2000 triggered the dispute over whether the MFN clause can be used to introduce the dispute settlement mechanism set out in a third-party treaty into the basic treaty, the later arbitration tribunal has not reached a conclusion on this dispute, and the SCO states have become the parties to the relevant disputes for many times.[12] The MFN

[11] *See* Art. 5(4) of China — ASAN IIA: For greater certainty, the obligation in this Article does not encompass a requirement for a Party to extend to investors of another Party dispute resolution procedures other than those set out in this Agreement.

[12] *See* H&H Enterprises Investments Inc v. Arab Republic of Egypt. ICSID, Case No. ARBO9/15; AsiaPhos Limited and Norwest Chemicals Pte Limited v. People's Republic of China. ICSID, Case No. ADM/21/1; Ansung Housing Co Ltd. v. People's

exception clause in the China — Russia BIT is relatively special for it does not specify in the MFN clause that the MFN treatment applies to procedural matters, nor does it include procedural matters in the MFN exception clause. Instead, it adds in its protocol that the MFN treatment applies to the administrative review procedure conducted by investors of one party in another party.

III. Disputes Involving MFN Treatment in respect of SCO States

Similar to the national treatment clause, the MFN clause is used to regulate issues related to discrimination against foreign investors based on nationality, and the specific application should be based on comparison (Ustor, 1974, p. 117). In international arbitration of investment disputes, the purpose of invoking the MFN clause is usually to request the arbitral tribunal to apply the more preferential treatment in a third-party treaty to the parties to the basic treaty, and rarely invokes the MFN clauses to attempts to allege that the domestic measures of the host state violate MFN treatment and thus constitute discrimination (Wang, 2020, p. 184). In international investment arbitration involving SCO states, the purpose of invoking the MFN clause by the parties concerned is not only to reach the modification or derogation of the basic treaty by comparing the basic treaty with the third-party treaty, but also to obtain more preferential treatment granted to other foreign investors by the host state according to its domestic measures.

III.1. Invoke MFN Clauses to Expand the Content of Basic Treaty

It has been recognized by many arbitral tribunals that MFN clauses can be used to import substantial provisions like the Fair and Equitable Treatment clause from a third-party treaties into the basic

Republic of China. ICSID, Case No. ARB/14/25; Vladimir Berschader and Motse Berschader v. The Russian Federation. SCC Case No. 080/2004; RosInvest Co UK Ltd v. Russian Federation. SCC Case No. V079/2005; Beijing Urban Construction Group Co Ltd v. Republic of Yemen (Beijing Group v. Yemen). ICSID, Case No. ARB/14/30.

treaties, thus creating new investor protection obligations for parties to the basic treaties.[13] A scholar points out that this practice is no longer controversial, and it creates a unified standard of investment protection treatment for investors from different countries, making the legal framework for regulating investors more harmonious (Sharmin, 2018, p. 85). In contrast, international investment arbitration cases where SCO states are disputing parties focus more on revising or derogating the procedural provisions in the basic treaty through MFN clauses, which is still in debates.

In *AsiaPhos* [Singapore investor] *v. China*, the claimant held that the MFN clause of the 1985 China — Singapore BIT expressly stipulates that Art. 5, 6 and 11 do not fall within the scope of application of MFN treatment.[14] However, the dispute settlement mechanism in the 1985 China — Singapore BIT is stipulated in Art. 13. Moreover, the MFN clause, as a clause aimed at ensuring that the treatment previously granted by the host state to investors of one state matches the treatment later granted by the host state to investors of another state, its application to the dispute settlement mechanism is barrier-free.[15] The Tribunal first cited the *Berschader v. Russia* case that also involved the SCO states. The arbitral tribunal of *Berschader v. Russia* pointed out that the replacement of the dispute settlement clause set out in the basic treaty through the MFN clause is legitimate only in two circumstances: first, the MFN clause "expressly and unambiguously" clarifies that it can be applied to the dispute settlement clause; second, modifying the dispute settlement provisions of the basic treaties through MFN provisions is in line with the contracting purposes of the parties. The Tribunal held

[13] Rumeli Telekom, A.S. and Telsim Mobil Telekomunikasyon Hizmetleri; AS. v. Republic of Kazakhstan (Rumeli v. Kazakhstan). ICSID, Case No. ARB/05/16, Award (29 July 2008), Para. 560, 575 and 581–619; LESI SpA and ASTALDI; SpA v. People's Democratic Republic of Algeria (LESI v. Algeria). ICSID, Case No. ARB/05/3, Award (12 November 2008), Para. 150–164; ATA Construction, Industrial and Trading Company v. The Hashemite Kingdom of Jordan (ATA v. Jordan). ICSID, Case No. ARB/08/2, Award (18 May 2010), Para. 125 and 133.3; OAO Tatneft v. Ukraine (OAO Tatneft v. Ukraine). UNCITRAL, Award (29 July 2014), Para. 365.

[14] Art. 4 of 1985 China — Singapore BIT: Subject to Art. 5, 6 and 11, neither Contracting Party shall in its territory subject investments admitted...

[15] *See* AsiaPhos Limited and Norwest Chemicals Pte Limited v. People's Republic of China. ICSID, Case No. ADM/21/1, Award, p. 14.

that the wording of excluding Art. 5, 6 and 11 from the MFN application scope in the basic treaty does not expressly and unambiguously allow the replacement of the dispute settlement clause in accordance with the MFN clause. For the purposes of the contracting Parties, the Tribunal held that the exchange of letters between the contracting parties during the signing period of the 1985 China — Singapore BIT indicated that the contracting parties recognized that the arbitration consent listed in the dispute settlement clause could be modified after renegotiation and new agreement was reached, and the new arbitration clause would replace the dispute settlement clause of the basic treaty. Therefore, the introduction of a new dispute settlement mechanism directly based on the MFN clause is not consistent with the contracting purpose of the parties.[16]

In *Pugachev* [French investor] *v. Russia*,[17] the claimant *Pugachev* held that since *Maffezini* case first used the MFN clause to circumvent procedural matters such as "exhaustion of local remedies" and cooling-off periods, and in many subsequent cases, the arbitral tribunal supported the modification or reduction of the procedural provisions of the basic treaty through the MFN clause,[18] MFN clause's application to procedural matters has been a well-settled practice.[19] The Respondent, the Russian Federation, held different view that indeed, it is true that many arbitral tribunals support the application of MFN clauses to procedural matters, it does not mean that this approach is free of doubt, and different arbitral tribunals will reach different conclusions facing

[16] AsiaPhos Limited and Norwest Chemicals Pte Limited v. People's Republic of China. ICSID, Case No. ADM/21/1, Award, pp. 78–80.

[17] Sergei Viktorovich Pugachev v. The Russian Federation. No administering institution.

[18] *See* Siemens AG v. Argentina. ICSID, Case No. ARB/02/8; Gas Natural SDG, S.A. v. Argentina. ICSID, Case No. ARB/03/10; Camuzzi International, S.A. v. The Argentine Republic. ICSID, Case No. ARB/03/2; RosInvest v. The Russian Federation. SCC, Case No. V079/2005; National Grid plc v. Argentine Republic. UNCITRAL; Suez, Sociedad General de Aguas de Barcelona, S.A. and Vivendi Universal SA v. Argentina and AWG Group Ltd v. Argentina. ICSID, Case No. ARB/03/19.

[19] *See* Sergei Viktorovich Pugachev v. The Russian Federation. Award on Jurisdiction dated 18 June 2020, p. 60.

different cases and different BITs.[20] Since the claimant did not acquire French nationality at the time of the investment involved, the 1989 France — Russia BIT was not applicable, and the tribunal awarded that it has no jurisdiction and did not review the MFN issue.

In *RosInvest* [UK investor] *v. Russia*, the claimant, RosInvest, sought to introduce the dispute settlement provisions of the Denmark — Russia BIT with the wider scope of the arbitration consent through the MFN clause. The arbitral tribunal first pointed out that, in terms of the impact on investors, since the substantial provisions in the third-party treaty can be introduced through the MFN clause, it is more reasonable to introduce procedural provisions with less impact on the rights and interests of the parties through the MFN clause. Secondly, from the perspective of the protection of investors' rights and interests, procedural clauses like substantial clauses have protective value for investors and their investments on the same dispute matter, and are both worthy of preferential modification through MFN clauses. In addition, the Tribunal took a different view from *AsiaPhos v. China*. The Tribunal held that the fact that the dispute settlement matters were not explicitly specified in the MFN exception clause meant that the application of the MFN clause to the dispute settlement matters was legitimate.[21]

In *Berschader* [Belgian investor] *v. Russia*, in addition to the aforementioned disputes about the introduction of substantive provisions through MFN clauses, there were also disputes about the introduction of procedural provisions through MFN clauses. The respondent, the Russian Federation, does not expressly object to the application of the MFN clause to procedural benefit, pointing out that the BIT applied in this case is the Belgium — USSR BIT, and the treatment referred to in the MFN clause is the "treatment within the territory of the Soviet Union." Therefore, only clauses in BITs concluded by the Soviet Union rather than Russia and a third-party state can be introduced through MFN clauses. Therefore, the dispute settlement procedures

[20] Sergei Viktorovich Pugachev v. The Russian Federation. Award on Jurisdiction dated 18 June 2020, p. 39.

[21] *See* RosInvest Co UK Ltd. v. The Russian Federation. SCC, Case No. V079/2005. Award on Jurisdiction, pp. 75–79.

stipulated in the UK — Russia BIT, which was advocated by the claimant Bershchader, cannot be introduced into the basic treaty. Although the arbitral tribunal rejected the Russian Federation's defence of the treaty succession, it also rejected the intention of the parties to agree to introduce a dispute settlement mechanism through the MFN clause at the time of the conclusion of the treaty from the perspective of treaty interpretation. That is, the term "within the territory" indicates that the treatment referred to in the MFN clause is the treatment actually enjoyed by foreign investors in the territory of the host state, while the right to settle disputes through international arbitration tribunals is not the treatment enjoyed in the territory of the host state.[22]

III.2. Invoke MFN Treatment to Derogate Domestic Measures by the Host State

Disputes about obtaining a more favourable treatment of a host state under domestic measures through MFN provisions often revolve around "like circumstances." In *Bayindir* [Turkish investor] *v. Pakistan,* claimant Bayindir held that of the 35 construction projects contracted by the National Highway Authority of Pakistan to multiple foreign investors, only 6 were completed on schedule, but only Bayindir received a termination notice and its personnel and property were expelled from Pakistan. Bayindir received significantly lower domestic treatment than other foreign investors. Bayindir first advocated the introduction of fair and equitable treatment (FET) clauses in a third-party treaties through MFN clauses, and second, Pakistan constituted a violation of the FET clause newly imported in the BIT between Turkey and Pakistan. The arbitral tribunal recognized the applicant's claim to invoke the FET clause through the MFN clause, but further pointed out that the application of the FET clause must follow the "like circumstances" rule, and the 29 construction projects that had not been completed on schedule were delayed for different reasons, such as the change of the subject matter of the construction contract, renegotiation of the

[22] *See* Vladimir Berschader, Moise Berschader v. The Russian Federation. SCC, Arbitration V (080/2004). Award Rendered in Stockholm on 21 April 2006, pp. 56–70.

construction period, capital turnover, land ownership, etc. The claimant only proved that it had received different treatment from other foreign investors, but failed to prove that it was in similar circumstances with other foreign investors, so the claimant did not violate the introduced FET clause.[23]

In *Tashkent* [Uzbekistan investor] *v. Kyrgyzstan,*[24] the claimant Tashkent argued that Kyrgyzstan nationalized only four Uzbek-owned resorts located on the Issyk-Kul Lake (which is located in Kyrgyzstan) and did not take similar measures against other resorts owned by foreign investors near the lake. Such differential treatment in Kyrgyzstan took place when all foreign investors were in a similar situation and thus violated the provisions of the MFN.[25] The tribunal did not award on the alleged violation of the MFN, having ruled that Kyrgyzstan's measures constituted illegal expropriation.

Different from *Bayindir* and *Tashkent*, in *İçkale* [Turkish investor] *v. Turkmenistan* case, the tribunal directly rejected the claimant's claim to introduce the FET provisions through the MFN provisions and pointed out that the existence of the MFN obligations preconditions that the different investors of the contracting party and of the non-contracting party used for comparison are in similar circumstances.[26] Only under this premise, the MFN clause's function of introducing provisions in third treaty is activated. Although both arbitral tribunals reasoned around "similar circumstances," the arbitral tribunal in *Bayindir* case held that "similar circumstances" did not affect the introduction of the content of a third-party treaties. If different BITs concluded by

[23] *See* Bayindir Insaat Turizm Ticaret ve Sanayi a.ş. v. Islamic Republic of Pakistan. ICISD case, No. arb/03/29. Award dated 27 August 2009, pp. 120–123.

[24] JSC Tashkent Mechanical Plant, JSCB Asaka, JSCB Uzbek Industrial and Construction Bank, National Bank for Foreign Economic Activity of the Republic of Uzbekistan v. Kyrgyz Republic. ICSID, Case No. ARB(AF)/16/4.

[25] Art. 3.1 of the Kyrgyzstan — Uzbekistan BIT (1996): Each Contracting Party shall provide fair and equitable treatment to investments and the income of investors of the other Contracting Party on its territory, no less favorable than that it accords to investments and revenues of its own investors and/or investments and returns of investors of any third state.

[26] İçkale İnşaat Limited Şirketi v. Turkmenistan. ICSID, Case No. ARB/10/24. Award dated 8 March 2016, Para. 328.

the same state stipulate different levels of preferential treatment, then the more preferential treatment should be unconditionally extended to the other BIT. And "like circumstances" is only used as a criterion to judge whether the introduced FET clause has been violated. However, the arbitral tribunal in the *Ickale* case placed the review of "similar circumstances" before the introduction of the content of a third-party treaty, holding that the spread of the more preferential treatment to other BITs was not unconditional, and that more preferential treatment could be introduced into the basic treaty only when the provisions of different BITs would enable investors of different nationalities to obtain different levels of preferential treatment under similar circumstances.

IV. The Dilemma in the Interpretation of MFN Clause in China — SCO State BIT

Although there have been no MFN international investment disputes between China and other SCO states, the above-mentioned MFN investment disputes involving SCO states are still effective in reflecting the attitude of SCO states towards the application of MFN provisions, which may provide guidelines for the application and improvement of MFN provisions in BITs between China and other SCO states in the future. In the above cases, whether introducing procedural clauses through MFN clauses or changing the treatment under the domestic measures of the host state through MFN clauses, arbitral tribunals have made different reasoning and judgments in each similar issue, and the "inconsistent awards" problem is essentially the result of "inconsistent interpretation" (Jin, 2020, pp. 179–181). Therefore, problems in the application of MFN provisions in BITs between China and other SCO state should be predicted from the perspective of treaty interpretation, according to the above cases.

IV.1. The Difficulty to Clarify the Subjective Requirements for Importation of Procedural Clauses

In BITs between China and SCO states, it is difficult to clearly explain the scope of application of MFN clauses simply based on the

text. On the one hand, the scope of application of the MFN clause is only summarized by elements such as "territory," "investors," "investment," and "investments-associated activities," without "expressly and unambiguously" specifying procedural clauses such as a dispute settlement mechanism. On the other hand, the MFN exception clause generally does not include the dispute settlement mechanism. However, according to the *Vienna Convention on the Law of Treaties*, treaties should be interpreted in accordance with their plain wording and context and with reference to the usual meaning of the object and purpose of the treaty. When the meaning is still unclear or difficult to understand, supplementary information of interpretation should be utilized. Therefore, the MFN clauses in the BITs of China — SCO states should be interpreted from two perspectives: the text of the treaty and supplementary information.

In *AsiaPhos v. China*, when the provisions of the treaty could not expressly and unambiguously indicate that the MFN clause could be applied to the dispute settlement mechanism, the arbitral tribunal used information related to the preparation of the treaty conclusion, namely, the exchange of letters during the negotiation process. In the letters, both contracting parties agree that that the dispute settlement mechanism should be modified after additional negotiations and the consensus is reached. They further specify that the agreements made during the exchange of letters shall be part of the BIT.[27] However, not all cases have such supplementary means of interpretation. In *RosInvest*, unable to find supplementary information to help interpret the MFN provisions, the arbitral tribunal used an interpretation method, which is not generally recognized by international investment law, holding that the procedural nature of the dispute settlement mechanism makes it less important than the substantive provisions and should be deservedly introduced into the basic treaty.[28] In addition, the tribunal again retreated to the terms of the treaty after the fruitlessness of the interpretation through supplementary materials, pointing out that the

[27] *See* AsiaPhos Limited and Norwest Chemicals Pte Limited v. People's Republic of China. ICSID, Case No. ADM/21/1, Award, p. 14.

[28] *See* RosInvestCo UK Ltd. v. The Russian Federation. SCC, Case No. V079/2005. Award on Jurisdiction, pp. 77–79.

exception clause not listing the dispute settlement mechanism was sufficient to provide legitimacy for the application of the MFN clause to the dispute settlement mechanism. The arbitral tribunal in *RosInvest* case did not only use the special interpretation method, which is not generally recognized in the field of international investment dispute arbitration, but it also interpreted the treaty without making recourse to supplementary means of interpretation stipulated in the *Vienna Convention on the Law of Treaties*. Indeed, it is difficult to find out whether the arbitral tribunal subjectively seeks the most favorable interpretation mode after having reached a prior conclusion. However, "the interpretation task of arbitrators should be to make sure that the meaning of treaty terms is consistent with the motivation of the parties when they conclude the treaty, and it is to discover rather than create the meaning of treaty terms" (Mingxin, 2015, p. 176). Such interpretation method is obviously not in line with the functional positioning of international investment arbitration tribunals.

In the aforementioned cases, in order to prove the jurisdiction of the arbitral tribunal, the claimant tries to introduce the more favorable arbitration clauses in a third-party treaty through the MFN clause. However, China and Russia, as the respondent, and even the arbitral tribunal, as the adjudicator, did not explicitly deny the legality of applying the MFN clause to the dispute settlement mechanism. Rather, they showed their negative perspective through interpreting MFN clauses from specific BIT's wording and parties' contracting situations. Perhaps, as some scholar stated, the *Maffezini* case, more than two decades ago, opened the door to the application of MFN provisions to dispute settlement procedures (Garmoza, 2010, p. 14) leading the application of MFN clause on dispute settlement mechanism to an affirmative conclusion (Qiao, 2011, pp. 61–62). There is an opinion in the academic literature connecting the finality of an arbitration award to the award of *Maffezini* case and pointing out that this precedent finally affirmed the applicability of a MFN clause to dispute settlement procedure (Mrisho et al., 2023, p. 311). The debates over the application of MFN provisions on disputes settlement mechanism should be advanced to the specific conditions under which MFN provisions are able to apply to the dispute settlement mechanism in

individual cases. In addition, the relevant disputes are not an issue of "consistency of awards" but of "consistency of interpretations" (Huang, 2022, pp. 49–51). The research on the application of MFN clauses to dispute settlement procedures should focus on clarifying the specific conditions for application so as to promote the consistency in the interpretation mode of the scope of application of MFN clauses rather than the consistency in the scope of application of MFN clauses. What is also note-worthy is that the relevant documents of the thirty-sixth session of Working Group III of the United Nations Commission on International Trade Law (UNCITRAL) also pointed out that the study of "consistency of rulings" should focus on whether relevant awards are in the same scene and field.[29] To sum up, the problems in the scope of application of MFN clauses in BITs between China and SCO states are as follows: the exception clauses are relatively similar and do not clearly indicate the states' attitude towards introducing a new dispute settlement mechanism through MFN clauses, which makes it difficult to predict the interpretation conclusion of the arbitral tribunal on this issue in international investment disputes.

IV.2. The Debates over the Nature of the Treatment

Another imperfection of MFN clauses in BITs between China — SCO states is that they do not specify that the treatment stipulated in MFN clauses is "the treaty-level treatment to be" or "the factual level treatment." Taking the cases of *Bayindir v. Pakistan* and *İckale v. Turkmenistan* as examples, the BITs involved in the two cases have completely the same provisions on "treatment" and set up special articles to list in detail various investor rights that the parties hope the host state will protect.[30] Besides, both MFN clauses have incorporated

[29] UNCITRAL. Possible Reform of Investor-State Dispute Settlement (ISDS): Consistency and Related Matters, A/CN.9/WG.III/WP.150[R], 2018, New York, United Nations. Para. 10.

[30] Art. 1(2) of the Turkey — Turkmenistan BIT and Art. 1(2) of the Turkey — Pakistan BIT: (a) shares, stocks or any other form of participation in companies, (b) returns reinvested, claims to money or any other rights to legitimate performance having financial value related to an investment, (c) movable an immovable property, as well as any other rights in rem such as mortgages, liens, pledges and any other similar rights.

the wording of "like circumstances."[31] However, completely consistent and detailed terms are not enough to ensure the predictability and consistency of interpretation conclusions in international investment arbitration cases. In the two cases, the arbitral tribunals conducted the "like circumstances" review at different times, which essentially stems from the arbitral tribunal's understanding of "treatment" rather than "like circumstances." The arbitral tribunal in the *Bayindir* case unconditionally introduced the provisions in a third-party BIT into the basic BIT, and used "similar circumstances" to judge whether the introduced provisions were violated, indicating that the arbitral tribunal in this case interpreted "treatment" as the "the treaty-level treatment," which is a kind of treatment in the due state. That is, merely the treaty provision and not the exact and existing treatment foreign investors have actually enjoyed. This view has also been supported by scholars and arbitral tribunals.[32] It means a higher standard of protection for international investors and an automatic and unconditional multilateralization (Xu, 2013, p. 257). However, the arbitration tribunal in the *İckale* case first made the "similar circumstances" review and then judged whether to introduce the more favorable provisions in the third-party treaty into the basic treaty, indicating that it interpreted "treatment" as "the actual and concrete treatment," the situation in which foreign investors can have access to the legal framework of the host state. This view defined the treatment as the actual state. If in fact the situations of investors of the contracting party to the basic treaty and of the non-contracting party are not similar, or if no investors of the party to the BIT that includes more preferential treatment have made investments in the host state, there are no two qualified treatments for comparison, and the multilateralization function of the MFN clause cannot be activated.

The BIT between Turkey and Turkmenistan and the BIT between Turkey and Pakistan both stipulate "treatment" in great detail, but

[31] Art. 2(2) of the Turkey — Turkmenistan BIT and Art. 2(2) of the Turkey — Pakistan BIT: Each Party shall accord to these investments, once established, treatment no less favorable than that accorded in similar situations.

[32] MTD Equity Sdn. Bhd. and MTD Chile, S.A. v. Public of Chile. ICSID, Case No. ARB/ 01/7, Decision on Annulment, 21 March 2007, Para. 64.

still fail to guarantee the consistency of the arbitration tribunal's interpretation on "treatment." The particular reason lies in that the two detailed MFN clauses only list the objective activities associated with investments and ignore the distinction between the MFN clauses' factual status and their legal effect. That is, it is not indicated in BITs whether the so-called "treatment" is the actual state or situation that domestic investors can obtain in the host state, or the legal effect that the investment protection provisions ought to have. BITs between China and SCO states also adopt the traditional mode of listing the objective activities referred to by the treatment, without specifying whether the treatment should be interpreted as merely a provision wording stipulated therein or the actual situation of investors in the host state. Therefore, it may be difficult to clarify the reference system for a "more preferential treatment" in future international investment disputes between China and other SCO states.

V. Suggestions on Improving the MFN Clauses in the Future BIT Upgrading Negotiations

At present, the scale of China's investment in Russia and Central Asian states continues to expand, and its investment continues to increase (Wang, 2021, p. 93) In November 2021, the *14th Five-Year Plan for High-Quality Development of Foreign Trade* issued by the Ministry of Commerce of China pointed out that China should strengthen economic and trade cooperation mechanisms with Russia and Central Asian states, implement economic and trade cooperation agreements with the Eurasian Economic Union, and promote bilateral trade and investment cooperation. In 2023, the *Report on the Development of China's Overseas Investment and Cooperation 2022* released by the Ministry of Commerce indicated that China's wind power investment and solar photovoltaic investment are mainly concentrated in Central Asia at present.[33] Agricultural investment is concentrated in states and regions such as Central Asia and Russia. Russia and Central Asian states are important investment input states of China, and bilateral investment

[33] PRC Ministry of Commerce. China's Outbound Investment and Cooperation Development Report 2022, pp. 51, 61.

treaties between China and relevant states should be further upgraded to meet the needs of China's continuous expansion of investment scale in relevant states. At present, negotiations on upgrading bilateral investment treaty between China and Russia started in December 2022.[34] As the Belt and Road Initiative continues to advance, investment cooperation between China and other SCO states will be further deepened, and a new round of negotiations on upgrading BITs will also be launched. The improvement of MFN provisions in future BIT upgrade negotiations should be carried out from the following three aspects.

V.1. Improving the Wording of Treatment

First of all, when setting out the scope of "treatment," the word of "investment-related activities" should be avoided, nor should the treatment be specified by citing other investor treatment clauses. Contracting parties should try to set out the objective activities that they wish to be covered by MFN treatment. BITs concluded by China after 2010 basically follow this explicit wording mode. China — Canada BIT defines treatment through amply listing activities associated with such treatment: "establishment, purchase, expansion, management, operation and sale or other disposal of investments within its territory."[35] The China — Uzbekistan BIT[36] and the China — Tanzania BIT[37] add some more detailed activities: maintain, use and enjoy investments. Such explicit provisions have also been adopted in the *Regional Economic Comprehensive Partnership Agreement* to which China is a party and in the recent BITs between China and other SCO states.[38] This indicates that the use of the explicit wording mode to specify "treatment" has

[34] PRC Ministry of Commerce, Russia's Ministry of Economic Development. Joint Statement on Initiating Negotiations on Upgrading the Investment Agreement between the Government of the People's Republic of China and the Government of the Russian Federation Signed on 9 November 2006.

[35] Art. 5(1)(2) of the China — Canada BIT.

[36] Art. 4(1) of the China — Uzbekistan BIT.

[37] Art. 4(1) of the China — Tanzania BIT.

[38] *See* Art. 4(2) of the Hungary — Kyrgyzstan BIT, Art. 5(1) of the Myanmar — Singapore BIT, Art. 4(3) of the Saudi Arabia — Hong Kong Special Administrative Region BIT, Art. 5(2) of the Kazakhstan — Singapore BIT, Art. 4(2) of the Kyrgyzstan —

become the trend of drafting MFN clauses when SCO states conclude BITs. In addition, the difference in the meaning of the word "relevant" in different languages will also lead to inconsistent interpretation in international investment dispute arbitration. In *AsiaPhos* case, the respondent — China — believes that the Chinese version of the BIT involved in the case uses the word 有关 (youguan), and it should be a strong connection in the Chinese context. That is, it is directly generated from or directly related to something. It matches the English words "over" or "concerning," while the claimant believes that the English version of the BIT uses the word "involving," which means an abstract and extensive relationship.[39] In *Sanum v. Laos*[40] and *Heilongjiang International Economic & Technical Cooperative Corp v. Mongolia,*[41] the disputing parties also had debates over the Chinese word 有关 and its equivalents in other languages. It can be seen that 有关 in the Chinese context is not simply corresponding to "concerning," "over" and "involving" in English. Therefore, changing "activities involving investments" or similar wording to explicitly listing the investment activities that contracting parties wish to protect not only conforms to the trend of SCO states to conclude BITs, but also helps to promote the consistency of the meanings of the provisions in the Chinese and foreign languages versions of BITs, thus promoting the consistency of the interpretation.

In addition, the actual, or the concrete nature of "treatment" shall be specified in the MFN clause, making it clear that "treatment" shall be the actual situation that investors of the other party find themselves in according to the provisions of the BIT and the domestic laws and regulations of the host state. Without specifying such an "actual" nature,

Turkey BIT, Art. 5(2) of the Kazakhstan — Singapore BIT, Art. 4(2) of the Kazakhstan — United Arab Emirates BIT, Art. 4(2) of the Turkey — Uzbekistan BIT.

[39] AsiaPhos Limited and Norwest Chemicals Pte Limited v. People's Republic of China. ICSID, Case No. ADM/21/1, Dissenting Opinion, p. 5.

[40] Sanum Investments Limited v. The Government of the Lao People's Democratic Republic. Judgment of the Court of Appeal of Singapore 57, 29 September 2016, Para. 126.

[41] China Heilongjiang International Economic & Technical Cooperative Corp et al. v. Mongolia. Permanent Court of Arbitration (PCA), Case No. 2010-20, Award, 30 June 2017, Para. 439.

the MFN clause may be interpreted as being able to import more favorable provisions in a third-party treaties into the basic treaty unconditionally, thus creating unpredictable new treaty obligations for the parties and improperly breaking through the relativism of bilateral treaties. The arbitral Tribunal in *ICS v. Argentina* had pointed out that "treatment" should be the obligation of the host state to the foreign investor through its domestic legal framework in accordance with its international law obligations to be observed under international treaties or customary international law.[42] The tribunal in *Daimler v. Argentina* held that the term "treatment" originally refers to the way one party treats the other, and in the context of international investment refers to the act or omission of a host state in order to regulate, protect or otherwise interact with a particular investor and his investment.[43] In both cases, the views of the arbitral tribunals indicated that "treatment" is not a BIT stipulation as it should be, but the actual treatment accorded to foreign investors by the host state through its domestic legal framework. To make it clear, the method to reflect the "actual nature" in the MFN clause, the tribunals can refer to the China — Saudi Arabia BIT in which the wording of "subject to its laws and regulations" was adopted[44] or refer to the Turkey — Venezuela BIT to use the expression of "within the framework of its laws and regulations"[45] to indicate that the treatment referred to in the MFN clause is the actual treatment that the host state can give under its national laws and regulations.

[42] ICS Inspection and Control Services Limited (United Kingdom) v. The Argentine Republic. PCA, Award on Jurisdiction, Para. 296.

[43] Daimler Financial Services AG v. Argentine Republic. ICSID, Case No. ARB/05/1. Award, Para. 218–220.

[44] Art. 3(2) of the China — Saudi Arabia BIT: Subject to its laws and regulations, each Contracting Party shall grant investments once admitted and investment returns of the investors of the other Contracting Party a treatment not less favorable than that accorded to investment and investment returns of its investors.

[45] Art. 5(1) of the Turkey — Venezuela BIT: Each Contracting Party shall admit in its territory investments on a basis no less favorable than that accorded in like circumstances to investments of investors of any third State, within the framework of its national laws and regulations.

V.2. Incorporating the "Like Circumstances" Rule to Clarify the Prerequisite of Application

The rule of "like circumstances" is an important precondition for the application of the MFN clause, which means that the MFN clause in each treaty has its own specific application premise that the investors used for comparison are in same or similar situations (Yannick, 2007, p. 767). The advantage of the "like circumstances" rule is that it helps to prevent the blind application of MFN provisions in order to level the international investment environment. The non-discriminatory nature of the MFN clause requires that the host state shall not discriminate against nationals of the contracting state in the host state compared with nationals of other states, so as to create a level playing field among nationals of different states regardless of their nationality (Schill, 2009, p. 516). The premise of the existence of such discrimination is that the home state investor who is treated differently is in a similar situation as compared with the third state investor. It should be presumed that the host state does not take discriminatory measures against the investors of the home state and the host state does not undertake the obligation of MFN if the "like circumstances" standard has not been met.[46]

It is not a rule of customary international law to follow such a rule in the application of the MFN clause. If the MFN clause does not expressly incorporate the wording of "like circumstances," arbitral tribunals in international investment disputes do not necessarily and automatically apply this rule.[47] In order to clarify the applicable precondition of the MFN clause, the expression of "like or similar situation or circumstances" should be incorporated to the MFN clause in the future upgraded BIT between China and SCO states. It can refer to the China — Turkey BIT and the China — Uzbekistan BIT for exact wording. According to the data revealed by the UNCTAD, a total of 39 BITs have come into force since 2020, involving Turkey,

[46] İçkale İnşaat Limited Sirketi v. Turkmenistan. ICSID, Case No. ARB/10/24, Para. 328.

[47] *See* Bayindir Insaat Turizm Ticaret ve Sanayi a.ş. v. Islamic Republic of Pakistan. ICISD, Case No. ARB/03/29.

Uzbekistan, Kyrgyzstan, India, Iran, Myanmar and other SCO states.[48] Among them, only Angola — United Arab Emirates BIT and United Arab Emirates — Zimbabwe BIT do not include the "like circumstances" rule in the MFN clause. The Belarus — India BIT even goes so far as to explain that whether investors of different nationalities are in similar situations should be judged from the perspective of the situation as a whole. It also gives some illustrative and non-exhaustive examples of several factors to determine: (a) the goods or services produced or consumed by the investment; (b) the actual or potential impact of the investment on the local area or environment; (c) practical challenges of managing investments.[49] The data shows that the incorporation of "like circumstances" rules is not only a new trend of MFN clauses in the world, but also a new trend for SCO, which can provide guidance for the future negotiation of BITs between China and SCO states.

V.3. Clarifying China's Attitude towards Application on Procedural Matters

The purpose of specifying in the MFN exception clause whether the MFN clause applies to the dispute settlement mechanism in third-party treaties is to promote "consistency in interpretation methods" and "predictability of interpretation conclusions" in international investment dispute cases. If the basic treaty does not clearly indicate

[48] Japan — Bahrain BIT, Hungary — Oman BIT, Jersey — United Arab Emirates BIT, Congo — Rwanda BIT, North Macedonia — United Arab Emirates BIT, Georgia — Japan BIT, Israel — United Arab Emirates BIT, Hungary — Kyrgyzstan BIT, Zambia — United Arab Emirates BIT, Hong Kong Special Administrative Region — Mexico BIT, Cote d'Ivoire — Japan BIT, Morocco — Japan BIT, Myanmar — Singapore BIT, Belarus — Uzbekistan BIT, Hong Kong Special Administrative Region — United Arab Emirates BIT, Korea — Uzbekistan BIT, Australia — Uruguay BIT, Cape Verde — Hungary BIT, Australia — Hong Kong Special Administrative Region BIT, Japan — Jordan BIT, United Arab Emirates — Uruguay BIT, Indonesia — Singapore BIT, Belarus — India BIT, Zambia — Turkey BIT, United Arab Emirates state — Zimbabwe BIT, Singapore — Rwanda BIT, Kenya — Singapore BIT, Japan — United Arab Emirates BIT, Kyrgyzstan — Turkey BIT, Belarus — Turkey BIT, Hungary — Iran BIT, Rwanda — United Arab Emirates BIT, Turkey — Uzbekistan BIT, Costa Rica — United Arab Emirates BIT, Angola — United Arab Emirates BIT, Ethiopia — United Arab Emirates BIT, Cote d'Ivoire — Turkey BIT and China — Turkey BIT.

[49] Art. 4(1) of the Belarus — India BIT.

whether the MFN clause can be used to introduce the dispute settlement mechanism in the third treaty, the international investment dispute arbitral tribunal will often interpret it from many different and subjective aspects. The *Maffezini* case did not only introduce the dispute settlement mechanism, but also set a precedent for the interpretation of the MFN clause without mentioning the text of the MFN clause at all, bringing a trend of excessive reference to precedent in the relevant rulings on this issue. Later the *Gas Natural v. Argentina*[50] tribunal and the *Tecmed v. Argentina*[51] tribunal also similarly and directly appealed to the contracting background and had a preference for invoking prior arbitral awards without analyzing the terms of the treaty. Some of the rulings even used the scholar doctrine.[52] The aforementioned *RosInvest* case even deviated from the interpretation sequence of "terms — preparation information" stipulated in the *Vienna Convention on the Law of Treaties*.

China should expressly and unambiguously clarify in the future BITs with other SCO states that the MFN clause cannot be used to introduce the dispute settlement mechanism. On the one hand, it can directly state in the MFN exception clause that "the treatment referred to in this Article does not include the dispute settlement mechanism or procedure under any other international agreement." A more precise expression could be used, "MFN treatment referred to in this Article does not include or does not apply to dispute settlement mechanisms or procedures between investors and contracting party, as listed in article…" On the other hand, it can indicate in the preparatory documents such as a letter of exchange or protocols that "both parties agree that the dispute settlement mechanism in the treaty can only be modified after the parties renegotiation and agreement and at that time the new provisions will replace the original provisions of the treaty."

[50] *See* Gas Natural SDG, S.A. v. The Argentine Republic. ICSID, Case No. ARB/03/10, Decision of the Tribunal on Preliminary Questions on Jurisdiction.

[51] *See* Técnicas Medioambientales Tecmed v. United Mexican States. ICSID, Case No. ARB(AF)/00/2, Award dated 29 May 2003.

[52] *See* Plama Consortium Limited v. Republic of Bulgaria. ICSID, Case No. ARB/03/24, Decision on Jurisdiction; Wintershall Aktiengesellschaft v. Argentine Republic. ICSID, Case No. ARB/04/14, Award dated 8 December 2008.

Another important way is stipulating in the protocol that "the parties agree to apply the MFN provisions to specific procedural matters just as the China — Russia BIT does."[53] In addition, if upgrading negotiations cannot be initiated for the time being, the contracting parties can make clarifications by issuing a joint statement. For example, the China — Kazakhstan BIT, the China — Kyrgyzstan BIT and the China — Tajikistan BIT all stipulate that the contracting parties can meet to study the supplement to the treaty. China and the above-mentioned countries can make such a clarification by means of a joint statement before the negotiation on the upgrade of the BIT.

VI. Future Prospects: The Realistic Effect of the MFN Clause as the Link Point of Investment Treatment Multilateralization

However, the domestic investment laws of China, Russia, Pakistan, Tajikistan, Uzbekistan, Kazakhstan, and Kyrgyzstan are all oriented and aimed at attracting foreign investment, and all require foreign investment to promote sustainable development in the host state in terms of environment, human rights, labor protection, and related ideological values. However, the huge differences in political system, state system, religion and moral values among SCO states also make them adopt different standards for foreign investment access (Wang, 2019, p. 29). In addition, among the BITs between China and other SCO states, only the China — India BIT, the China — Russia BIT, and the China — Uzbekistan BIT contain national treatment clauses, and all of them are post-establishment national treatment (post-establishment national treatment means that the treatment enjoyed by foreign investors or foreign-invested enterprises after establishment is no less favorable than that enjoyed by domestic investors or enterprises in the domestic country). At present, the SCO is still facing difficulties in integrating old and new states and different expectations for economic cooperation among states.

[53] Art. 3 of the Protocol of the China — Russia BIT stipulates that the domestic administrative reconsideration procedure should be conducted on a basis of most favored nation treatment.

Multinationalization of investment protection standard and investment facilitation within the framework of SCO face many problems, especially the problem that the mechanism of investment facilitation and multilateralization in the form of multilateral investment agreement has not yet been established. In the stage of investment access, although the differences of SCO states in terms of polity, state system, religion and morality lead to different standards for investment access, the prevailing MFN clause makes it possible for foreign investors to propose the same preferential rights for access to a host state. Obviously, there are intergenerational differences in investments protection clauses in BITs between China and SCO states, but investors of parties to the older generation of BITs can enjoy a more preferential treatment accorded to investors of parties as compared with the new generation of BITs, such as the FET clause or more preferential expropriation and compensation provisions, if the standard of "similar circumstances" is met.

If the MFN clause can correctly play its role as a link of investment treatment protection multilateralization and help solve various difficulties of investment treatment multilateralization within the framework of SCO, it will have a great practical effect based on its investment potential. The SCO has become an international organization with important global influence in diplomatic, political, economic and trade, cultural and other fields. Since its establishment in 2001, the SCO has been deepening cooperation in energy, finance, economy, trade and investment. At present, under its framework regional economic ties are becoming increasingly close. Among them, investment has become an important form of regional economic cooperation, and the scale of investment cooperation among SCO countries is expanding day by day. The SCO countries are basically covered by the Belt and Road Initiative. As early as the end of 2019, China's investment in various types of SCO member states had reached 87 billion US dollars. Deepening the SCO's direct investment has become one of the priorities for strengthening regional cooperation (Wei and Sun, 2023, p. 78). The development goal of SCO requires its member states to continuously deepen economic, trade and investment cooperation.

At present, the investment law system under the framework of SCO is still largely bilateral, and the process of investment facilitation is

still fragmented. Therefore, in the practice of investment arbitration, investors of SCO state states can resort to the MFN clause in their BITs to break the dualism-based investment system, so that the *de facto* multilateralization and integrated investor protection treatment can emerge. In this way, the overseas interests of investors from one SCO state to another SCO state will be protected as much as possible.

VII. Conclusion

MFN treatment, as a multilateralization obligation given to the contracting parties under the bilateral international investment mechanism, has made the MFN clause a common link in the construction of multilateralization investment system under the framework of the bilateralism-based international investment law. At present, investment cooperation within the SCO is faced with problems such as the incomplete implementation of investment facilitation measures and the deeply rooted bilateralism. However, the current international investment arbitration cases involving SCO states show that there are problems such as the fragmentation of the interpretation method of the scope of application of the MFN clause by the arbitration tribunal, which leads to the improper expansion of the discretion of the arbitration tribunal. In this regard, China, as one of the founding states of the Shanghai Cooperation Organization, should strive to continue to improve the MFN clause through subsequent supplement, renegotiation and upgrading of the BITs, so that the MFN clause can focus on the "actual treatment," respect national sovereignty, and ensure that foreign investors in the host state can exactly enjoy the most favorable treatment under the domestic legal framework of the host state.

References

Dolzer, R. and Schreuer, C., (2012). *Principles of International Investment Law*. Oxford University Press.

Garmoza, A.P., (2010). Extending Application of Most-Favored-Nation Treatment to Dispute Resolution Clauses of Investment Treaties. *International Commercial Arbitration Review*, 2 (2), pp. 12–29.

Huang, Y., (2022). Interpretation of International Investment Arbitration Treaties: Value Trade-off and Rule Construction. *Commercial Arbitration and Mediation*, 6, pp. 49–59.

Jin, Y., (2020). Consistency of Treaty Interpretation in International Investment Dispute Settlement: Practice Conflict, Value Reflection and Reform Goal. *Global Law Review*, 5, pp. 178–192.

Mingxin, Zhu, (2015). Appearance and Essence of MFN Clause's Application on Investment Dispute Settlement Procedure: from the Perspective of Treaty Interpretation. *Law and Business Research*, 3, pp. 171–183.

Mrisho, M.I., Tran, T.K.D., Ghani, H.U. and Kipanga, K.B., (2023). Investor-State Dispute Settlement and the Application of the Rule of Law under the ICSID Convention. *US-China Law Review*, 7, pp. 297–314.

Perez-Aznar, F., (2017). The Use of Most-Favoured-Nation Clauses to Import Substantive Treaty Provisions in International Investment Agreements. *Journal of International Economic Law*, 4, pp. 777–806.

Qiao, J., (2011). Research on the Applicability of the MFN Clause in BITs in Dispute Settlement. *Journal of Rule of Law*, 1, pp. 61–69.

Schill, S.W., (2009). Multilateralizing Investment Treaties Though Most-Favored-Nation Clauses. *Berkeley Journal of International Law*, 2, pp. 492–569.

Sharmin, T., (2018). Application of MFN to the Substantive Standards: Why Should We Re-Investigate the Uncontested? *Manchester Journal of International Economic Law*, 15, pp. 85–113.

Ustor, E., (1974). Fifth Report on the Most-Favoured-Nation Clause by Mr. Endre Ustor, Special Rapporteur. New York, United Nations.

Wang, S., (2019). Legal Issues of Investment Facilitation in Shanghai Cooperation Organization. *International Business Studies*, 1, pp. 26–39.

Wang, X., (2021). The Principle of Exhaustion of Local Remedies in the ISDS Provisions of Bilateral Investment Treaties between China and Five Central Asian States. *Journal of Guangxi Social Sciences*, 11, pp. 92–100.

Wang, Y., (2020). From Procedural to Substantial: New Disputes on the Application Scope of MFN Treatment in International Investment Treaties. *Tsinghua Law Journal*, 5, pp. 182–207.

Wei, W., Sun, K., (2023). Study on the Efficiency of China's Direct Investment in Major SCO Countries. *Northeast Asia Economic Research*, 6, pp. 77–90, doi: 10.19643/j.cnki.naer.2023.06.007.

Xu, S., (2013). "Bilateralism" and "Multilateralization" of International Investment Treaty Protection. *Wuhan University Review of International Law*, 16, pp. 256–278.

Yannick, R., (2007). The Application of the Most-Favored-Nation Clause to the Dispute Settlement Provisions of Bilateral Investment Treaties: Domesticating the "Trojan Horse." *The European Journal of International Law*, 4, pp. 757–774.

Information about the Authors

Ren Yanyan, PhD, Assistant researcher, China National Institute for SCO International Exchange and Judicial Cooperation, Shanghai, China
renyanyan@shupl.edu.cn
ORCID: 0000-0003-0953-7560

Zhao Zhixin, Master of International Law of Shanghai University of Political Science and Law, Shanghai, China
asistoxin@163.com
ORCID: 0009-0001-1268-162X

STATE SOVEREIGNTY

Article

DOI: 10.17803/2713-0533.2024.3.29.569-594

The Concept and Essence of Public Law Enforcement of State Sovereignty

Sergey M. Zubarev, Denis B. Troshev

Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

Abstract: In the conditions of sharp aggravation of the international and political situation in the world and risks for the existence of the Russian Federation, the central place in the activities of public authorities is given to ensuring state sovereignty. In modern conditions it is required to create an adequate to new challenges and threats concept of public-law provision of state sovereignty of the country, based on a modern theoretical basis, including the latest achievements of public-law (state-legal) sciences. The authors consider different approaches to the definition of the essence and content of the concepts of "public-law provision" and "internal state sovereignty." The study revealed that the first of them has not yet received proper theoretical substantiation, and the second, despite the centuries-old history of study and a large number of special legal works, is characterized by numerous and often contradictory interpretations, including those in strategic planning documents. The current situation hinders the solution of one of the most complex and serious theoretical and applied tasks, on which the security of the Russian Federation and its further progressive socio-economic development largely depends. The authors substantiated the conclusion that the public law provision of internal state sovereignty of the Russian Federation should be considered in a broad and narrow sense. In a broad sense, it represents an optimal combination of lawmaking and

law enforcement based on a sufficient level of legal culture, which allows stable and sustainable functioning of public power and public administration in the country, to ensure the balance of public and private interests, rights and freedoms of citizens in the face of new challenges and threats. In a narrow sense, public law provision of internal state sovereignty is reduced only to normative legal acts of various legal force, regulating the organization and functioning of public authority, the implementation by its bodies of managerial functions and powers, interaction with civil society institutions and business, taking measures to ensure the rights, freedoms and legitimate interests of citizens and organizations in changing conditions.

Keywords: public law; legal support; public legal support; sovereignty; internal state sovereignty; new challenges and threats; public authorities

Acknowledgements: The reported study was funded by Russian Science Foundation, project number 24-18-00764

Cite as: Zubarev, S.M. and Troshev, D.B., (2024). The Concept and Essence of Public Law Enforcement of State Sovereignty. *Kutafin Law Review*, 11(3), pp. 569–594, doi: 10.17803/2713-0533.2024.3.29.569-594

Contents

I. Introduction

The events of the last two years, which have sharply aggravated the international and military-political situation, have essentially raised the question of the existence of the Russian Federation as a sovereign state. Therefore, ensuring state sovereignty in all its multidimensional content

becomes a central element of the activities of all public authorities and officials.

In modern conditions, the public legal safeguarding of State sovereignty of the Russian Federation is one of the main factors in increasing the level of protection of citizens and strengthening the security of society and the State. There are serious positive achievements in this matter, in particular, the legislation has been substantially updated and by-laws have been adopted, which made it possible to promptly minimize new challenges and threats to the state sovereignty of the country associated with a sharp increase in political, military, sanctions and information pressure on the Russian Federation after 24 February 2022. External challenges and threats, which together, in fact, constitute a hybrid war against our state, are undoubtedly aimed at destabilizing the domestic political and socio-economic situation in it, and, as a consequence, at the development of economic stagnation, financial crisis, social conflicts, the growth of crime, including terrorism and extremism. These and other negative phenomena in the medium and long term may become internal threats to the state sovereignty of the Russian Federation. In this regard, it is necessary to create a system of public law support of the state sovereignty of the country adequate to new challenges and threats, which should be built on a modern theoretical basis, including the latest achievements of public law (state legal) sciences. In this case, in the methodological aspect, it is extremely important to determine the essence and content of the two basic concepts — "public legal support" and "state sovereignty."

II. Public Law Enforcement: Concept and Essence

The first of them has not yet received proper theoretical substantiation. In most scientific works representatives of various public law sciences mention the term "public law provision," but do not give an interpretation to it (Antipova, 2022; Maslov, 2023; Komissarov et al., 2023). In other works, even devoted to the problems of public law provision of various types of activities, this concept is also not disclosed, and its content is identified with public law regulation (Ivanova, 2016; Stepanov, 2009).

At the same time, reducing public law provision to regulation not only contradicts the semantics of the word "provision,"[1] but also, and more importantly, it contradicts the semantics of the word "regulation" and it does not reflect the entire legal diversity of the content of this concept. Thus, it is advisable to analyze the basic properties of the categories of "public law" and "legal security" that constitute its essence.

In theoretical jurisprudence, the concepts of "law" and "public law" are correlated as general and private. Therefore, undoubtedly, public law has all the features inherent in law in general. At the same time, since the times of Ancient Rome, the allocation of public law as a type of law ensuring the interests of the state has become traditional for all legal systems. For the first time the definition of public law, recognized in theory as classical, was given by the Roman jurist Ulpianus and subsequently it was developed in the works of numerous scholars representing different historical periods, countries and legal doctrines. At the same time, the essence of public law remains unchanged — its focus on achieving public interests, imperative regulation, the presence of an authoritative subject, strict hierarchy and subordination of subjects of law and legal acts.

Ensuring state sovereignty of any country, and the Russian Federation is no exception, is carried out primarily through the norms and institutions of public law. To understand the essence of public law enforcement, among many important general theoretical provisions, the conclusion that "law appears in the form of (1) ideas, representations; (2) legal prescriptions (dictates or regulations) emanating from the state, and (3) actions or relations in which the ideas, principles and prescriptions of law are realized" (Goyman, 2001, p. 71) is of particular importance. And if legal ideas and perceptions are of greater importance at the stage of elaboration of conceptual approaches to the organization of public law enforcement, then legal prescriptions and actions of

[1] In explanatory dictionaries the word "provide" is usually defined as: "1) to provide sufficient material means for life; 2) to supply with what n. in the necessary quantity; 3) to make quite possible, actual, indubitable; 4) to shield, protect" (see, e.g., Ozhegov, S.I., (2019). Explanatory Dictionary of the Russian Language: ca. 100,000 words, terms and phraseological expressions. Ed. by Skvortsov, L.I. 28th ed., rev. Moscow; 2019. P. 1201. (In Russ.).

subjects of legal relations on their implementation have a direct impact on its formation and functioning.

In modern conditions, recognizing the value of doctrinal ideas about state sovereignty and legal aspects of its provision (Shumkov, 2002; Grachev, 2009; Chernyak, 2007; Khalatov, 2006), the authors of this study attach special importance to the consolidation of conceptual legal ideas and approaches to the organization of public law provision of state sovereignty of the Russian Federation in strategic planning documents. Sharing the position of scientists that documents of strategic nature represent a special kind of legal acts, which are specially created for the formation and fixation of legal policy (Mushinsky, 2015; Gvozdeva, 2020; Chepurnova and Ishchenko, 2022), we substantiate the opinion on attributing such documents to strategic management acts (Zubarev, 2024). Such acts, as a rule, contain norms-ideas, norms-goals, norms-objectives, norms-principles, being the basis for the adoption of other normative legal acts.

The most important of the strategic management acts — the National Security Strategy of the Russian Federation, approved by the Decree of the President of the Russian Federation No. 400 dated 2 July 2021,[2] directly refers to the protection of the constitutional order, sovereignty, independence, state and territorial integrity of the Russian Federation to the national interests at the present stage (p. 2, 25). Ensuring state sovereignty in its various manifestations (including economic, financial, cultural, informational) is one of the goals of each of the established strategic national priorities. There is no doubt that it is the branches of public law that are called upon to become the basis for comprehensive activities to achieve them.

Recognizing the role and importance of legal prescriptions of international law in ensuring Russia's external sovereignty, and the norms of criminal law and criminal procedure law in protecting state sovereignty from external and internal encroachments, the authors of this study focus their attention on the state and legal branches of public law (constitutional, administrative, financial), the norms of

[2] *See* Decree of the President of the Russian Federation No. 400 dated 2 July 2021 "On the National Security Strategy of the Russian Federation." Collection of Legislation of the Russian Federation. 2021. No. 27 (Part II). Art. 5351. (In Russ.).

which are primarily designed to ensure the stability of the functioning of institutions of state power, political peace and social cohesion within the country, its progressive social and economic development and the well-being of its citizens, the priority of their rights and freedoms.

The norms of constitutional law define the basic principles and characteristics of state sovereignty of Russia, the foundations of its political and state legal system, establish the legal status of man, their basic inalienable rights, freedoms and duties, thereby securing the interests of society, the state and the individual.

Administrative legal norms, developing constitutional provisions, specify the organization and functioning of the executive power as the main actor in ensuring the internal state sovereignty of the Russian Federation, determine the directions and content of the managerial activity of these bodies of the state to achieve this public interest, maintain its consensus with the interests of citizens and their associations, as well as the development of mechanisms of interaction between the executive bodies of public power and institutions of civil society.

The norms of financial law form the basis for the activities of the state, commercial and non-commercial organizations to ensure the financial sovereignty of Russia, primarily the stability of the financial system, the stability of the national currency, the availability of financial resources for citizens and businesses, the financial security of all participants in economic relations.

The prescriptions of information law make it possible to ensure the information sovereignty of the country, in particular, independence in the development and use of information technologies, means and objects of informatization, information and communication systems, guaranteeing information security, etc. The prescriptions of information law make it possible to ensure the information sovereignty of the country.

Therefore, it is obvious that the basis of public law provision of internal sovereignty of the Russian Federation consists of legal means of state legal branches of public law.

In this case, it is also appropriate to talk about legal means as tools for achieving the legal goal — the satisfaction of public interest, which is the internal state sovereignty of the country. Thus, to answer the questions about the essence and content of its public law provision will

largely help the instrumental theory of law, the foundations of which were laid by the outstanding Russian jurist S.S. Alekseev (Alekseev, 1966). The quintessence of this theory is the idea that one of the essential properties of law as a whole and its individual elements is their ability to be a means of achieving certain goals (Alekseev, 1987; Sapun, 2002; Shundikov, 2009). The instrumental approach, in our opinion, allows us to identify all the variety of legal means that form and contribute to the realization of the whole legal provision and its central, public law, segment.

One of the authors of this article back in 1999 in his PhD thesis put forward a hypothesis that the concept of "legal security" should be considered in a broad and narrow sense. In a broad sense, this term covers the whole process of development of means of legal regulation and their use in the practical activity of subjects of law to achieve actual results in a particular sphere of social relations. In a more specific (narrow) sense, legal support is a set of legislative and other normative legal acts regulating this sphere (Zubarev, 1999, pp. 124–1 26).

In subsequent years, the above hypothesis was directly or indirectly confirmed by the research results of other scientists. V.A. Kozbanenko with regard to the state civil service legal support in a broad sense considers legal support as "an integral system of interrelations and relations, combining the interaction of socio-legal elements and legally significant measures affecting the formation and implementation of state service legal relations. In a more specific (narrow) sense it appears as a system of legislative and other legal acts regulating the organization and activities of civil servants in the sphere of implementation and administrative-legal status; it coincides with the concept of its legal regulation" (Kozbanenko, 2003, p. 12). Here, there is an objection to the inclusion in the broad understanding of legal support in addition to legal measures of social and legal elements, which seems unnecessary, because social phenomena and factors in the formation and implementation of legal relations act as their prerequisites, legal facts that do not have a legal nature.

Following a similar approach, A.N. Arzamaskin distinguishes in the concept of legal support the system of legal and other means. According to the author "the system of legal means, in fact, represents

legal regulation by means of special legal means (rule-making, legal implementation, law enforcement, means of individual legal regulation, and measures of coercive and encouraging nature). The group of other means consists of a number of security measures: material and technical, organizational and managerial, personnel, ideological nature" (Arzamaskin, 2016, p. 50). In this case, the author, on the one hand, allows excessive fragmentation of legal means (one of the forms of the implementation of law is law enforcement, which, accordingly, includes means of individual legal regulation and measures of coercion and encouragement), on the other hand, supplements legal support with non-legal measures, which contradicts the very essence of this legal phenomenon.

In recent years, theoretical and applied problems of legal security have been successfully developed by M.P. Imekova. It is necessary to agree with many conclusions of the scientist, made on the basis of the instrumental theory of law. First of all, with such a conclusion that "it seems unreasonable to reduce legal support exclusively to legal regulation (including the system of norms enshrined in legal acts and designed to regulate the activities of any subjects) or legal activity. These phenomena relate to different planes of legal reality. Legal support unites these phenomena, thus creating conditions for achieving its specific purpose of provision" (Imekova, 2023a, p. 213). At the same time, it is correct to note the presence of "the subjective side of legal reality (legal consciousness, legal education, legal education, legal culture, legal psychology, legal understanding), which the author calls other means of legal influence, creating an ideological basis for legal support" (Imekova, 2023a, p. 215). At the same time, it is debatable whether the scientist includes in legal support in addition to legal means as a separate component of "legal relations on their implementation." It seems that the legal relation, the content of which is formed by mutual rights and obligations of the relevant subjects, is itself a legal means.

To achieve the goals of our research, another work by M.P. Imekova is of undoubted interest (Imekova, 2023b), in which a distinction is made between private-law and public-law security. Based on the instrumental approach, the scientist proposes to divide legal security depending on the purpose (the type of interest satisfied — public or

private) into two types: public-law and private-law security (Imekova, 2023b, p. 148). The purpose of public-law security, in the author's fair opinion, is the satisfaction of public interests, i.e., having a high degree of social significance. The need to satisfy them is inevitably reflected in the means of public law enforcement, the activity mediated by them, the type of legal regulation (Imekova, 2023b, p. 153). M.P. Imekova singles out the following features of public law enforcement, which sufficiently disclose its legal nature, and therefore it is advisable to set them out in detail. Firstly, legal means directly come from public entities. Public entities centrally determine the types and combination of such legal means. Moreover, public legal entities enshrine in such means models of behavior that cannot be changed by subjects of law. The main legal means used in public law enforcement are normative legal means such as peremptory norms of law, as well as enforcement acts. Secondly, the public-law entity and the authorities authorized by it are obligatory participants of legal relations on the implementation of legal means. They act in such relations as carriers of public power. In this regard, legal relations on the implementation of legal means within the framework of public-law support are relations of power and subordination (subordination). Thirdly, public legal support mediates such types of activities as law making and law enforcement. Fourthly, the analysis of legal means and legal relations on their implementation within the framework of public law enforcement allows us to conclude that such enforcement is characterized by permissive type of legal regulation (Imekova, 2023b, pp. 153–154).

In general, supporting the author's position, there is a need to pay attention to some controversial provisions. Earlier, within the framework of consideration of the concept of legal support, we have already expressed our negative opinion on the separation of legal relations from legal means. In addition, we cannot agree with the researcher's statement that public legal support mediates such activities as law making and law enforcement. In our opinion, it is law making and law enforcement that constitute the essence of this type of security, since only authorized public authorities and certain organizations, to which state powers have been delegated, can carry out these types of activities to achieve public interest.

Finally, the main objection. When describing the concept of legal support, M.P. Imekova quite justifiably included in its content other means of legal influence (legal consciousness, legal education, legal education, legal culture, etc.), but, unfortunately, she did not do it in relation to public-law support. In our opinion, it is impossible to achieve the goal of public law enforcement without a proper level of legal culture and legal consciousness of both state and municipal employees and individual citizens, as well as the population as a whole. Professional legal culture and legal consciousness are necessary for representatives of the apparatus of public administration in the implementation of rule-making, adoption of individual acts within the framework of resolving specific life situations, and the performance of other legally significant actions. It is undeniable that the higher the level of legal professionalism of state and municipal employees, the higher the quality of lawmaking and law enforcement activities, the more realistic is the achievement of a specific public interest as a goal of public law enforcement. Thus, there is a positive legal impact both on individual citizens and on a significant part of people who consciously, by virtue of inner conviction, support the legal decisions of public authorities, bring their behavior in line with the purpose and will expressed in legal acts.

The low level of legal culture and legal consciousness of the managerial staff of public authorities not only negatively affects the level of law and order in the system of public administration, but also provokes the development of legal nihilism in society. In this case, even the perfect legal acts will not be implemented in practice, which makes public interests unattainable.

Thus, it is proposed to understand the process of developing means of legal regulation and their application in the practical activities of subjects of public administration to achieve certain socially significant (public) interests as public legal support.

III. The Concept and Essence of Internal State Sovereignty of the Russian Federation

Problems related to the definition of the concept and essence of state sovereignty, with varying degrees of intensity have been

worrying scientific circles for many centuries, and to this day remain largely unresolved and controversial. Of course, there is no shortage of legal research on this issue, it was noted more than twenty years ago (Marchenko, 2003, p. 186). Since that time, the fund of such studies has been significantly enriched and today there are numerous definitions of various types of state sovereignty and its variations (Troshev, 2024, p. 12). At the same time, a single definition of state sovereignty, which would suit both scientists and practitioners (both legislators and law enforcers), has not been formulated.

At the present stage of development of social and political thought, such types of sovereignty as state, national, and people's sovereignty are clearly manifested. The essence of these categories, their content, characteristics and features receive different interpretations depending on the affiliation of the researcher to one or another school of socio-political thought (e.g., neoliberalism, neorealism), up to the loss of meaning in the concept of sovereignty. This is due to the fact that in the era of globalization its bearer — the state — is dying out and delegates its powers to supranational entities, or vice versa — towards the ideas of maximum sovereignty of states in the light of the spread of the concepts of deglobalization (Ivanov, 2010). We believe that the growing confrontation between different states is largely due to the difference in the understanding of state sovereignty and the possibility of encroaching on it. As Charles E. Ziegler quite rightly notes, it is interpreted differently in different countries, and if, for example, in Russia and China the ideal is full and inviolable sovereignty for all countries, in the United States the model is full sovereignty for the United States and partial sovereignty for other countries (Ziegler, 2012, p. 12).

New challenges and threats have moved the scientific debate about the content of the concept under study from the theoretical to the practical plane. Today, more than ever, there is a need to develop new approaches to the definition of the concept and essence of state sovereignty. This is one of the most complex and serious theoretical and applied problems, the solution of which largely determines the security

of the Russian Federation and its further progressive socio-economic development.

So, about the concept of state sovereignty. First, let us limit the subject of the study. The fact is that the already mentioned concepts of state sovereignty are by no means exhaustive. Within the framework of this article, its gradation into internal and external is of scientific interest. C. Krasner distinguishes internal sovereignty and sovereignty of interdependence (or external) (Krasner, 1999, pp. 3–4). The first one concerns the way of organizing power in the state, effective management of its territories. The second one leads to the plane of international legal relations. In the framework of this study, the emphasis will be placed specifically on internal state sovereignty, due to the fact that in legal science there is still an insufficient level of theoretical research of legal instruments to ensure not so much external (international) as internal state sovereignty, the lack of an interdisciplinary approach to the study of both public-law provision of internal state sovereignty as a whole and its individual elements, as well as their transformation under the influence of new challenges and challenges.

Analyzing scientific works (Smorchkova, 2024; Inalkaeva, 2024), legal acts of management of public authorities of the Russian Federation, including acts of strategic planning, we see that the term "sovereignty" in terms of its internal aspects is actively integrated into many of them, primarily in the context of measures to ensure it, for example, stimulating economic development, innovation, reducing measures of foreign influence, the development of information technology. But, unfortunately, these measures are not followed by a comprehensive understanding of the concept and essence of Russia's internal state sovereignty. To fill this gap, let us answer a few questions.

Firstly, what is sovereignty as a legal category? Despite the clearly increasing tendencies of widespread use of the concept of "state sovereignty of Russia," scientific literature and normative legal and law enforcement acts show a wide range of terminology used to describe it. In various sources, state sovereignty appears as a feature, quality, property, characteristic of the state, an element of its legal status, etc. The state sovereignty of Russia is used as a sign, quality, property, characteristic of the state, an element of its legal status.

For example, according to the decision of the Constitutional Court of the Russian Federation,[3] sovereignty is interpreted as a qualitative feature of the state.

In the Declaration of the Congress of People's Deputies of the RSFSR No. 22-1 dated 12 June 1990[4] the sovereignty of the RSFSR was defined as a natural and necessary condition for the existence of statehood of Russia. In the Declaration on the observance of sovereignty, territorial integrity and inviolability of borders of the member states of the Commonwealth of Independent States,[5] sovereignty is named as a principle, along with the principles of territorial integrity and inviolability of state borders. Subparagraph 2, Para. 7 of the Strategy of Economic Security of the Russian Federation for the period until 2030, approved by the Decree of the President of the Russian Federation No. 208 dated 13 May 2017,[6] defines economic sovereignty of the Russian Federation as objectively existing independence of the state in the conduct of domestic and foreign economic policy, taking into account international obligations.

Subparagraph "i" Para. 4 of the Strategy for Scientific and Technological Development of the Russian Federation, approved by Presidential Decree No. 145 dated 28 February 2024, refers to sovereignty as "the ability of the state to create and apply knowledge-intensive technologies."[7]

[3] *See* Resolution of the Constitutional Court of the Russian Federation No. 10-P dated 7 June 2000 "On the case of verifying the constitutionality of certain provisions of the Constitution of the Republic of Altai and the Federal Law 'On General Principles of Organization of Legislative (Representative) and Executive Bodies of State Power of the Subjects of the Russian Federation'." Collection of Legislation of the Russian Federation. 2000. No. 25. Art. 2728. (In Russ.).

[4] *See* Declaration of the Congress of People's Deputies of the RSFSR No. 22-1 dated 12 June 1990 "On State Sovereignty of the Russian Soviet Federative Socialist Republic." Vedomosti SND and VS RSFSR. 1990, No. 2. Art. 22. (In Russ.).

[5] *See* Declaration on the observance of sovereignty, territorial integrity and inviolability of borders of the member states of the Commonwealth of Independent States (adopted in Moscow on 15 April 1994). SPS "ConsultantPlus". (In Russ.).

[6] *See* Decree of the President of the Russian Federation No. 208 dated 13 June 2017 "On the Strategy of Economic Security of the Russian Federation for the period up to 2030." Collection of Legislation of the Russian Federation. 2017. No. 20. Art. 2902. (In Russ.).

[7] *See* Decree of the President of the Russian Federation No. 145 dated 28 February 2024 "On the Strategy of Scientific and Technological Development of the Russian Federation." Collection of Legislation of the Russian Federation. 2024. No. 10. Art. 1373. (In Russ.).

We do not find other examples of normative interpretation of the concept of state sovereignty. Even in the materials of the profile Commission of the Federation Council of the Federal Assembly of the Russian Federation on the protection of state sovereignty and prevention of interference in the internal affairs of the Russian Federation does not argue the need for a legislative definition of this term. At the same time it is proposed to enshrine in law the definition of "external interference in the internal affairs of the Russian Federation" to create a system of legislative measures to protect state sovereignty.[8]

In the scientific legal literature on this issue, there is an even wider range of judgements. Thus, sovereignty is referred to as "fundamental state science category," at the same time pointing to it as a constitutionally protected value, principle and means of protection of the legal system (Taribo, 2024). They write about state sovereignty as a form of manifestation of popular sovereignty (Krasinski, 2017). They propose to consider state sovereignty as a legal property (feature) of the state (Efremov, 2020, p. 15). There is an interpretation of state sovereignty as "a special legal nature of state power, due to which it is supreme and independent" (Leonov, 2013, p. 132). Another point of view is that state sovereignty of a modern state, first of all, should be considered as a legal status of a specific social community formed on a certain territory and being a part of the world community. It represents one of the means that allow the state to achieve its goals (Melekhin, 2009). There is also such an interpretation — "the sovereignty of the state is its property characterizing the independence and autonomy of the state from the influence of other states in the exercise of its internal and external functions" (Duisenov, 2023).

Many authors avoid identification of sovereignty altogether, moving in their works to the disclosure of its characteristics, properties, signs and features. Thus, Y.A. Tikhomirov notes that nowadays sovereignty, as before, is understood as the independence and autonomy of state power inside and outside the country (Tikhomirov, 2013). However, in our opinion, it is still necessary to identify state sovereignty as a quite specific legal category, namely, to propose its interpretation as a feature

[8] Available at: http://council.gov.ru/structure/commissions/iccf_def/plans/88007/ [Accessed 17.06.2024]. (In Russ.).

of the state, characterizing its legal status regardless of the type of legal relations in which the state participates, whether they are legal relations of internal or external (international legal) nature.

Secondly, who is the bearer of internal sovereignty — the bodies of state power, the state itself, the people? Etymologically, "bearer" is "one who is endowed with something, can serve as an exponent, representative of something"[9]. The Constitution of the Russian Federation unambiguously determines that the bearer of sovereignty and the only source of power in the Russian Federation is its multinational people (Part 1 Art. 3). The President of the Russian Federation has repeatedly drawn attention to this fact, thus, addressing the Federal Assembly of the Russian Federation, he emphasized that "it is the people of Russia who are the basis of the country's sovereignty, the source of power."[10]

Theories according to which it is the people (or nation) that is the bearer of sovereignty are the most widespread. Further adherence to this theory leads to the understanding that it is the people in a democratic state that possesses, both actually and legally, the entirety of state power. In general, such views have their roots in the epochs of thinkers (G. Grotius, J.J. Rousseau) who recognized the people as the bearer of sovereignty. Today we find similar provisions in many constitutions of the countries of the world.

The practical embodiment of sovereignty, the bearer of which is the people, is carried out through democratic procedures associated with the formation of government bodies, which the people represent and act in their interests, or through the direct expression of the will of the people. State sovereignty embodies the idea of popular sovereignty through a set of specific legal principles underlying the sovereignty of the state and is formally enshrined in the system, structure and competence of public authorities authorized to represent the people. As Y.A. Tikhomirov rightly writes, sovereignty expresses the public nature of public power,

[9] Ozhegov, S.I., Shvedova, N.Y., (1992). Explanatory Dictionary of the Russian Language. Moscow. Available at: http://ozhegov.info/slovar [Accessed 03.07.2024]. (In Russ.).

[10] *See* Address of the President of the Russian Federation to the Federal Assembly of the Russian Federation dated 21 February 2023. Available at: http://kremlin.ru/events/president/news/70565 [Accessed 15.06.2024]. (In Russ.).

within the country the people, the nation, is the source of power, and the state is the main link of the political system, performing functions in the interests of society. Thus, the people's sovereignty finds its expression in the sovereignty of the state (Tikhomirov, 2013).

Thirdly, to what extent is it appropriate and correct from the legal point of view to divide sovereignty into internal and external? The treatment of sovereignty from internal and external aspects has long been familiar. Some authors believe that such a division is artificial (Krasinski, 2017), considering that the state cannot be sovereign only in internal or external affairs. Agreeing with the opinion about the unity of state sovereignty, nevertheless, it should be stated that this approach is by no means an obstacle to the separation and independent study of various aspects of sovereignty — internal and external, as well as further detailed study of individual elements of internal state sovereignty.

The term similar to "internal sovereignty" is reflected in various normative legal acts. Thus, the Concept of Foreign Policy of the Russian Federation, approved by Presidential Decree No. 229 dated 31 March 2023,[11] speaks of sovereignty in domestic policy. At the same time, official documents still much more often use the wording "interference in the internal affairs of Russia," including in the same act and in many others.[12] We believe that this wording is a description of one of the manifestations of encroachment on the internal sovereignty of the state. In addition, the acts enshrine provisions concerning cultural and economic sovereignty (National Security Strategy of the Russian Federation), technological sovereignty (Strategy for Scientific and Technological Development of the Russian Federation), financial sovereignty (Strategy for the Development of the Financial Market of the Russian Federation until 2030[13]), and information sovereignty

[11] *See* Decree of the President of the Russian Federation No. 229 dated 31 March 2023 "On Approval of the Concept of Foreign Policy of the Russian Federation." Collection of Legislation of the Russian Federation. 2023. No. 14. Art. 2406. (In Russ.).

[12] *See*, for example: National Security Strategy of the Russian Federation. (In Russ.).

[13] *See* Order of the Government of the Russian Federation No. 4355-r dated 29 December 2022 "On Establishing of the Strategy for the Development of the Financial Market of the Russian Federation until 2030." Collection of Legislation of the Russian Federation. 2023. No. 1 (Part III). Art. 476. (In Russ.).

(Concept for the Development of the Securities Market in the Russian Federation).[14]

Therefore, it becomes obvious that the public-law provision of state sovereignty is a multilevel task, affecting various spheres and directions and found legislative reflection in many normative legal acts in the field of defense, security, economy, finance, energy, food and many others.

The interest of researchers in various manifestations of sovereignty is also increasing proportionally. In the scientific literature of recent years, we meet works devoted to economic, tax, information sovereignty (Boldyrev, 2023; Romanovsky and Romanovskaya, 2022; Baranova and Shmagun, 2022; Krasyukov, 2023; Zharova, 2021). At the same time, we believe that each of these manifestations of sovereignty, in turn, can be studied in terms of internal and external aspects.

Fourth, what are the main properties, key characteristics of internal state sovereignty? According to the classical concept, state sovereignty without its division into internal and external aspects is characterized by unity and inalienability, supremacy, independence and autonomy of state power.

The Constitutional Court of the Russian Federation in its ruling No. 10-P dated 7 June 2000 pointed out such characteristics of state sovereignty as "supremacy, independence and autonomy of state power, completeness of legislative, executive and judicial power of the state on its territory and independence in international communication."

The Recommended Glossary of Terms and Definitions of the CSTO Member States in the sphere of ensuring national and international security defines the following attributes of sovereignty: supremacy of the state power, its unity, autonomy and independence in external and internal affairs.[15]

[14] *See* Decree of the President of the Russian Federation No. 1008 dated 1 July 1996 "On Establishing of the Concept of Securities Market Development in the Russian Federation." Collection of Legislation of the Russian Federation. 1996. No. 28. Art. 3356. (In Russ.).

[15] *See* Recommended Glossary of Terms and Definitions of the CSTO Member States in the Sphere of National and International Security (adopted on 19 December 2023 by Resolution 16-6.3 of the Parliamentary Assembly of the Collective Security Treaty Organisation).

The scientific literature has noted the authors' desire to identify other properties that determine the internal sovereignty of the modern state, for example, such as self-sufficiency, resistance to the influence of external factors and state control over internal assets (Filin, 2023). At the same time, these attributes, in our opinion, only fragmentarily illustrate the content of state sovereignty in a particular sphere or branch of state-administrative activity, and do not have a universal, conceptual and generalizing significance.

The use of synergetic approach in the study of normative legal acts and numerous scientific sources on this issue allowed us to identify the following as the basic signs of internal state sovereignty.

1. Supremacy and completeness of state power within the state. This property finds its expression in the extension of state power to all citizens and organizations within the territorial borders of Russia, the binding nature of all its decisions for the participants of legal relations, the creation of an independent system of national law and the supremacy throughout the country of the Constitution of the Russian Federation, laws and other normative legal acts, the provision of state management decisions with legal guarantees and measures of state coercion. But the true supremacy and completeness of state power is possible only with legitimate, stable and sustainable functioning of state administration, democratic procedures for the formation of public authorities, continuous improvement of the forms of popular will and public control, correcting, if necessary and within the limits established by law, the activities of public authorities.

Speaking about the supremacy and completeness of state power as a characteristic of state sovereignty, we mean state authorities of both federal and regional levels, the competence of which is built in accordance with the Constitution of the Russian Federation and normative legal acts adopted in development of its provisions. For example, the constitutional norm (Art. 73) enshrines the entirety of state power of the subjects of the Russian Federation outside the jurisdiction of the Russian Federation and the powers of the Russian Federation on subjects of joint jurisdiction of the Russian Federation and the subjects of the Russian Federation. At the same time, the norm

does not mean that state sovereignty in this case is transferred from the Russian Federation to its subjects.

At the same time, it should be noted that the legal component of ensuring the supremacy and completeness of state power in the territory of the country in the conditions of new challenges and threats acquires additional complexities that require the development of new approaches to the formation and implementation of public-law support of its functioning.

2. Inalienability of state sovereignty. In the scientific literature there are opinions that in the conditions of globalization and integration a number of states, for example, from among the European Union, partially alienate sovereignty in favor of a supranational corporation (Filin, 2023). At the same time, given that the bearer of sovereignty is the people of the Russian Federation, even by joining supranational associations of various orientation and nature, Russia's internal sovereignty is not alienated. Moreover, the Constitutional Court of the Russian Federation in its ruling No. 10-P dated 7 June 2000 stressed that the Constitution of the Russian Federation does not allow any other bearer of sovereignty and source of power than the multinational people of Russia, and, therefore, does not presuppose any other state sovereignty than the sovereignty of the Russian Federation. The sovereignty of the Russian Federation, by virtue of the Constitution of the Russian Federation, excludes the existence of two levels of sovereign powers within a single system of State power, which would have supremacy and independence, i.e., it does not allow for the sovereignty of either republics or other subjects of the Russian Federation. This means the inadmissibility of alienation of sovereignty within Russia. In the recent past, our country has experienced both the "parade of sovereignties" and two Chechen wars, which posed a real threat to the unified sovereignty and territorial integrity of the state. And today, internal State sovereignty is impossible without actively countering any manifestations of separatism, nationalism and chauvinism.

3. The autonomy and independence of state power in managing the affairs of society implies that the fulfilment of the tasks and functions of the state is carried out by it exclusively freely within the legal framework without any pressure, interference, primarily from destructive political

forces, big business, criminals, etc. Our state had a bitter lesson of the 1990s, when the highest echelons of power were negatively influenced by the "semibankirshchina" and the activities of local authorities were often actually paralyzed. Our state had a bitter lesson of the 1990s, when the highest echelons of power were under the negative influence of the "semibankirshchina," and the activities of local authorities were often actually paralyzed by criminals.

In the conditions of the existing market economy and global economic ties the possibility of genuine autonomy and independence of state power is put under serious doubts, but the results of the state policy pursued by Russia demonstrate the opposite, and today the legal basis for ensuring the autonomy and independence of state power is laid virtually in all areas of state management activity. At the same time, the autonomy and independence of state power does not mean the absence of public control over its implementation. Public control of civil society institutions and individual citizens in modern conditions should acquire a new sound, not in words, but in practice to ensure the effectiveness of the activities of government bodies and their officials.

4. Guaranteed rights and freedoms of citizens, balance of public and private interests. Civilized mankind, in fact, throughout its history has been trying to establish an optimal balance between the interests of the population and the state. Undoubtedly, this thesis is fully relevant for the internal state sovereignty. After all, the latter is not a value in itself, but only a condition for the realization of freedom and autonomy of the will of the people. At the same time, a strong state power can significantly limit the freedom of the population, in this regard, any state and society faces a difficult choice between sovereignty and freedom, security and human rights.

At first glance, it may seem that the concept of "state sovereignty" does not "coexist" with ensuring human rights. The state in the person of public authorities, being the creator of normative legal acts and realizing their execution, is not bound by these acts itself and can act beyond their boundaries, thus the power of the state is unlimited, absolute. However, the modern public-law reality demonstrates the opposite. The rights and freedoms of man and citizen according to Art. 18 of the Constitution of the Russian Federation determine the meaning, content

and application of laws, the activities of legislative and executive power, local self-government and are ensured by justice. This constitutional provision is a norm of direct effect regardless of the current situation.

In the context of the new challenges and threats facing the Russian Federation, the internal limits of State sovereignty are inextricably linked to the rights and freedoms of man and citizen. In the current crisis, arbitrary restriction by the State of fundamental human and civil rights and freedoms poses a threat to State sovereignty and is therefore inadmissible.

In this regard, internal state sovereignty consists in the guarantee of freedom, independence, autonomy of the will of the bearer of sovereignty — the people, the balance of public and private interests within the state, the rights and freedoms of man and citizen.

Thus, the internal state sovereignty of the Russian Federation as a legal category is an inalienable feature of the state that determines its legal status as a party to legal relations formed in connection with the internal affairs of the state. Internal state sovereignty is characterized by inalienability, supremacy and completeness of state power, its independence and autonomy, guaranteed rights and freedoms of citizens, balance of public and private interests.

IV. Conclusion

With regard to our study, it is proposed to understand under the public-law provision of internal state sovereignty of the Russian Federation a set of public-law means, tools, methods of protection, maintenance, guaranteeing the legitimacy and supremacy of state power, stability of the balance of public and private interests, observance of rights, freedoms and legitimate interests of citizens and organizations.

The most important elements here are, firstly, law-making, i.e., direct activity of public authorities authorized to do so to develop, adopt, amend and repeal legal norms. Consequently, legal norms most fully express public interests and those regularities within the framework of which they will operate. The creation and improvement of a unified, internally consistent and consistent system of legal norms should meet the needs of ensuring internal state sovereignty in the face of new

challenges and threats. Secondly, law enforcement as a complex power activity to implement and protect legal norms that ensure the stability of state sovereignty of the Russian Federation in the conditions of new challenges and threats. This form of implementation of law dominates in the sphere of ensuring state sovereignty, where there is a particular need for precise definition of the rights and obligations of the parties, state control over the development of relations, introduction of elements of stability, stability and certainty into this development. Thirdly, the legal culture of subjects of law, which allows officials, state and municipal employees to maintain a high level of quality of legal decisions in the sphere of ensuring state sovereignty, and in relation to the personality of each citizen, means a combination of knowledge and understanding of the law with the conscious execution of its prescriptions.

Therefore, legal culture and legal consciousness are an organic part of public law enforcement, which is based on legal education as a purposeful activity to form legal attitudes that allow to adequately perceive, consciously apply, observe and (or) fulfil legal norms. In modern crisis conditions, all public authorities and their officials should take various measures to strengthen legal education and enlightenment of the apparatus of public administration and the entire population to form a high legal culture, legal attitudes and value-legal orientations, allowing to resist various destructive manifestations, adequately perceiving and evaluating legal information, processes, phenomena and acting in relation to them in accordance with this assessment. Individual and collective attitudes and value orientations based on law should be implemented in conscious lawful behavior.

Thus, the public-law provision of internal state sovereignty of the Russian Federation should be considered in two aspects. In a broad sense, it represents an optimal combination of lawmaking and law enforcement based on a sufficient level of legal culture, which allows stable and sustainable functioning of public power and public administration in the country, to ensure the balance of public and private interests, rights and freedoms of citizens in the face of new challenges and threats.

In a narrow sense, the public-law support of internal state sovereignty is reduced only to normative legal acts of various legal

force, regulating the organization and functioning of public authority, the implementation of managerial functions and powers by its bodies, interaction with civil society institutions and business, taking measures to ensure the rights, freedoms and legitimate interests of citizens and organizations in changing conditions.

References

Alekseev, S.S., (1966). *Mechanism of Legal Regulation in the Socialist State*. Moscow: Yuridicheskaya Literatura. (In Russ.).

Alekseev, S.S., (1987). Legal means: statement of the problem, concept, classification. *Soviet State and Law*, 6, pp. 12–19. (In Russ.).

Antipova, D.D., (2022). To the Question of the Concept of "Competence" in Budgetary Law. *Finance Law*, 11, pp. 37–41, doi: 10.18572/1813-1220-2022-11-37-41. (In Russ.).

Arzamaskin, A.N., (2016). Definition of the Concept of "Legal Support:" Statement of the Problem. *Nauka i shkola*, 6, pp. 47–51. (In Russ.).

Baranova, A.F. and Shmagun, E.S., (2022). Digital Sovereignty of the EAEU in the context of Ensuring Economic Security. *State Power and Local Self-Government*, 7, pp. 29–34, doi: 10.18572/1813-1247-2022-7-29-34. (In Russ.).

Boldyrev, O.Y., (2023). Economic Sovereignty of the State and Strategic Management: Constitutional and Economic Aspects. *State Power and Local Self-Government*, 12, pp. 34–38. (In Russ.).

Chepurnova, N.M. and Ishchenko, A.A., (2022). Some Aspects of Improving Administrative and Legal Regulation of Strategic Planning in the context of Constitutional Reform in the Russian Federation. *Administrative Law and Process,* 1, pp. 22–27, doi: 10.18572/2071-1166-2022-1-22-27. (In Russ.).

Chernyak, L.Y., (2007). General Theoretical Problems of State Sovereignty. Cand. Diss. (Law). Chelyabinsk. (In Russ.).

Duisenov, E.E., (2023). Some Theoretical Issues of Integration of Constitutional Legislation in the EAEU Countries. *Journal of Russian Law*, 4, pp. 107–121, doi: 10.12737/jrp.2023.045. (In Russ.).

Efremov, A.A., (2020). *Information and Legal Mechanism of Ensuring State Sovereignty of the Russian Federation*. Dr. Diss. (Law). Moscow. (In Russ.).

Filin, A.Y., (2023). The Problem of State Sovereignty in the context of World System Analysis. *Aktual'nye problemy rossijskogo prava*, 12, pp. 41–51, doi: 10.17803/1994-1471.2023.157.12.041-051. (In Russ.).

Goyman, V.I., (2001). *Law in the System of Normative Regulation. General Theory of Law and State*. Edited by Prof. V.V. Lazarev. Moscow: Yurist. (In Russ.).

Grachev, N.I., (2009). *State Structure and Sovereignty in the Modern World: Issues of Theory and Practice*. Dr. Diss. (Law). Volgograd. (In Russ.).

Gvozdeva, A.A., (2020). The Role of Strategic Planning Acts in the System of Constitutional and Legal Regulation. *Russian-Asian Law Journal*, 2, pp. 19–24. (In Russ.).

Imekova, M.P., (2023a). The Concept of Legal Support. *Bulletin of Tomsk State University*, 487, pp. 212–219, doi: 10.17223/15617793/487/24. (In Russ.).

Imekova, M.P., (2023b). Legal Support of Private Interest. *Lex russica*, 76(9), pp. 146–159, doi: 10.17803/1729-5920.2023.202.9.146-159. (In Russ.).

Inalkaeva, K.S., (2024). Formation of Federative Relations in the Russian Federation: Experience, Problems, Prospects of Sevelopment. *State Power and Local Self-Government*, 5, pp. 3–5, doi: 10.18572/1813-1247-2024-5-5-3-5. (In Russ.).

Ivanov, V., (2010). The State and Sovereignty. In: *Theory of the State*. (In Russ.).

Ivanova, S.A., (2016). Public-Law Enforcement of Civil-Law Relations: Statement of the Problem. *Obrazovanie i pravo*, 2, pp. 87–97. (In Russ.).

Khalatov, A.R., (2006). Sovereignty as a State Legal Institute. Cand. Diss. (Law). Sochi. (In Russ.).

Komissarov, A.V., Komissarov, M.A., Abakumova, E.Y., (2023). Modern Approaches in Legal Support of the Mechanism of State Control of Entrepreneurial Activity. *Law and Economics*, 9, pp. 35–40. (In Russ.).

Kozbanenko, V.A., (2003). Legal Support of the Status of State Civil Servants (Theoretical and Administrative Aspects). Dr. Diss. (Law). The Author's Abstract. Moscow. (In Russ.).

Krasinski, V.V., (2017). *Protection of State Sovereignty*. Moscow: Norma, Infra-M Publ. (In Russ.).

Krasner, S.D., (1999). *Sovereignty: Organised Hypocrisy*. Princeton: Princeton University Press.

Krasyukov, A.V., (2023). Tax Sovereignty: Concept and Content. *Taxes*, 1, pp. 31–36, doi: 10.18572/1999-4796-2023-1-31-36. (In Russ.).

Leonov, A.S., (2013). State Sovereignty: Etymology and Prehistory of the Concept Development. *Bulletin of N.I. Lobachevsky Nizhny Novgorod University*, 3(2), pp. 131–135. (In Russ.).

Marchenko, M.N., (2003). State Sovereignty: Problems of Sefinition of the Concept and Content. *Jurisprudence*, 1, pp. 186–197. (In Russ.).

Maslov, K.V., (2023). Bodies of Internal Affairs as Subjects of Legal Provision of Tax Security of the State. *Administrative Law and Process*, 7, pp. 49–52, doi: 10.18572/2071-1166-2023-7-49-52. (In Russ.).

Melekhin, A.V., (2009). *Theory of State and Law*. 2nd ed., rev. and suppl. (In Russ.).

Mushinsky, M.A., (2015). Strategies, Concepts, Doctrines in the Legal System of the Russian Federation: Problems of Status, Legal Technique and Correlation with Each Other. *Yuridicheskaya Technika*, 9, pp. 491–493.

Romanovsky, G.B. and Romanovskaya, O.V., (2022). On Digital Sovereignty. *Constitutional and Municipal Law*, 9, pp. 25–31, doi: 10.18572/1812-3767-2022-9-25-31. (In Russ.).

Sapun, V.A., (2002). The Theory of Legal Means and the Mechanism of Realisation of the Right. Dr. Diss. (Law). N. Novgorod. (In Russ.).

Shumkov, D.M., (2002). Social and Legal Grounds of State Sovereignty of the Russian Federation (Historical and Theoretical Analysis). Dr. Diss. (Law). St. Petersburg. (In Russ.).

Shundikov, K.V., (2009). Goals and Means in Law. Cand. Diss. (Law). Saratov. (In Russ.).

Smorchkova, L.N., (2024). To the Question of Methodology of Administrative Legal Regulation in the Sphere of Economics. *Administrative Law and Process*, 6, pp. 15–18, doi: 10.18572/2071-1166-2024-6-15-18. (In Russ.).

Stepanov, D.G., (2009). Public Legal Support of Entrepreneurial Activity. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 3, pp. 227–232. (In Russ.).

Taribo, E.V., (2024). The Category of "Sovereignty" in the Practice of Russian Constitutional Justice. *Constitutional and Municipal Law*, 3, pp. 2–6, doi: 10.18572/1812-3767-2024-3-2-6. (In Russ.).

Tikhomirov, Y.A., (2013). Legal Sovereignty: Spheres and Guarantees. *Journal of Russian Law*, 3, pp. 5–20. (In Russ.).

Troshev, D.B., (2024). *Administrative and Legal Protection of the Sovereignty of the Russian Federation from Unfriendly Actions of Foreign States*. Moscow: Prospekt Publ. (In Russ.).

Zharova, A.K., (2021). Ensuring the Information Sovereignty of the Russian Federation. *Jurist*, 11, pp. 28–33, doi: 10.18572/1812-3929-2021-11-28-33. (In Russ.).

Ziegler, Ch.E., (2012). Differences in Perceptions of Sovereignty among the United States, China, and Russia. *Comparative Politics*, 3(1), pp. 3–14. (In Russ.).

Zubarev, S.M., (1999). Legal Support for the Reform of the Criminal Executive System. Cand. Diss. (Law). Moscow. (In Russ.).

Zubarev, S.M., (2024). Strategic Acts of Management as a Form of Managerial Decision-Making in the Field of Ensuring National Security and State Sovereignty of the Russian Federation: Problems of Hierarchy. *Courier of Kutafin Moscow State Law University (MSAL)*, 5, pp. 25–36, doi: 10.17803/2311-5998.2024.117.5.026-035. (In Russ.).

Information about the Authors

Sergey M. Zubarev, Dr. Sci. (Law), Professor, Head of the Department of Administrative Law and Procedure, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
smzubarev@msal.ru
ORCID: 0000-0003-4322-3602
ResearcherID (Web of Science): B-2029-2019

Denis B. Troshev, Cand. Sci. (Law), Associate Professor, Department of Administrative Law and Procedure, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
d.troshev@list.ru
ORCID: 0009-0004-8542-663X

LEGAL EDUCATION

Article

DOI: 10.17803/2713-0533.2024.3.29.595-618

Perspectives of Bilingual Training of Lawyers in Russia: The Demands of Time and Society

Natalia A. Abramova, Polina E. Marcheva

Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

Abstract: The paper is devoted to analyzing the necessity to teach law students legal rhetoric in two languages: in Russian and in English, with the purpose to facilitate constructive international cooperation for the conservation of historical and cultural heritage in the modern world, which corresponds to the priorities of the Concept of Foreign Policy of the Russian Federation at present. The bilingual study of legal rhetoric, as any other curriculum discipline, will contribute to the education transition to a qualitatively new level. The term "bilingual training" began to be widely used in the 1990s. It used to be defined as "a purposeful process in which two languages are used when the second language becomes a means of training rather than the subject." It is in the course of bilingual training that conditions are created for the formation of inter-subject integration, thought flexibility in relation to intercultural communication and the development of linguistic abilities in future lawyers, which is extremely important for professional activities in the field of jurisprudence. The bilingual course of rhetoric serves as a good example of developing professional competences and intercommunication pragmatic skills encouraging students to enhance their key professional competences along with deepening their awareness of procedural and substantive areas of law. The authors also dwell on the key elements of rhetorical analysis applicable to main professional

competences in the context of the tertiary educational paradigm based on the accomplishments of domestic methodologists.

Keywords: Concept of the Foreign Policy of the Russian Federation; rhetoric; oratory; intercultural communication; lawyer; bilingual education; bilingual training

Cite as: Abramova, N.A. and Marcheva, P.E., (2024). Perspectives of Bilingual Training of Lawyers in Russia: The Demands of Time and Society. *Kutafin Law Review*, 11(3), pp. 595–618, doi: 10.17803/2713-0533.2024.3.29.595-618

Contents

I. Introduction

Modern educational processes in tertiary education are aimed at developing the students' personal capacities, expanding opportunities for in-depth education through "individual educational trajectories" (Klimova et al., 2023), including linguistic ones. Along with traditional forms and methods, alternative educational technologies are intensively integrated, including bilingual training (Tatkalo and Sarkisyan, 2021; Batalshchikova and Gridneva, 2022; Urusova and Kodzokova, 2023; Bryksina, 2016).

The Concept of the Foreign Policy of the Russian Federation was approved by the Decree of the President of the Russian Federation on 31 March 2023. As specified in Para. 1 of the General Provisions of the Concept, the Concept is "a strategic planning document that provides

a systemic vision of national interests of the Russian Federation in the domain of foreign policy, fundamental principles, strategic goals, major objectives and priority areas of the Russian Foreign Policy."[1]

One of the priorities stated in the Concept is to enhance Russia's role in the global humanitarian space, consolidate the position of the Russian language in the world. In this regard, it is important to pay special attention to training lawyers in communication skills, including training in a foreign language, to facilitate a constructive international cooperation aimed at preservation of historical and cultural heritage as stated in the Concept. Thus, we agree with Dezhneva that "a communicative element based on the foreign language of the educational process should be harmoniously linked with the future profession of a graduate" (Dezhneva, 2008, p. 76).

For this purpose, in many universities students are required to master a foreign language along with curriculum subjects (Marcheva and Kholina, 2021, p. 690). For example, in Kutafin Moscow State Law University (MSAL) the Department of Legal Translation, the Department of the English Language, the Department of Foreign Languages and the Department of International Moot Court Competitions have been founded and are operating with the purpose to encourage studying foreign languages in the context of future careers in law. First, these departments assist students in studying curriculum legal subjects in a foreign language, offering the courses in legal translation, practical courses of foreign languages for lawyers, courses in translation of legal documents, etc. Second, through participating in and organizing moot courts and ADR competitions in foreign languages the acquired knowledge and skills are integrated in practical skills when participating in events held in a non-native language students acquire knowledge in procedural and substantive legal issues. Third, language departments assist in the development and implementation of the curricula and syllabi for Master's Courses held in English.

[1] The Concept of the Foreign Policy of the Russian Federation (as approved by the President of the Russian Federation dated 31 March 2023. Available at: https://mid.ru/ru/foreign_policy/official_documents/1860586/ [Accessed 07.06.2023]. (In Russ.).

This work is also connected with other departments developing bilingual tutorials, course books and textbooks to help Russian and foreign students master the law subjects in a foreign language. Bilingual course books and textbooks implement the methodology of bilingual vocational training that, on the one hand, helps students better understand the subject and, on the other hand, help them master a foreign language quicker due to enhanced motivation. As an example, we will refer in our paper to the outcomes of the use of the textbook entitled "Rhetoric for Lawyers: A Bilingual Course" (Abramova et al., 2023, p. 376) co-authored by professors of three departments: the Department of Philosophy and Sociology, the Department of Advocacy and the Department of International Moot Court Competitions. The textbook was prepared in accordance with the requirements of the Federal State Educational Standard of Higher Education in the areas of Jurisprudence (40.03.01, Bachelor's Degree), Legal Safeguards of National Security (40.05.01, Specialist's Degree) and Forensic Examination (40.05.03, Specialist's Degree). The expected audience for this textbook is students studying at the law faculties and departments.

Today, legal relationships are deemed as first-priority relationships in the design of the state and society at both national and international levels. The interpretation of legislative activities in the media and the access of mass audience to the activities carried out by law-upholders and law-enforces require the lawyers to comply with the highest standards of professional communication skills. The skills that are more acute for members of the legal community include a good command of the language of the law-making procedure and the ability to correctly formulate and define ideas and thoughts in order to make them clear not only to the professional community, but also to ordinary citizens. Rhetoric as an academic subject is the discipline that is able to form in would-be lawyers' critical skills of professional public speaking and the ability to use them in a variety of professional multilingual situations (institutional discourses).

The material presented in bilingual course books and textbooks should be aimed at the development of rhetorical skills of the students that are necessary to create an effective argument, to improve their ability to speak in public and influence the audience and decision-

makers, as well as to provide Russian-speaking students with the language training. Their purpose is to provide assistance to students in their study of the laws of public speech preparation and making an expected impact on the audience in typical communicative speech situations in two languages: Russian and English.

II. Methodology

Bilingual teaching and training have been used in various fields for quite a long time. However, the teaching methodology itself has undergone qualitative changes. The changes were aimed at making students feel more comfortable and confident not only in the educational environment, but also after starting their professional activities.

In this regard, the use of the interdisciplinary approach in the development and further use of bilingual teaching methods in relation to a particular professional activity is of particular importance. The methodology of bilingual teaching of legal rhetoric has been successfully tested among students of Kutafin Moscow State Law University (MSAL). It has helped future lawyers to acquire the necessary knowledge and skills for successful online and offline communication and functioning in various legal professional activities as in-house lawyers, attorneys, legal advisers, etc.

The modern method of bilingual teaching is based not only on providing educational material in two languages, but also through the transfer of customs, traditions and values of different nations. Due to the use of integrated approaches students do not currently need to accumulate knowledge obtained as a result of mastering individual subjects (foreign language, regional studies, specialized subjects, etc.). The methodology currently used develops students' complexity and scale of thinking, encourages them to acquire tolerance and multicultural skills in a significantly shorter time.

As a result, based on this study, a conclusion was formulated that the synthesis of the linguistic, subject and intercultural component contributes to the formation of bilingual-communicative professionally oriented competence. Moreover, it is aimed at developing the ability and

readiness to use a foreign language as a means of obtaining information on the specialty from different areas of its authentic functioning.

The methodology of teaching rofessional activities differs due to the need to master certain knowledge, skills and abilities, but the general modern approaches used at present certainly help to reduce the amount of time required for immersion in a foreign cultural environment, and most importantly, allow one to avoid "biases in the study of language or culture in favor of a foreign one." Bilingual professional training itself contributes to the expansion of the information and educational space of students, the development of the personality of a future lawyer in an intercultural and interlingual context (Urusova and Kodzokov, 2023, p. 216).

The authors focus on the thesis that understanding of the subject matter and intercultural components of two different legal cultures having comprehensive and independent rhetorical foundations contribute to the formation of the bilingual communicative professional competence in addition to the development of the ability and willingness of the students to use a foreign language as a means to obtain relevant information from different areas of authentic functioning of a foreign language. Thus, the authors attempt to provide a comprehensive comparative analysis of different schools of business communication in order to draft recommendations regarding bilingual teaching of rhetoric to law students and elucidate main provisions substantiating rhetorical analysis of public speaking in the domestic school of rhetoric.

III. Features of Intercultural Communication of a Lawyer

Communication (from French "communication;" Latin "communication," i.e., *message transmission*) is commonly understood as a socially constructed process of transmission and perception of information in terms of interpersonal and mass communication. Whereas *professional communication* means a specific form of human interaction, assuming people to communicate, share thoughts, information, ideas, etc., in the process of employment in a particular subject area" (Nemytina, 2014, pp. 53–54). In the process of professional communi-

cation, the lawyer consults clients, helps negotiate and talk business, represents and defends clients in court.

Of course, when any verbal interaction to a lawyer is taking place, one must take into account national peculiarities of his client and interlocutor, because approving the stance of Roy L. Lewicki, David M. Saunders, Bruce Barry and John W. Minton (Lewicki et al., 2015, p. 37), we believe that culture affects the style of our communications, both verbal and non-verbal. Depending on culture, there are differences in body language: the same behavior can be considered offensive in one culture and completely harmless in another.

"In Russian society, there is an acute problem of finding ways of harmonious development and conflict-free coexistence of various cultures for the upbringing and education of a citizen of a single cultural society" (Mayorova, 2010). The same is true for foreign students, since in the process of studying they should form an idea of the brilliant school of Russian business rhetoric, both in practical and theoretical terms. Rhetoric is not abstract and not universal. It is always national, since it is based on the national language. Thus, within the scope of this paper we can speak about Russian, German, American, Japanese rhetoric, but not about universal rhetoric. General rhetoric means the principles of the prose texts construction, but these principles are always applied in a particular culture in a particular national language. Therefore, "the national personality characteristics of a business partner should also be taken into account in business communication" (Samygin, 2021, p. 120).

Many researchers, including Samygin and Stolyarenko, define the following national styles of business relationships: American, French, German, English, Chinese, Japanese, South Korean, Arabic (Samygin and Stolyarenko, 2007, pp. 173–181).

In the process of training lawyers, it is necessary to take into consideration the main trends and prospects in the development of the modern world, namely, that in the first place university or law school graduates will have to interact with the representatives of the BRICS,[2]

[2] BRICS — Brazil, Russia, India, China, and South Africa.

SCO,[3] and CSTO countries.[4] Thus, it is important that academic curricula provide the students with the opportunity to study the specifics of communication and peculiarities of business ethics of the residents of these countries.

In this regard, the national styles of business relations in India, South Africa, Brazil, etc., are of particular research interest. For example, Sergey Frank (Frank, 2008, pp. 59–67), who studied the features of business communication in India, South Africa and Brazil, believes that students need to know that **in India,** it is important to communicate politely with people of all ages and to build business relationships based on trust. In India, an ancient tradition to shake hands remains, but a more common greeting now is a friendly nod. If a person to whom you are speaking slightly shakes his head from one side to another during a conversation, his gesture should not be confused with European gesture of denial. Such a gesture in India means attention and understanding.

The South Africans tend to slow the pace of the business communication. They believe that professional success, privacy and the ability to enjoy free time should not contradict each other. When contacting a partner at the first time, you must use the full name. Strong British roots give the South Africans the ability to play by the rules, they can be tough in business relationships. At the same time, the South Africans are often inclined to choose such a decision when although the host is the winner, her opponent does not suffer defeat.

The Brazilians are gifted with eloquence from nature. They are endowed with the talent to immediately establish warm relations, they know how to choose the right tone when discussing difficult topics, and they tend to bypass sharp corners. The golden rule of business meetings in Brazil says that the position and manner of a business partner is fruitful and capable of creating mutual understanding as long as there is an atmosphere of friendliness and harmony at the negotiating table.

Therefore, it is of particular importance to design pedagogical technologies in such a way that knowledge about national characteristics of the peoples of any country is formed not in parallel with the study of

[3] SCO — Shanghai cooperation organization that includes the Russian Federation, Tajikistan, Kyrgyzstan, China, Kazakhstan, Uzbekistan, India, and Pakistan.

[4] CSTO stands for the Collective Security Treaty Organization that includes Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russian Federation, and Tajikistan.

a foreign language and the disciplines necessary for the implementation of professional activities, but in a way of a bilingual course. Training and apprenticeship programs within the programs of student exchange and "studying abroad" programs broaden the opportunities, knowledge, life experience of future specialists. They also contribute to their comprehensive training (Shtokman and Shtokman, 2005, p. 23). However, such practice is not available to all students due to various reasons. In this regard, it is important and necessary to introduce new technologies and teaching methods for training competitive specialists that will allow students to obtain the necessary knowledge and skills in their native educational environment. But only a comprehensive and interdisciplinary approach will allow students to master the knowledge in the shortest possible time, and will also allow them to feel harmonious and confident in the modern educational environment.

Thus, we can conclude that awareness of the culture, etiquette and national characteristics of the representative of a country will help the lawyer to be more successful in business communication. Substantive elements of this knowledge can be taught to law students within the framework of the bilingual course of rhetoric, when two languages can serve as the means for gaining information from foreign sources, demonstrating the outcomes of educational procedure and implementing the outcomes in professional competences. At the same time, interdisciplinarity and comprehensiveness of training will help to reduce the duration of training.

IV. Features of Intercultural Communication of a Lawyer on the Internet and their Relevance for Bilingual Teaching

Currently, digitalization and informatization continues. Due to shortage of time, people are less likely to meet in person; they have to communicate remotely, which has become widespread. Lawyers are not an exception. They communicate on the Internet through chat rooms, forums, webinars, and online conferences.

Communication in the Internet is mediated through a computer or a special device. It is only possible if the sender and the recipient have access to the Internet, they have the skills to operate a computer,

they are able to read and create telecommunication texts. But if we are talking about intercultural communication, lawyers are expected to know a foreign language or several languages.

We should mention the existence of the point of view that the knowledge of a foreign language is not necessary for communication on the Internet since there is always the opportunity to use online machine translation tools. However, we do not share this point of view, as we believe that relying on an online translation tool does not result in effective communication. Effective communication is possible only when the participants of the conversation know the language of each other at least to the extent that facilitates collaboration.

Communication on the Internet is performed using both verbal and non-verbal means of communication and specific vocabulary, the composition of which is constantly updated and is characterized by blurring of the essential differences between communication (interpersonal, group, mass and intrapersonal types of communication).

"The Internet as a means of intercultural communication has its advantages and disadvantages. As an advantage, it should be noted that through communication with representatives of other cultures, people could broaden their horizons, form an idea about a particular culture that differs from their culture. However, there are also disadvantages that include the risks of dissemination of information on racism, incitement to ethnic hatred and recruiting for terrorist organizations" (Galyashina and Nikishin, 2021, p. 160).

Intercultural communication on the Internet occurs both online and offline, the participants of the communication can communicate both orally and through the exchange of messages. To save time, the participants of communication can ignore the spelling rules, put words together and come up with new words (Abramova, 2021).

Thus, it is safe to say that a system of graphical tools has been formed, and, as a result, a new symbolic meaning of a written text has developed.

Another example of intercultural communication on the Internet is an international scientific and practical conferences that are currently widespread. Participants of such conferences can make presentations and engage in discussions with the participants, share experiences and knowledge. And bilingual communicative competence of a lawyer in this case is extremely relevant.

Understanding the issues associated with online communication should be a priority (Turaev, 2021, p. 1512). Similar to any relatively new phenomenon, the Internet is generating many conflicting expectations ranging from unfounded fears to false hopes, which leads to ambiguity of assessments of this phenomenon. Therefore, there is a necessity to create virtual ethics. The objectives of virtual ethics are to include a moral evaluation of the process of virtual communication, theoretical justification of ethical norms and principles governing the conduct in this field, and, finally, the creation of mechanisms to ensure adherence to these standards and principles.

Features of virtual ethics are defined in accordance with the specificity of the object of study. The Internet belongs to no one; it is not controlled by anyone, and it is therefore not controlled by the participants of virtual communication. Virtual communication is generally anonymous and participants may at any time evade contacting, while the possibility of legislative regulation of this area is relatively small, at least at the moment. This gives the user an illusory sense of unlimited freedom to the point of permissiveness (Larionova and Gorchakova, 2021, p. 58). However, as in any social environment, the Internet has its own unwritten rules and norms that define the rights and obligations of participants of the interaction and enable it to maintain its own existence without any external power regulation. These rules are called netiket (net — network and etiquette — etiquette) and they are international. The importance of this knowledge is difficult to overestimate, because on the one hand, there is the mediatization of legal discourse (Nadeina and Chubina, 2023, p. 58). On the other hand, legal discourse actively affects everyday speech and, in the media, professional look from the point of view of rhetoric is very important to form a proper understanding of these processes among young audiences.

V. Public Speaking in Lawyer's Work

For the legal profession based on the "man-to-man" model, communication skills form an important element of professional competence. A lawyer must be able to transmit and receive significant and relevant information in order to achieve the goals of interpersonal

relations, to influence the consciousness and behavior of people using words. In the context of increasing globalization, a lawyer is expected to be able to communicate professionally both in a native and a foreign language.

Professional legal communication, the objective of which is to provide interaction among persons participating in transfer, exchange, and perception of information, combines legal and communicative elements. The legal element provides for deliberating legally significant information, legal opinions, solutions to problems using legal tools and legal implications of the chosen strategy. The communicative element involves the knowledge of different methods, techniques and rules of communication. Only a comprehensive and skillful combination of legal and communicative elements can lead to a successful outcome for the protection and restoration of violated rights and interests of an individual.

The public speaking skill is one of the most important elements of the communicative competence in professional interaction. Many legal practitioners are also engaged in the activities of educational institutions, in the system of training of professional communities, they have their blogs, speak to the media, participate in academic and practical conferences, congresses, and round tables. To succeed as public speakers, they need to employ a compilation of rhetorical and practical experience.

Success of a lawyer in public speaking depends on many factors. First, a speaker needs a clear understanding of the topic of public speaking, he needs to determine the purpose that will penetrate and guide the whole speaking and determine the type of the speech: whether it is informative, persuasive, entertaining, or etiquette. In a multilingual environment, a speaker choses the means of persuasion that comply with the determined purpose of the speech.

The second factor of success is the richness, scrutiny, and relevance of the presented material. Therefore, it is extremely important to search and, which is more important today, select arguments for statements from reliable and reputable sources based on critical thinking.

The third element determining perceptability of public speaking is its clarity and, as a consequence, effectiveness, which is predetermined

by a clear structure of a statement, logical construction of arguments and reasoning. A lawyer should be not only an expert in the field of law, but he should also be good at logical thinking, i.e., be able to consistently build his statement, to reason and justify the statement made, persuasively refute the opinion of an adversary, to explain the conceptual nature of the processes and phenomena, to make logical conclusions. It is well known that the structure of any presentation consists of three stages: an introduction, a main part, and a conclusion. Unfortunately, many speakers make such mistakes as composite heterogeneity, lack of logic, inability to finalize the statement, proving a well-known proverb that says "You started speaking with delight and finished with a sorry sight!"

The success of public speaking largely depends upon how skillful a speaker uses a toolkit of logical and psychological persuasion, awakening the inner voice of the audience, forcing the audience to engage in an internal dialogue with the speaker, encouraging them to make decisions based on internal beliefs. A lawyer should remember that an argument is always targeted at a specific audience in a specific situation and take into account the specific purpose.

Much of the perception of public speaking depends upon how perfect the forms of the language are, upon the style, creativeness, emotionality, and suggestive potential of the speech. A lawyer violating the rules of the native and foreign languages speaking in monotonous, unemotional manner, loses the trust and sympathy of the audience.

Among the reasons why public speaking is often ineffective we can name the lack of the speaker's ability to achieve reciprocity in communication with the audience, establish rapport, follow the audience's reaction, and adjust the dialogue to the audience's expectations during the speech presentation depending on the reaction of the audience. Each speaker should remember that public speaking is a monologue only in form. In fact, it is the dialogic interaction with the listener, and if not, then there is no effectiveness. To this end, public speech should be reasonably rich in vocal techniques of dialogization in order to contribute to an active interaction with the audience.

Indeed, the most important factor for successful public speaking is the impact the personality of the speaker makes on the audience. "We do not listen to the speech; we listen to the person" is one of the

basic premises of rhetoric. Therefore, attractiveness of the speaker is largely determined by the image of a lawyer, his popularity, reliability, credibility, and demeanor.

Studying of the foundations of public speaking skills in both native and foreign language paradigms allows students to develop expressiveness, clarity, and precision of their style, creates and widens proper mindset, awareness and knowledge resulting in developing public speaking skills in the context of the study of legal subjects and their application in practice.

VI. Statements of a Lawyer in Court

Professional work of a lawyer is associated, in particular, with the statements made by a lawyer in court (or any other forum deemed to be the place where justice is administered, e.g., an arbitration tribunal or mediation center). Of course, this applies, in particular, to advocates representing their clients in court and out of court, and the prosecutor.

A court-room lawyer in any jurisdiction where he is practicing, must be familiar with the substantive and procedural law, to be able to analyze, draft and submit procedural documents, and work with the case. Also, a courtroom lawyer will need to acquire the knowledge and skills in the field of courtroom eloquence in order to be able to make his speech persuasive.

A court-room lawyer needs skills of courtroom eloquence at the final stage of the hearings, at the stage of oral arguments, as it is at this stage that the lawyer has the opportunity to provide the court and other parties to the proceedings with the result of his work conducted at the pre-trial stage and in the course of the trial.

The stage of oral arguments is the final part of the trial when, exchanging the statements, the participants involved in the case sum up the results of the evidence examination and the court is provided with the grounds on how the case should be resolved on the merits.

Professional communication of persons participating in oral arguments is regulated by the rules of procedural law that prescribes the sequence of speeches, but does not regulate either the structure or the content of the speeches themselves. Thus, the task of a courtroom

lawyer is to work scrupulously both on the content (the legal element), on the form (the linguistic element), and on ethics (the ethical element) of his speech.

The legal element of courtroom arguments provides an analysis of the evidence, the standings of the parties to the case, the facts given, the characteristics of the accused and witnesses, as well as the reference to and analysis of legislative norms, jurisprudence and case law. Of course, the courtroom speech of a lawyer in civil proceedings differs from the speech of a lawyer in criminal proceedings. Thus, the objective of the lawyer representing a claimant or a defendant in a civil case is to persuade the court of the validity of the claims or objections, while the prosecutor's objective and the objective of the defense lawyer is to substantiate the guilt or innocence of the defendant.

The linguistic element of courtroom arguments is determined by the structure of the speech itself and the linguistic devices used. Thus, Professor Sergeev draws attention to the accuracy and purity of the style, diversity of words, decency, simplicity and strength, euphony and other features of oral arguments. At the same time, in order to effectively convince the court, Professor Sergeev advises using imagery, metaphors and comparisons, antitheses, and other rhetorical devices. According to him, a speech made up of reasoning alone cannot stay in the minds of people who are not used to this (Sergeev, 2019, pp. 13–18).

The ethical element of courtroom arguments, despite being subjected to numerous studies and contemplations, still leaves much to research**.** The ethics of court arguments includes a set of rules of conduct that participants of the court session should adhere to when delivering their speech (oral arguments). If *ethics* is a set of rules of conduct (usually in relation to a certain social group), we are talking about professional ethics, we refer to moral requirements related to the specifics of a certain profession, for example, the ethics of judges, advocates or prosecutors.

Let us consider what ethical requirements are imposed on judges, lawyers and public prosecutors in the Russian Federation.

Judges in their professional activities are guided by the Code of Judicial Ethics approved by the 8th All-Russian Congress of Judges held on 19 December 2012. The principles and rules of professional conduct

of judges are set out in Chapter 3 of the Code. Thus, the Code of Judicial Ethics enshrines the obligation of a judge to adhere to highest cultural standards in proceedings, to maintain order during the court session, to behave in dignified, patient, polite manner towards all the participants of court proceedings (Cause 7 Art. 11).

Advocates in their professional activities must comply with the rules set forth in the Code of Professional Ethics of the Advocate adopted by the 1st All-Russian Congress of Advocates on 31 January 2003. The preamble of the Code states that "the existence and activity of the Bar community is impossible without observance of corporate discipline and professional ethics, concerns of advocates for their honor and dignity and the authority of the Bar."

The principles and rules of professional conduct of an advocate are set out in the first Section of the Code of Professional Ethics of the Advocate. Thus, a lawyer has no right to make statements derogating the honor and dignity of other participants, even if those participants behave themselves improperly and impolitely (Para. 7 Clause 1 Art. 9). Objecting to the action (inaction) of judges and persons participating in the proceedings, an advocate must object in a proper manner and in accordance with the law (Art. 12).

State prosecutors, as well as advocates, must comply with ethical standards enshrined in the Code of Ethics of the Prosecutor of the Russian Federation approved by Order No. 114 of the Prosecutor General's Office of the Russian Federation dated 17 March 2010. Thus, a prosecutor, in his formal and informal capacity is obliged to strive in any situation to preserve personal dignity and not to commit acts that give reason to doubt his honesty and decency (Clause 1.3 Art. 1). During the proceedings, the court refrains from actions that can be regarded as actions exerting undue influence on the process of administration of justice (Art. 2.1.11). In relations with other participants in the judicial process, a prosecutor shall adhere to the formal business style, demonstrate integrity, politeness, impartiality and respect for all participants of the court session (Art. 2.1.12). Also, a prosecutor should adhere to the business style of clothing corresponding to the status of a public official, comply with etiquette rules regarding jewelry (2.1.17).

Thus, lawyers who speak in the courtroom, especially judges, advocates and public prosecutors, must comply with the established ethical rules and regulations. Disrespect, offensive and insulting statements and other manifestations of unethical behavior are unacceptable.

During the proceedings in criminal and civil cases, disagreements between the participants, including disagreements between the advocate and the public prosecutor or between lawyers representing the parties, are certainly "not only possible, but sometimes inevitable, and, therefore, disputes are inevitable" (Revina, 2016, p. 37). During a dispute it is difficult to maintain composure and behave in an ethical manner. However, it should be noted that a dispute that is taking place in the courtroom is not just a dispute the participants of which can use any words and expressions in order to win. The argument that is being conducted in the courtroom "requires great tact and the ability to use its techniques, taking into account the situation prevailing in the courtroom as a result of the trial" (Sapozhnikov, 1971, p. 73). Only in this case, the judge, after analyzing the arguments given by the parties, analyzing the arguments heard, will be able to establish the truth in the case and make a reasoned and fair decision.

Therefore, a controversy between the parties in the courtroom should be formal and restrained. In this regard, it is worth agreeing with S. Aria who argued that "criticism of the rival will become much more effective if it is calm and reasoned, i.e., ethical. A courtroom speaker may seek to evoke the emotions of judges, but not to demonstrate his own." (Aria, 1996, p. 50). Both the judge and the parties, being in the courtroom, should demonstrate compliance with high culture standards and not allow disrespect for themselves, since, as Boikov notes, "the legal maturity of a specialist cannot be characterized only by a certain amount of knowledge and skills. It includes the appropriate level of moral development of an individual, mastering ethical requirements of this profession." (Kolokolova, 2010, p. 301).

Thus, in order to successfully perform in the courtroom, a lawyer must elucidate the legal, linguistic and ethical elements of the speech, he has to possess knowledge in the field of judicial eloquence, and scrupulously prepare for speeches, especially for speeches to be pronounced in court arguments.

VII. Rhetorical Analysis of Courtroom Disputes in the Lawyer's Work

A legal dispute constitutes the foundation of a lawyer's professional work, i.e., a process where each party proves its own standing and provides its own interpretation of the situation, criticizing the arguments of an adversary. The interaction between adversarial parties allows us to see a variety of points of view on the same problem, provides additional information, helps to clarify the positions of those who are involved in a dispute.

Therefore, for any practicing lawyer it is important to understand the nature of speaking in court arguments, types of dispute adherent to different legal cultures, rules of their implementation, depending on national specifics and purpose.

During a dispute, there is always a contradiction in an explicit or implicit form**,** which helps us define a problem and clarify the positions of the parties. In the course of collective discussion, the problem is either resolved (dispute, discussion, argument) or each of the opposing parties remains of the same opinion (discussion, controversy).

Depending on the intentions of the adversaries and the purpose of the dispute, arguments can be constructively aimed at developing a common position, discussing solutions to the problem, refuting an incompetent approach, etc. It can also be destructive, turning the discussion into a scholastic dispute, discrediting the opponent and the idea underlying the dispute, etc. It is very important for a lawyer to understand the true reasons for entering into a dispute and court arguments in order not to succumb to provocations.

For the dispute to proceed rationally, it is necessary to observe the logical and moral and ethical rules of conducting a dispute, discussion, and court arguments. They include: 1. a clear understanding of the subject matter of the dispute by each of the parties; 2. a clear understanding of the purpose of the discussion-dispute and the strategy for achieving the purpose of the dispute; 3. preparation of a credible argument; 4. respect for the opponent; 5. unacceptability of social or physical pressure.

In the majority of cases, arguments forming the subject matter of the dispute can be both correct and incorrect, depending on the purpose,

provided information, a source and method of presentation. A lawyer should have an idea about acceptable (loyal) and unacceptable (disloyal) methods of conducting a dispute in order to conduct a discussion tactfully and meaningfully (Abramova et al., 2023, p. 53). A dispute or discussion can quite often turn into a conflict situation, where one of the adversaries demonstrates incorrect behavior or makes incorrect judgments in relation to the opponent. To prevent a dispute from escalating into a conflict, it is necessary to remain calm and maintain composure and resort to a counter against every unacceptable behavior.

As practice shows, legal dialogue can be conflict and conflict-free in nature. In various areas of legal relations, the conflict situation can manifest itself in different ways and, consequently, it can be resolved logically and ethically in different forms. For example, in the process of conflict-free legal consultation, interviewing, mediation, or in discussions on legal issues in a soft-conflict mode, the priority cross-coefficient of ethical evaluation of a dialogue is whether it is logical or illogical, whether provided argumentation is an evidentiary statement or a sophistic speculation.

If a legal controversy is taking place in the mode of acute conflict, for example, in the interrogation of the accused for convicting him of a crime, then logic alone is not enough, because. it is not always effective. In such cases, it is important to take into account tactics, ethics, psychology, pragmatic and communicative expediency of communication.

In order to make professional communication held in the form a discussion effective, it is important to learn how to behave in a dispute properly and analyze the behavior of partners. The success in the dispute can be affected by extralinguistic factors, such as the volume and height of the voice, the tone of the voice, intonation, tempo, gaze, facial expressions, gestures, demonstration of attitude towards the opponent.

Along with logical and ethical elements, a legal dispute also has aesthetic, psychological, rhetorical and other elements, the knowledge and application of which encourages a lawyer as a professional communicator to conduct a dialogue more effectively, avoiding errors and revealing errors in the arguments of opponents.

The persuasiveness of a lawyer's standing during a dispute directly depends on the quality of the arguments, they must be true, reliable, they must not contradict each other and be sufficient to prove the claimed point.

There are two types of arguments: arguments "for" (for the premise) and arguments "against" (against the premise). Describing the arguments "for," it should be noted that they should be truthful, based on authoritative sources, available, simple and understandable, as close as possible to the opinions of the audience; reflecting objective reality, corresponding to common sense. The arguments "against" should persuade the audience that the provisions cited in support of the criticized premise are very dubious, they do not stand the critical argumentation. The systematic presentation of arguments gives them strength and persuasiveness.

During the dispute, the lawyer, justifying the thesis, can use direct or indirect evidence. The direct proving is conducted with the help of strong arguments, without involving any assumptions that contradict the thesis: a direct reference to arguments, facts confirming the premise, a reference to a law rule.

The indirect proving is provided by putting forward an antithesis (assumption) and establishing its falsity. On the basis of the law of excluded middle, a conclusion is drawn: since the thesis and the antithesis exclude each other, the falsity of the antithesis means the truth of the thesis.

Lawyers often use a special form of proving — refutation — in their court argumentation. In court proceedings, proving by the defense of the defendant's innocence and the refusal of the prosecutor to bring a charge serve as the refutation.

In different audiences and legal situations, various types of refutation are effective: refutation of a thesis, criticism of arguments, failure of demonstration. For example, criticism of the arguments of a procedural opponent is important in court proceedings, since the unfounded nature of the crime serves as a reason for the acquittal of the accused by virtue of the presumption of innocence.

The argumentation used by a lawyer in a discussion and court argumentation is always focused on a specific audience with its mental

representations of good and evil, the world order, justice and the current legal situation.

Despite universal and doctrinal considerations regarding issues referred to the field of rhetoric, their examination based on bilingual materials will result in better understanding of the complex legal discourse, which will be advantageous for law students due to the complex nature of many legal disputes involving foreign element.

VIII. Conclusion

In the paper, the authors have analyzed the problems of developing students' motivation to study a foreign language in interaction with professional training in legal rhetoric. Synthesis of the language elements, subject matter and the intercultural element contributes to the formation of bilingual communicative professional competence, in addition to the development of the ability and willingness to use a foreign language as a means to obtain information from different areas of the authentic functioning of the relevant legal information. Bilingual vocational training contributes to the expansion of the information and educational space for students, development of the personality of a future lawyer in cross-cultural and cross-language contexts.

However, we need to keep in mind that foreign students coming to Russia to study law will also need comprehensive and reliable bilingual course books and textbooks. "In Russian society, there is an acute problem of finding ways of harmonious development and non-conflict coexistence of various cultures in the education and training of a person of a monocultural society" (Mayorova, 2010). Understanding of this premise is of particular importance for foreign students studying in Russian law schools and faculties, since, during their studies, they will have to scrutinize an outstanding school of Russian rhetoric, both practical and theoretical, mastering of which is not possible without understanding the origins of its formation.

The authors substantiate the need to develop bilingual textbooks with the aim of strengthening the role of Russia in the global humanitarian space, strengthening of the Russian language in the world. The Russian language is of great importance not only for the Russian Federation, but

for the world civilization, because it is one of the world's languages and the most important tool for other Nations to understand humanistic values of Russian culture, education and science, thereby increasing the authority and protection of Russia's geopolitical interests.

References

Abramova, N.A., editor, (2021). A Word in the Digital Epoch. *Proceedings of the Student Scientific and Practical Conference dedicated to the 15th anniversary of the adoption of Federal Law No. 53 "On the State Language of the Russian Federation."* Moscow: Kutafin University publishing House. (In Russ.).

Abramova, N.A., Golovina, N.M. and Marcheva, P.E., (2023). *Rhetoric for Lawyers: Bilingual Course*. Moscow: Prospekt Publ. (In Russ.).

Aria, S., (1996). Kindness will save the World (On the Moral Principles of Advocacy). *Rossijskaya Justitsiya [Russian Justice],* 2. (In Russ.).

Batalshchikova, E.Yu. and Gridneva, A.N., (2022). Bilingual Education: Advantages and Disadvantages. *Bulletin of Lugansk State Pedagogical University. Series 3. Philology. Media Communications,* 2(76), pp. 64–68. (In Russ.).

Bryksina, I.B., (2016). Linguistic methodological foundations of professionally oriented foreign language teaching in a non-linguistic university (bilingual/bicultural aspect). *Tambov University Review. Series: Humanities*, 1(153), pp. 17–26. (In Russ.).

Dezhneva, V.V., (2008). The development of motivation to learn a foreign language and its relationship to the success of professional training of students of universities of the Ministry of Internal Affairs of Russia. *Psychopedagogy in Law Enforcement*, 2(33), pp. 76–77. (In Russ.).

Frank, S., (2008). *Business without boarders: Business Communication, Negotiations, Presentations*. Trans. from Germ. Moscow: Olymp-Business Publ. (In Russ.).

Galyashina, E.I. and Nikishin, V.D., (2021). Peculiarities of Administrative Cases on Recognition of Information Materials as Extrem-

ist and their Examination in terms of Secure Internet Communication. *Aktual'nye problemy rossijskogo prava*, 16(7), pp. 159–167, doi: 10.17803/1994-1471.2021.128.7.159-167. (In Russ.).

Klimova, T.A., Kim, A.T. and Ott, M.A., (2023). Students' Individual Educational Trajectories as a Condition for High-Quality University Education. *University Management: Practice and Analysis*, 27(1), pp. 23–33, doi: 10.15826/umpa.2023.01.003

Kolokolova, N.A., (ed.), (2010). *An Advocate in Criminal Proceedings*. Moscow: Unity-Dana; Zakon i pravo Publ. (In Russ.).

Larionova, A.V. and Gorchakova, O.Yu., (2021). Destructive Communication among Youth on the Internet: Socio-Political Context. *Russian Foundation for Basic Research Journal*, 5(107), pp. 141–150, doi: 10.22204/2587-8956-2021-107-05-141-150. (In Russ.).

Lewicki, R., Saunders, D. and Barry, B., (2015). *Essentials of Negotiation*. 6th ed. New York: McGraw-Hill Education.

Marcheva, P. and Kholina, E., (2021). Methodology of Teaching Law Disciplines in Russian and English to Law Students: A Digital Form and Traditional Content. *Kutafin Law Review*, 9(1):4, doi: 10.17803/2313-5395.2021.4.18.690-712.

Mayorova, I.I., (2010). Trends in the Development of Education and Upbringing of Indigenous Peoples in Canada and Australia (19th — 20th centuries). Cand. Sci. (Pedagogy) Diss., Moscow. (In Russ.).

Nadeina, T.M. and Chubina, E.A., (2023). Interaction with media as an important component of a lawyer's professional communication. *Scientific Research and Development. Modern Communication Studies,* 12(2), pp. 58–62. (In Russ.).

Nemytina, M.V., editor, (2014). *Professional skills of a lawyer: a textbook and workshop*. Moscow: Yurayt Publ. (In Russ.).

Revina, I.V., (2016). Moral Criteria of Judicial Pleadings. *Advokatskaya praktika [Advocate's Practice],* 5, pp. 37–40. (In Russ.).

Samygin, S.I., (2021). *Business Communication. Standard of Speech*. 5th ed. Moscow: Knorus Publ. (In Russ.).

Samygin, S.I. and Stolyarenko, L.D., (2007). *Business Communication for Students*. Rostov-on-Don: Phenics Publ. (In Russ.).

Sapozhnikov, I., (1971). Arguments in the Prosecution Statement. *Sotsialisticheskaya zakonnost [Socialist Legality]*, 10, p. 73. (In Russ.).

Sergeev, V.I., editor, (2019). *Advocacy in Russia*. 5th ed. Mosow: Yustitsinform Publ. (In Russ.).

Shtokman, E.A. and Shtokman, A.E., (2005). *Higher education in the USA*. Moscow: Publishing House of the Association of Construction Universities; 2005. (In Russ.).

Tatkalo, N.I. and Sarkisyan, I.R., (2021). Bilingual education as a prerequisite for overcoming the language barrier and ensuring the academic success of students in the era of globalization of culture. *Uchyonye zapiski. Electronic scientific journal of the Kursk State University*, 4(60), pp. 616–626. (In Russ.).

Turaev, K.S., (2021). Internet Communication and its Role in Shaping Public Opinion in the Context of Globalization. *Political Science Issues*, 5(69), pp. 1512–1517, doi: 10.35775/PSI.2021.69.5.023. (In Russ.).

Urusova, L.H. and Kodzokova, B.V., (2023). Modern Bilingual Education: Advantages and Disadvantages. *Law and Management*, 3, pp. 215–219, doi: 10.24412/2224-9133-2023-3-215-219. (In Russ.).

Information about the Authors

Natalia A. Abramova, Dr. Sci. (Pedagogy), Associate Professor, Department of General Educational Disciplines, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
naabramova@msal.ru
ORCID: 0009-0008-0417-854X

Polina E. Marcheva, Cand. Sci. (Law), Associate Professor, Department of Advocacy, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
pekorotkova@msal.ru
ORCID: 0000-0002-6899-1950

ACADEMIC EVENTS

DOI: 10.17803/2713-0533.2024.3.29.619-629

The Law of the Shared Norm

Evgeniy V. Malyshkin
St. Petersburg University, St. Petersburg, Russian Federation

Cite as: Malyshkin, E.V., (2024). The Law of the Shared Norm. *Kutafin Law Review*, 11(3), pp. 619–629, doi: 10.17803/2713- 0533.2024. 3.29.619-629

On 23 May 2024 St. Petersburg Academy of Postgraduate Pedagogical Education named after K.D. Ushinsky organized and hosted the Conference "Thought as an Event: in Memory of Alexander Isakov." The Conference was not only an academic event, but also a personal attempt made by each participant to say heartwarming farewell to Alexander Isakov, who had recently passed away. Fiends, students and close colleagues of Professor Isakov took part in the Conference. The format of dialogical exchange of ideas contributed to the general idea of paying tribute to an outstanding philosopher and thinker of the modernity.

The Conference was opened by **Gulnara Khaidarova**'s report entitled "The Time of Reconstruction." The event of thought in the philosophical tradition is self-valuable and autonomous. However, it is precisely its unconditionality that generates the need for a certain illuminated stage arranged in a special way: it must have friendliness (*philia*) as the ability to give place to thoughtful utterance and love as an illuminating force. Alexander N. Isakov thought and talked a lot about this. "Humanism and Christian Love" is the title of the report that he prepared, but he did not have time to perform. This "and" should

be understood as an addition to completeness, as a recognition of the insufficiency of "normal" humanism. Here it is necessary to keep in mind that functional literacy has become a general trend in school and higher education. Friendliness, Gulnara Khaidarova argues, is a necessary complement to humanism, and without friendliness it does not make sense at all.

Walter Benjamin, analyzing one of B. Brecht's poems, noted that friendliness is both the source of the creative power of thought and the need to communicate thoughts to others. We find friendliness at the most critical moments of life — in birth, in the first steps in life, in saying goodbye to life, — and without it no event is possible. The key phrase in Benjamin's text is "he comprehended the futility of cruelty." Let me add here my own consideration: it is unexpected, but the relevance of this statement cannot be denied, it is already scary to admit it. The report provided an answer to this dilemma: whoever wants to overthrow rigidity should not miss any opportunity to show friendliness. And for Alexander Isakov it was characteristic of the ability to keep friendliness in an unclouded state, which created a sense of authenticity of a philosophical meeting and generated an event of thought.

Nikolai Ivanov structured his report in his usual manner, as an expanded metaphor. It is difficult, if at all possible, to retell such a report, since there is a great risk of losing not only the shades of meaning, but meaning itself, since the complexity of the metaphorical utterance cannot be reduced. But fortunately, every metaphor consists of individual replicas that in this case are significant in themselves, and we will undertake to reproduce them.

Ivanov's entire report was built around Plotinus' phrase "Every soul is and becomes what it looks at." In his soul Alexander Isakov was a desperate hack, a secular lion and a cavalry guard, but the third "Critics" by Immanuel Kant is in his hands. There was nothing in his look from an exemplary fighting man: no bearing, no pride. A bookish man and a hermit; a peaceful intellectual, who treated the civil slaughter, the universal fooling and brutalization of people with Tolstoy's inflexibility. Only in philosophy he appreciated what brings it closer to military discipline and makes it a science, namely: rigor.

Originality and brilliance of thought should always be preferred to its thoroughness, this is the only discipline of the mind.

Here, the tone of the paper becomes so elegiac that it is separated from tearfulness only by tragic irony, reminiscent of the stories by O. Henry. We will allow ourselves a detailed quote: "And yet, even as a joke, it was not for nothing that his friends nicknamed him 'Sashka the War.' He knew so much, and with such boyish enthusiasm he talked about wars, battles, generals, combat formations and branches of the armed forces, officer duels, carousing and love affairs, about weapons, standards, uniforms, ammunition, military orders and insignia, military customs and etiquette, military campaigns and exploits of heroes of all times and peoples. But especially, of course, Russian history."

Alexander Isakov loved the excitement of battle, not forgetting about the war as "of beginning of everything," according to Heraclitus, even at chess. Isakov's thought is a battle where nothing falls out of the pure field of the master's speculation. In this battle, not only self becomes a seer, but the world itself becomes sighted. Not every soul is ready to bear this world's gaze. With the test of transcendental fortitude of the soul, its baptism of fire begins. The experience of philosophy as such begins with this test: as preparations for death, according to Plato. Philosophy is the back mind in the face of death, always someone else's, and birth, always one's own. Despite of Aristotle's believe, philosophy does not begin with astonishment and it is not born free, for its own sake. Astonishment as such, *i. e.*, a surprised imagination, generates only unintentional fright and laughter. Only the admiration of the soul saves from speculative infertility. But it is impossible to conclude to admiration. Philosophy can become free if it wins its freedom. Therefore, the war is the beginning of everything, i.e., of the archetypal congeniality of thought and being.

Alexander Govorunov asked the question to clarify the phrase "drill training of the mind," whether it is possible to get a couple of lessons. As an answer, it was stated that, in an essential sense, the philosophical school is a drill. You have to be able not to spoil the row of those who are behind you. So that it is even. And to lift the leg to the correct height. Not higher, but not lower than the rest. It includes training camps, combat training, and shooting. After all, there

are idols all around — markets, caves, etc. You need to have time to examine all this and shoot it. Nevertheless, Aleksander Isakov did not like all that, although he delved, often even too deeply, into historic-philosophical distinctions. There is a war, and there is a civil massacre. And in thought, we can only talk about the original war, about settling personal accounts with the world.

One more noteworthy statement of the Conference declares that nothing makes a thought an event. There is nothing outside thought, which forces a thought to come true. When we interpret the dynamic world in terms of entities, we destroy it as an event. Therefore, the only thing that becomes an event is a test of the spirit for its presence.

Evgeny Malyshkin spoke about the course given by Aleksander Isakov at the Open Philosophical Faculty (recordings of these meetings are available on popular video hosting sites). The course contains two terms that are repeated over and over again and that are impossible to perceive directly: shared evidence and investment. Regarding the latter, in the case of communication between theology and philosophy, there is no talk of a reliable transfer of investments. What is it then? It is about neighborhood, or, as Gulnara Khaidarova said, about friendliness, which Aristotle calls not just *philia*, but *philophilia*, such a friendly disposition that invites you to do what you are already doing, but in an established community. God, death, love — this is what we need to discuss in the company of philosophy and theology. Thus, we are talking about the hyphen, about the "between:" death-immortality, God-Being, reason-love. But this hyphen itself precedes the subject.

There are two different ways to discuss such precedence. The first is as follows: reflection on the "between" itself, avec-, cum- — everything that we find in Nancy's book "Being singular plural." This method also has a limitation, which Aleksander Isakov notes: there are things that cannot be divided. Such are not only corporeal, material things. With regard to the latter, the sharing impossibility is obvious: half an apple is not the same as a whole apple. Therefore, if I share an apple with someone, I will share a friendly disposition, but not the apple itself. But it is also impossible to share primacy, just as it is impossible to share paternity. Much of the course given by Aleksander Isakov is devoted to this contradiction, the need to share obvious things when it is impossible to share a lot of them.

Now the second method of discussing mentioned precedence is also visible: reasoning about sharing itself, on the boundaries of sharing. In these limits the quantitative question is no less important than the qualitative: not only what you share, or with whom. But also, with how many? The quantitative dynamics of separation tells us something important about the sharing itself: how many elements are capable of being involved in this obviousness? The thesis repeated by Isakov about the unconscious God, "God is existence," can be grasped in quantitative terms: how does existence grow if the meanings are given to those who exists only in shared forms? There is a dynamic of sharing itself, therefore, questions can be asked not only within the limits of these three elements: I or you or between us.

Larionov inquired if we are talking about limits, then what cannot be invested in?

In Ivanov's opinion, it is impossible to invest in the field of fools or idols. For example, "objective reality," "cognized necessity," the world of truth comprehensible from the outside, the intelligibility of the world based on the intelligibility of objects of experience for everyone — all that is often passed off as philosophy itself, whereas in this case philosophy turns out to be only a means, a banknote put into our idols, in order, primarily, to reduce our freedom.

Nina Savchenkova said that Alexander Isakov drew her attention to Dietrich Bonhoeffer's book "Ethics." But she had a chance to read it only recently, and it became clear that there was a strong connection between what the German theologian wrote about and what Alexander Isakov spoke and wrote about. The general plot is: teachers and teaching. And even greater coincidence of themes is visible through Bonhoeffer's book "The Cost of Discipleship," where the same plot is discussed, but in different aspects, the call of Christ to follow him and how this call can and should be followed.

Obedience turns out to be not just a practice or discipline, but a desire. This concept turns out to be both a critique of the authoritarian model of knowledge transmission and Lacanian models of desire. The concept of desire as obedience unfolds in a certain epistemological modesty: there is no Subject declared, who speaks or wins his place, believes in his desire or insists on it. Ultimately, this concept becomes

self-referential, so much that it is impossible to say that "following is this and that." A similar revolution is taking place in film theory: the idea that big theories destroy the subject, i.e., cinema language, is accepted; ultimately, any interpretative model replaces the subject of interpretation itself. If the time of big theories has not passed in philosophy, and large and long-term projects still hold sway in many minds of our contemporaries, then Isakov can be called an adherent of a small theory.

But what is important here is not so much the refusal as the special ability to work with subject matter: working with a film, a book, a philosophical situation. And this is precisely what unites the style of Bonhoeffer and Isakov: the ability to work with details. Reading a film, for example, occurs through unfolding a small episode: it is lived, thought through, unfolded into a certain openness. In psychoanalysis, this is called a clinical vignette. And in psychoanalysis this turn has also taken place: now, even in supervision, they work not with cases, not with a whole plot, but with vignettes, based on which you can take some walks to grasp how this fabric is woven. As if we do not reach the whole, but enter into a certain openness, we are dealing with the horizon, that is, with the possibility of expanding the horizon.

One more answer to the question "What makes a thought an event?" says that starting with details, it would seem, is a common hermeneutic practice. Understanding is one thing, turning a detail into experience is another. When a thought produces a shared experience, we are dealing with an event.

In turn, Evgeniy Malyshkin admitted that in big theories we are dealing with a whole, with a set of discursive practices in which this whole is given, etc. But in small theories we are also dealing with the same thing, details are not given in themselves, they are always already inscribed in a certain context and then it will become noticeable. What is the difference between the big and the small then?

In fact, the answer to this question was in the question itself. The whole is given in big theories, that is, the pragmatic attitude. For example, a text can be written in different ways. First, formulate a concept, we can demand from the student a structure of the work, a

research plan. Or you can move in the opposite direction: one can be offended by some detail, some intonation, and then one can try to figure it out. The second path is much more hopeless, it is associated with uncertainty, with risk.

Professor Ivanov stated that much of what was said was close and true. Alexander Isakov's emphasizing of what seems like a trifle is very characteristic of him. Accepting the conclusions, Professor Ivanov insisted that the order of the sequence raised some doubts. The synthesis of service and desire in this concept of "following the step" is an example of a Taoist teacher. But the Taoists taught is the exact opposite: do as I do, do not follow me. And Alexander Isakov himself followed this thesis. Therefore, there is some kind of crack in the source that simply changes the very essence of the matter.

However, if Isakov was well oriented in philosophy, and everything was known to him, then in the religious tradition there was something that was unknown, not entirely clear, and that he hoped for. And it is important to stay with it as with some mystery. As if between Christ and His apostles something similar to friendship occurred, which is continuous and cannot be broken. This continuity should probably be called obedience.

Andrey Musatov insisted that Isakov's well-known virtues were based on his acquired understanding of what philosophy is. He liked to repeat that to practice philosophy is an author's business. But there are authorship and authorship. Alexander Isakov was precisely foreign to philosophizing tragic tone, when someone, inflamed with a noble passion, invites the whole world to witness how he resolves insoluble metaphysical questions. When, realizing the insolubility of these very questions, he is only engaged in describing the subjective conditions of their solvability.

Alexander Isakov distanced himself from this kind of romanticism. It was important for him that philosophy could take its place in a multidimensional dialogue with cultures, sciences, and arts. And the philosopher himself discovers his relevance and necessity, the demand for professionally posing questions of the ultimate kind. The first thing that catches the eye in Isakov's manner is complexity. Not only in the

sense of Plato's "everything beautiful is difficult," but also in the sense of complexity in composition, multi-aspect. And if we turn to the topic of education, then the question naturally arises: why is this complexity needed, which Isakov demonstrated continually in his lectures and papers?

To set a certain level of complexity, a certain bar. Young people, having tasted this complexity, will no longer be able to get involved in any discussion of so-called geopolitics, or other "actual" topics. If you thought at full-height, you will not want to return to squatting. Isakov often repeated that the task of a philosopher is to predict the nature of a future war. But it is not the task of philosopher to predict something. In what sense should this thesis be understood? Perhaps the very interdisciplinarity and multi-facetedness that creates the need for intellectuals can serve as a hint. As catastrophe theory can be applied in predicting wars. But it is still not very clear what philosophy has to do with it.

Evgeniy Malyshkin clarified that he always perceived this as a beautiful metaphor. Thus, Leibniz named 3 + 1 signs of reality: your judgment should have three different characteristics, but all the three can be replaced by a prediction. A philosopher has nothing to predict. But there is at least one thing that makes sense to point out: reality itself. And there is one thing in relation to which it always makes sense to think ahead: war. As in Heidegger, the future has an advantage over the present, because there will be a death.

Khaidarova in her statement said that Alexander Suvorov had a concept of anticipatory thinking. And the training of a military man comes down to the cultivation of this very anticipatory thinking. The quote itself is from Svechin, who was well acquainted with the works of Clausewitz and Kant. There is an interesting biographical fact: in February of 1922, Isakov began writing a work, and he wrote it, that was devoted to negotiations. How are negotiations possible at all and what is the conditions for the possibility of sitting at the same table.

In Professor Ivanov's opinion, the answer, in general, lies on the surface. This kind of formula, of course, is worth of reflection. It has metaphysical interest by virtue of its beauty. However, a character (i. e.,

of a war) is a form of a *priori*. This is beyond any forecast. There is nothing to anticipate in the war, its character is obviously unhuman. But theoretically this should be connected with a situation in which the being brings itself to the extreme. Not when the metaphysician goes to the edge of the earth (as every metaphysician should do), but when this edge belongs to the earth itself.

Ksenia Kapelchuk in her report reminded that on 23 May, when the Conference was held, another outstanding professor, Timofey Antonov celebrated his birthday, and perhaps it makes sense to try to compare his style of teaching with that of Alexander Isakov. If we were to produce a taxonomy of great lecturers, we would get two groups: producers of ideas and concepts and their keepers. Isakov and Antonov, for all their differences, were both keepers: if you noticed any gaps in knowledge or understanding of some sophisticated texts, you knew that they were the ones who could provide you with the answers. However, Isakov's discourse was quite sophisticated itself. It seems that talking about philosophical systems and concepts in the language of these very systems is rather a tautological matter: how can we understand Kant by means of another Kant? Isakov often performed a certain interpretative trick, referring to the classic literary works and films. But the remarkable feature of these interpretations was that he did not explain the incomprehensible through the understandable. On the contrary, the unknown encountered in the texts suddenly transformed what had long seemed familiar into something unexpected, and both semantic series finally got corresponded to each other and surprisingly they got clear.

In his article devoted to Dostoevsky and discussing the novel "Crime and Punishment," Alexander Isakov mentions Lacan's distinction between empty speech and full speech as one in which some kind of desire is invested. Can we regard one of the Isakov's latest texts Dostoevsky's Dialectic: The Name of the Father and the saving power of children's life itself as a full speech? Something caught Ksenia Kapelchuk's eye. When Alexander Isakov writes about "The Brothers Karamazov," he regularly calls it "Dostoevsky's final novel." How to understand this finality? In articles from different years, although they are very similar

thematically, the theme of children and childhood is only growing. In the earlier texts he turns to the Japanese researcher Nakamura, who points out that Dostoevsky has a Buddhist motive in his "Crime and Punishment," since it shows rebirth without redemption. But then this motif unfolds in the Isakov's course "The Thought as an Event," and the middle term here is precisely the concept of childhood, a return to a childlike state. Eventually in his text on "The Brothers Karamazov" Isakov refers to Walter Benjamin's account on Dostoevsky's "Idiot," that gives to this theme a new attitude perfectly matching with the figure of Alexander Isakov himself. A quote from W. Benjamin helps Ksenia Kapelchuk show that immortal life is not something infinite; it is eternal renewal, and Isakov's thoughts were characterized by this renewal, seemingly referring to the well-known idea of the immortality of the soul.

Oleg Nogovitsyn stated that just as in the discussion of several Kant's problems, the central concept for us is the experience of consciousness — this experience is the very "condition of possibility" of a priori synthetic propositions. Thus, in ancient commentaries on Aristotle's syllogistic it is not the forms of correct syllogisms that are discussed, but the ability to find a middle term: this is precisely the business of a philosopher, to find it. But how can we still speak of the unity of both the event of thought and those objects to which our experience is directed? In Christianity, this search is understood as a personal event that opposes the Neoplatonic teachings in which the God creates as a natural being; this Neoplatonic God cannot therefore be given his due, he cannot be revered. It is precisely this difficulty that Alexander Isakov draws attention to when he points out that Christianity begins not with the apostleship, but with the community, since it is impossible to speak on unique individual experience: faith is inherent in every act of consciousness, that is why Christianity becomes the intellectual tradition. To discuss the clash of two orders of universality in Christianity, Greek and Jewish, it is necessary to conclude: only that thought is true which helps to win the war. But the concept of war and contemplative life are poorly compatible. I do not think that Alexander N. Isakov has found a solution, but this is the horizon open to us.

The final utterance of Alexander V. Govorunov can be formulated as follows. Philosophy has no other language than the language of the history of philosophy. Therefore, philosophy is a special kind of temporality that is possible even outside of historicity. And every thought is an event if it is a responsibility. The responsibility should be understood rather as the ability and desire to be in the center of attention. Aleksander Isakov never condescended to the unpreparedness of the audience. To dare to be in the center, to dare to be among the best interlocutors, to dare to speak with the best thinkers in any audience — this is what it means to be a philosopher.

Information about the Author

Evgeniy V. Malyshkin, Dr. Sci. (Philosophy), St. Petersburg University, St. Petersburg, Russian Federation
malyshkin@yandex.ru
ORCID: 0000-0002-1247-4866

Kutafin Moscow State Law University (MSAL)

https://kulawr.msal.ru/

https://msal.ru/en/

kulawr@msal.ru

+7 (499) 244-88-88