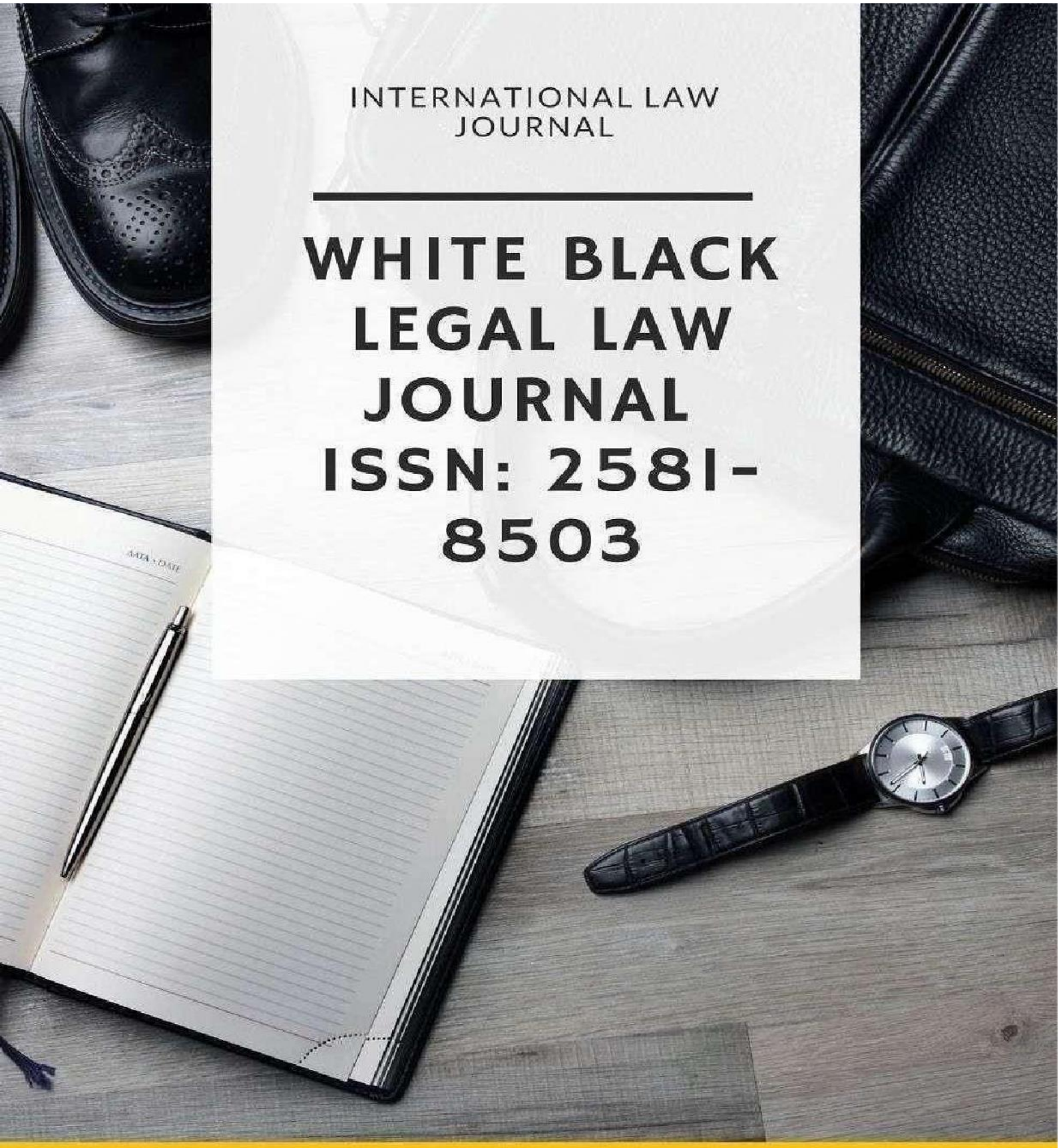


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

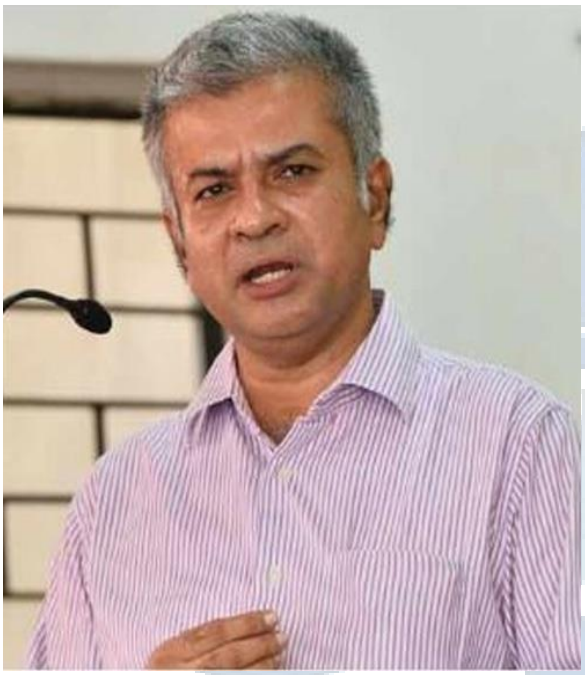
The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

 ISSN: 2581-8503

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Feb 2025 ISSN: 2581-8503

RIGHT TO PRIVACY: A COMPARATIVE ANALYSIS OF DATA LEGAL PROTECTION IN INDIA AND RUSSIA

AUTHORED BY: G MADHURAVALLI,
Advocate, Supreme Court of India
CO-AUTHOR - RADHIKA MAHESWARI

ABSTRACT

The purpose of this Research Article is to compare and contrast Nations like India and Russia in order to examine the differences between the Rights to Privacy and Data Protection, to understand the intent behind the privacy legislation in the two nations where such a unique type of centre is present. After encountering some significant judicial knowledge on the issues associated to data breach and privacy infringement, they developed their own approach to dealing with the privacy laws of its citizens. Numerous widely used applications have been blocked in both nations due to the judiciary's and government's recent actions about data protection and potential breaches. The difference of approach in resurrecting the privacy of its citizens have been the fundamental difference among the two, in this article the author tries to culminate the difference in the approach and the outcomes from them. The author employed the doctrinal research approach to generate a study of the topic, with a focus on primary data. This article will discuss the issues that gave rise to the data protection bill and amendment in the countries and their current deficiencies. Russia, on one hand, has reached a point where they are turning their arbitrariness to avoid data breach and the disclosure of personal information, while India is far behind in understanding how to handle its booming digital economy. We'll examine the underlying problems in this article and provide some reasonable, plausible explanations. The article aims to assess the strongest aspects of each system and suggest a sensible modification in both nations with respect to the *Vasudhaiva Kutumbakam*, One Earth, One Family, One Future, and look into the ideology behind both the system of Governance regarding the Data privacy and protection.

Keywords: Human Rights, Fundamental Rights, Right to Privacy, Digitalization, Data Protection

1. INTRODUCTION

Background and Significance of comparing India and Russia in terms of privacy and data protection laws

The right to privacy is a fundamental human right that logically flows from the rights to individual liberty and life. In this digital age, it is easier than ever to violate someone's right to privacy without any ill will. With the rise of digitalization and the information technology industry, people are frequently losing sight of the importance of protecting other's privacy, often without the victims even being aware that their rights have been violated.

The adoption of The Digital Personal data Protection Bill, 2023[i], (The digital persona data protection bill, 2023) and the extensive debate of its shortcomings with regard to recommendations to improve it through numerous revisions made it urgent to address the research gap this has caused. India is a democratic nation, therefore the check and balance provided by a law helps to adapt and improve the processes as needed.

The Russian Constitution, on the other hand, places a strong emphasis on the privacy of its residents; as a result, they are compelled to follow the law and its directives. The Russian Constitution's check and balance system includes a strict mechanism governing amendments, leaving little room for dynamicity.

"Article 21 of The Indian Constitution mentions Right to Life and Personal Liberty"[ii] which states that "No person shall be deprived of his life or personal liberty except according to a procedure established by law"- this article is placed at a pedestal for interpreting the value of Privacy and it is developing in line with current dynamic trends.

"Chapter 2 Rights and Liberties of Man and Citizen in Article 19 of The Russian Constitution" mentions "Equality before law and State shall guarantee equality of rights and freedom of man…" [iii] -it can be deducted that both the countries emphasize on Personal liberty and privacy of its citizens but the way of dealing with it is different.

It is suggested that these restrictions on the right to data protection and what qualifies as lawful processing represent a compromise between several legitimate interests. Showing that the controller/and processor's the data subject's interests are at odds with one another, however, is not in either party's or theirs. A corollary of the right to data protection is the emphasis on the

methods and circumstances under which personal data may be processed lawfully. The privacy principles that have been the foundation of regulatory efforts to protect personal data can be utilized to spot troubling activities in the processing of 'personal data. As a result, the right to privacy and the right to data protection cannot be separated.

The Research Article analyzes the present trends in Digital Privacy laws of both the countries which have definite different structures and their past nuances.

2. EVOLUTION AND JUDICIAL PERSPECTIVE OF RIGHT TO PRIVACY, DATA PROTECTION IN INDIA

The current legal framework provided by the Information Technologies Act, 2000 and supplemented by the other applicable general laws, The Digital Personal Data Protection Act, has raised several questions in the past that need to be resolved as soon as possible due to opposition from a number of sources with respect to Data protection and right to privacy in India. The Parliament and its agencies were alerted to the physical shortcomings, the absence of the dimensions of privacy rights, and the dynamic character of those rights by the rejection of the new privacy bill.

The deal breaker of question related to Right to Privacy and Data Protection was, On August 24, 2017, in Puttaswamy v. Union of India (*Puttaswamy v. Union of India*, 2017),[iv] the Supreme Court of India acknowledged the right to privacy for the first time. India now acknowledges the right to privacy as a basic right, and data protection law also has more attention. But in the past, the government would have seriously infringed on both rights. Additionally, access by the state would be exempt from the current protective systems. In this regard, there would be a legislative gap, making it impossible to rule out access to "EU" citizen data once it is kept on Indian soil.

Indian privacy Like the United States, India has experienced legal challenges to its right to privacy, but in 2017 their constitution fully enshrined it. The right to privacy was advocated for inclusion 'in "India's constitution when it gained independence from Britain in 1947". However, it was rejected because many people believed that if the right to privacy meant that "every private/civil communication would be elevated to that of Governmental papers,"[v](Vishalakshi Singh, 2014) it would interfere with state inquiries and investigative

authority. By drawing comparisons to the U.S. fourth amendment, the German, and the Irish constitutions[vi], attempts were made to include the right to privacy. The Supreme Court found that certain rights to privacy' are guaranteed by Articles 19 and 21[vii].

Article 19 dealt with providing freedom of "speech and expression …without the fear through oral/written/electronic/broadcasting/press,"[viii] implying that one has the right to say or express and broadcast without fear of persecution. Article 21' of the constitution of India[ix] protected both the right to life and the right to liberty, effectively prohibiting the state from interfering with either right without due process [x](Campbell, C. (2021). and after considering all applicable laws. Both articles, however, were insufficient in 'one of the earliest cases where defendants claimed that their right to privacy was in jeopardy. The Indian Supreme Court determined in the 1954 case of (*M.P. Sharma & Ors. vs. Satish Chandra and Ors*1954)[xi]. that the right to privacy was not guaranteed by the Indian Constitution and that its original drafters, who compared it to the Fourth Amendment in the United States, did not deem it appropriate to include such a right.

The case concerned the government's authority to "search and seize" papers from the defendant's property in order to uphold 'the right to property, which was deleted from India's constitution in 1978. As a result of the searches turning up self-incriminating papers, the defendant alleged that their right against self-incrimination' under Article 20[xii] and their right to privacy had been infringed. The state was within its rights to remove the objects and was within its rights to do so, according to the court, and the activities were only transitory and did not entirely violate their right to their property.

Kharak Sigh v. The State of Uttar Pradesh, (*Kharak Singh v. the state of UP*, 1962)[xiii] included the 'defendant, Kharak Sigh, who had been released from jail owing to a lack of evidence after being accused of bank robbery'. This case also dealt with the right to privacy as it related to surveillance. The police force that had detained him began monitoring the defendant and compiling a "History Sheet" that would allow them to follow his whereabouts. Kharak alleged that the department's trips to the defendant's residence during off-hours during the day and night violated his right to privacy, which is guaranteed under "Article 21, The Constitution of India (1950)"[xiv] and is a condition of having a good life and enjoying one's freedoms. The Court decided that the right to privacy was immaterial because it was not a right protected by the Indian Constitution, as it had in the former case. The police officers who went to the defendant's

residence interfered with Kharak's ability to exercise his right to life and liberty. Kharak's right to life and his freedom of movement, as stipulated by Article 19, were hindered by the police department restrictions, which were ruled to be unlawful. The Supreme Court disagreed that the right to privacy existed in the constitution in the two cases described above, so the defendants were unable to use it as evidence in court. In both cases, the defendants raised the issue of the right to privacy, but it was ultimately rejected by the court. In the Kharak case, one of the justices, Subba Rao, did, however, accept that privacy was a component of liberty. In cases decided after 1975, the Supreme Court found that the right to privacy existed, to a certain extent, but that it would essentially follow a common law system where judges make decisions based on precedent as there isn't any specific written or codified legislation that governs the situation.

3. LEGISLATIVE FRAMEWORK IN INDIA

Constitutional Provision on Right to Privacy and Data Protection

It wasn't until Justice K.S. Puttuswamy v. Union of India (*Puttaswamy v. Union of India,* 2017)[xv] that the Supreme Court's nine judges decided to make a revision and include the right to privacy in Part III of the Indian Constitution. 'In "2017, the Supreme Court of India decided that the right to privacy was a basic right, even while noting that privacy was in threat due to the development of new technologies"'. The Indian Constitution's article 21 was supported by the court in the case of Justice K.S. Puttaswamy (Retd) v. Union of India (*Puttaswamy v. Union of India,* 2017)[xvi] by stating that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."[xvii]

Data Protection Laws in India

Information Technologies Act, 2000

"The communication industry has frequently been the focus of previous data protection legislation, which has the drawback that it frequently lacks monitoring. In addition to the communication industry, there is additional legislation in place to protect the data that is kept on residents", including the 2009-created biometric system in India. India started moving toward enacting legislation approaching a data protection law with the passage of the Information Technology Act, 2000 (IT Act).[xviii]

The original act had undergone numerous modifications in 2008 and 2011. The Act attempted

to punish “those who exploited customer data, prevent theft and other cybercrimes, and handle the expansion of” "electronic commerce," which is the buying and selling of goods online. The organisation that stored the data was not penalised by the act; only those people who broke into the system were. In order “to avoid the disclosure of sensitive personal data or information”, sections 72A and 43A [xix] security methods and procedures were inserted in the 2008 modification.

People had the right to file lawsuits against the firms if it was discovered that their sensitive personal data had been compromised. With the implementation of the “Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules in 2011”, organisations in India that deal “with the collection and disclosure of sensitive personal data or information were subject” to new regulations. “The usage of Aadhaar, the contentious biometric identity programme that assigns each Indian resident a 12-digit number, was legalised in 2016 according to the Aadhar Act, as established by the Supreme Court”. Everybody is given a unique number that can be used to conduct official business, similar to the “Social Security Number system” in the U.S. The original purpose of Aadhaar, which is optional, was to get government benefits.

The Digital Personal Data Protection Act, 2023[xx]

The Act is related to the Digital Personal Data Protection Act, (2023)[xxi], which was recently passed by the Parliament of India and aims to control how digital personal data is processed. The Act recognizes the need for authorized processing but places a strong emphasis on individual’s rights to protect their personal data. It describes the creation of the Data Protection Board of India and includes clauses pertaining to the selection of a Chairperson and Members with backgrounds in data governance, law, and related subjects. The Appellate Tribunal offers a forum for appeals against the Board's orders, and the Board itself has the authority to investigate violations, issue directives, and inflict penalties.

Crucial terminology including “automated,” “data fiduciary,” “data principal,” and “personal data” are defined in the Act, offering a clear framework for application and interpretation. It lays out what data fiduciaries must do, including getting permission, informing data principals, and designating a Data Protection Officer. It also covers how children's personal data is processed, stressing the necessity for parental or legal guardian approval and outlawing tracking, behavioural monitoring, and child-targeted advertising.

The Act gives data principals a number of rights, including as the ability to obtain information about their personal data, the ability to have that data corrected or erased, and the ability to designate another person to act on their behalf in the event of their incapacity or death. The Act also describes the responsibilities of data principals, including following relevant legal requirements and offering genuine information while defending their rights.

The Act also creates adjudication and fines, allowing the Board to assess financial penalties after looking into and assessing a number of breach-related factors. It authorises voluntary undertakings and outlines the process for submitting an appeal to the Appellate Tribunal. The Act deals with crediting amounts generated through penalties to the Consolidated Fund of India and provides mediation as an alternative dispute resolution mechanism. Additionally, it grants the Central Government the power to issue orders and make information requests for the protection of the general public and national security.

The Act offers protection for activities conducted in good faith under its provisions and places emphasis on the law's compatibility with other laws. It also delimits the authority of civil courts to hear cases pertaining to the Board's jurisdiction and specifies the Chairperson's authority as well as the roles and protocols the Board must adhere to. Finally, the Act allows the Central Government to issue directives and credits the Consolidated Fund of India with amounts realized from fines. It also contains clauses pertaining to regulations, the defence of acts done in good faith, the authority to request information, and conformity with other laws.

App Ban in India due to Right to Privacy

The Indian government, in deliberation with the Ministry of Information and Technology, banned 59 Chinese applications during the border dispute between India and China. The Chinese apps were illegally transmitting personal data from India to India. These decisions about the app prohibition were made in order to protect the nation's integrity, security, and sovereignty. The Indian Constitution's Article 19(1)(a) guarantees the right to free speech and expression. This grants the general population the freedom to voice their ideas on any sociological subject on any public forum.

The app ban was majorly targeted to save the user data considering it imperative for the national security. The Central Government or another body may, in accordance with Section 69A, give instructions for the blockage of any material via computer resources. The government has

banned these Chinese apps in order to safeguard the nation's security by preventing the apps from sending sensitive personal data about Indian users to China for usage.

4. EVOLUTION AND JUDICIAL PERSPECTIVE OF RIGHT TO PRIVACY AND DATA PROTECTION IN RUSSIA

Unlike several Western nations, Russia lacks a robust legislative structure devoted to the protection of the right to privacy. The Russian Constitution does, however, offer some degree of private protection.

"Everyone shall have the right to privacy, personal and family secrets, the protection of honour and good name," reads Article 23 of the Russian Constitution. The foundation for Russia's protection of private rights is laid out by this clause.

There have been cases in which Russian courts have addressed privacy-related matters in case law. For instance, the Russian Constitutional Court has rendered decisions in matters concerning the right to privacy, especially when it comes to data protection and monitoring. Nevertheless, in comparison to places with more advanced privacy regulations, these lawsuits are frequently few in number. One such case is the 2018 verdict on the validity of extensive surveillance by the Russian Constitutional Court. The Court determined that some anti-terrorism policies implemented in Russia that allowed for extensive monitoring were illegal due to their violation of individual's private rights. This decision highlighted the importance of privacy rights in Russia's legal system.

Furthermore, Russia has accepted international treaties like the European Convention on Human Rights (ECHR) that contain rules pertaining to the right to privacy. Although the implementation of ECTHR rulings in Russia can be uneven, individuals in Russia who feel their privacy rights have been infringed upon may file an appeal with the European Court of Human Rights (ECTHR) in Strasbourg.

The right to privacy and the protection of personal information are both protected under the Russian constitution. These rights would be constrained, though, by the expansive powers granted to the Russian state to protect the country and fight terrorism. Therefore, privacy regulations would be used by Russian authorities as a tool to uphold political ideals, keep

control of the Internet, and defend the nation's interests. Despite the formal legal framework's initial appearance of thoroughness, the enforcement and execution of the legal rules would reveal severe problems. Intelligence and counterintelligence organisations were granted practically free access to all kinds of personal data in the lack of openness and judicial independence. These limitations on the right to privacy would also be compatible with a startling history of transgressions against the “European Convention on Human Rights” and other fundamental rights. This would include all Russian citizen’s personal information, which the Russian government may then access without their knowledge or permission.

It would be much easier for Russian law enforcement agents to get personal information if it were transferred to Russia via sites like Facebook, Twitter, or YouTube that Russian individuals frequently use to express their disapproval of government policies. Russian Internet users would therefore find it much more difficult to use these sites to express themselves anonymously online because the government would have much easier access to real identities. Similar to how Facebook, Google, and other platform’s messaging services might be exposed to the extensive surveillance systems used by the Russian government, this could have a chilling impact on the right to free speech.

LinkedIn is a well-known brand, especially in Europe and the US, where other sizable multinational IT firms with operations in Russia are headquartered. However, it was never very well-liked in Russia, thus the country’s domestic public opinion was unlikely to react negatively to its prohibition. On the other hand, according to Volkov of the Association for the Protection of the Internet, "the complete blockage of Facebook, Google, YouTube, or Twitter could trigger unwelcome street protests (Taylor Wessing, 2022)[xxii] To demonstrate what can happen to firms if they don't comply, the Russian authorities are using LinkedIn as an example to pressure them to bring their data to Russia, without really blocking them at this time. Unsettlingly, this instance also sparked the first known banning of a mobile application. LinkedIn was taken down from the Apple and Google app stores at the request of Russian authorities. Despite it being far from obvious if the law actually required this, it nonetheless happened. Apps are the "new choke point of free expression, according to Rebecca MacKinnon, Ranking Digital Rights at New America, because mobile phones are becoming a more common way for people to access the Internet. Thus, this might have established a risky precedent.

The Personal Data Law requires data processors to process data "with the use of databases situated in the territory of the Russian Federation, (The Constitution of the Russia Federation,1993)[xxiii] which includes non-Russian data controllers having to abide by all of its restrictions (the so-called "data localisation requirement"). Uncertainty surrounds the methods through which international controllers without a physical presence in Russia are expected to become aware of the regulations that apply to them and how the local privacy agency, Roscomnadzor, might check that they are following them.

It should be given top priority to draught data breach notification and privacy audit policies, review and update other internal policies and procedures in line with the amendments, compile records of processing activities, and update data processing agreements. The amendments made to the Russian data protection laws are very inconsistent in this regard.

Russia has implemented various laws and regulations that grant the government significant powers to monitor communications and collect data for national security purposes. For example, the "Yarovaya Law" passed in 2016 requires telecommunication providers to store user data for extended periods and provide access to security agencies upon request.

5. LEGISLATIVE FRAMEWORK IN RUSSIA

The Russian constitution under Article 23 and 24 carves out the picture of right to privacy and data protection and guarantees as the rights of man and citizen under chapter 2 of the Constitution of Russian Federation

"Article 23 of the Constitution of Russian Federation

1. Everyone shall have the right to the inviolability of private life, personal and family secrets, the protection of honour and good name.
2. Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages. Limitations of this right shall be allowed only by court decision." (The Constitution of Russian Federation , 1993)[xxiv]

Article 24 of the Constitution of Russian Federation

1. The collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent.
2. The bodies of state authority and local self-government, their officials shall ensure for everyone the possibility of acquainting with the documents and materials directly

affecting his or her rights and freedoms, unless otherwise provided for by law." (The Constitution of Russian Federation , 1993)[xxv]

Data Protection Law in Russia

The Russian Federation Constitution, the Labor Code, Federal Law No. 152 FZ of July 27, 2006, "On Personal Data" (also known as the Data Protection Act or DPA), and Federal Law No. 149-FZ of July 14, 2006, "On Information, Information Technologies and Protection of Information" (also known as the Information Law) are among the laws that govern the country.[xxvi]

Federal Law on Personal Data (No. 152-FZ)[xxvii]

The law which was initially enacted in 2006, is the primary legislation governing the collection, processing and storage and transfer of personal data in Russia, which further went through amendments, recent being 2023. The law applies to individuals and organisation including foreign organisation which deals in personal data of such.

The act defines personal data as any information which can directly or indirectly be used to identify a specific individual which may include basic details such as name, address etc to professional, biometric and financial information of such individual. Such data is heavily restricted and requires explicit consent from the individual, technical measures to be take to ensure the confidentiality and notification to the regulatory body -Roskomnadzor.

The consent to be obtained shall be voluntary, specific, informed, documented and revocable in nature, unless used for fulfilling legal obligation, protection the interest of the individual or others, public function or performance of contract and, or is in the legitimate interest of the data operator or a third party.

The Russian data protection law gives data subjects certain rights to manage and safeguard their personal data, including:

1. **Right to Information and Access (Article 14):** Individuals who provide their personal data have the right to be informed about how that data is processed. Data controllers are required to give information about the goals of processing, the origin of the data, the processing techniques, and specifics about any third parties that may receive the data.

2. **Right to Consent (Article 9):** In the absence of legally mandated exemptions, data subject's consent is required before processing their personal information.
3. **Right to Deletion (Right to be Forgotten) (Article 17):** When processing is no longer required or when a data subject withdraws consent, they have the right to ask that their personal data be deleted. Except in cases where there are legitimate reasons to retain the data, data controllers are required to abide by such requests.
4. **Right to Restriction of Processing (Article 18):** Data subjects may ask for processing to be restricted in certain situations, such as when contesting the accuracy of the data or objecting to processing. During the restriction period, data controllers are allowed to keep the data, but they are not allowed to process it any further.
5. **Right to Rectification (Article 16):** People who are the subjects of personal data have the right to ask that incomplete or erroneous information that data controllers have about them be corrected. Data controllers are required to take prompt action to rectify the data.
6. **Right to Data Portability (Article 20.1**): Individuals who provide their personal information have the right to have it returned to them in an organized, widely-used, and machine-readable manner. They can also ask for their data to be transferred to another data controller.
7. **Right to Object (Article 21):** The right to object to processing of personal data, including its use for direct marketing, is available to those who are its subjects. Data controllers must cease processing data unless there are legitimate grounds that take precedence over the rights, freedoms, and interests of the data subject.
8. **Rights Regarding Automated Decision-Making and Profiling (Article 22):** Data subjects are entitled to be free from decisions that materially impact their rights and freedoms that are based only on automated processing, including profiling.
9. **Right to Complain to the Data Protection body (Roskomnadzor) (Article 22.1):** If data subjects feel that their legal rights have been infringed upon, they may register a complaint with Roskomnadzor, the Russian data protection body. (Placeholder1) (Understanding Russian Federal Law on Personal Data Protection: A Comprehensive Guide) [xxviii]

The most of the clauses outlining the majority of the requirements covered here are found in the DPA, which is the most complete source for Russian data protection regulations. The Constitution (Articles 23 and 24) guarantees even greater rights to privacy, and the Information

Law establishes regulations pertaining to information in a wider context. Particular guidelines for data protection in work interactions can be found in the Labor Code. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention) (ratified by Russia in 2006). Dla Piper (2022).[xxix]

Federal Law No. 149-Fz of July 27, 2006 on Information Technologies and The Protection of Information. Ministry Of It. (2007).[xxx]

The Federal Law No. 149-FZ of July 27, 2006[xxxi], which addresses information, informational technologies, and information protection in Russia, is the document in dispute. The legislation delineates the extent of its oversight, encompassing the entitlements to seek, obtain, transfer, generate, and distribute data, the utilization of information technology, and guaranteeing the safeguarding of data. It provides definitions for fundamental terms used in the legal field, including electronic documents, information, and informational technology. The laws are founded on ideas like the inviolability of private life, transparency about state operations, and freedom of information.

The law also covers the following topics: information that is generally available, information that is legally protected, information holder's rights and obligations, and the right to access information. In order to safeguard morality, health, the rights and legitimate interests of persons, as well as the basis of the constitution, it also establishes the limitations on information access. In order to restrict access to websites that contain prohibited content, it also addresses information sharing, the duties of an Internet information coordinator, and the creation of a registry for network addresses and domain names. The law also includes safeguards against acts such as unauthorised modification, destruction, and access to data.

The law stresses the significance of guaranteeing the security and veracity of information and covers the precise processes for limiting access to websites carrying content that is forbidden.[xxxii]

App Ban in Russia for Protection of Right to Privacy

According to research conducted in 2019 by internet freedom advocates Roshomsvoboda found that there were almost 440000 incidents where the individuals were confronted with some type of block while trying to access online content in Russia. O'Driscoll, A. (2020)[xxxiii] The

necessity to safeguard Russian internet user's privacy, state security, and the Russian internet itself has been used by legislators to defend these regulations. In actuality, these regulations establish opaque content-blocking practices, make mass censorship and widespread surveillance easier, and jeopardize the security and privacy of people's online communications. (Dubey, S. 2023).[xxxiv]

The Russian Government has banned or blocked many websites even for unknown reasons, for example, Russia was strict about the access to online gambling in the early 2020 and blocked nearly 35,000 sources for violating gambling and lottery legislation were blocked.

6. COMPARATIVE ANALYSIS

Both the countries even after being very different in type of Government established, focuses equally on the Right to Privacy and Data Protection laws.

India and Russia, promised the Right to Privacy as the citizen's right in the Constitution itself. The constitutional provisions, supplemented by the judicial precedents and interpretation provides for such right very particularly. In addition to the constitutional provisions, both Russia and India have Information Technologies Act and Data protection Laws to specifically protect and regulate the online data and process of such collection and consumption data.

The Right to privacy and data protection further involves the right to take consent from the individual to collect and share such data, right to be forgotten or deletion of such data, which in enshrined within the IT law and Data protection law in India as well as Russia. Further, both the countries provide for statutory body to registered complaints if such breach of privacy or misuse of data is to be found.

7. CONCLUSION

There is an unprecedented need to update privacy and data protection laws and standards in accordance with established, tested global initiatives "given the dynamic and constantly" changing situation in "India, which is replete with challenges", growing foreign investment, and economic growth in a rapidly developing digital world. Even while the absence of comprehensive regulation is concerning, it has been countered by recent efforts by the government, the public, and the industry. These initiatives seek to fortify the current legal system, add to proactive viewpoints and laws, and assist the courts in holding noncompliant

companies responsible for deficient data security. It would be prudent for businesses wishing to establish operations in India to follow local laws, particularly considering how sensitive the Indian legal system has grown to privacy and data protection concerns.

Numerous changes are anticipated for the future of data protection legislation and the right to privacy when combined, especially after the passage of new data protection bills and acts in India and Russia, respectively. Both of these countries have learned from the challenges that have been experienced in the past, and the new laws that have been introduced focus on the positive developments in the "right to privacy and data protection".

The primary issue since the introduction of the new introduced bills in both the countries, namely India and Russia, is with the uniformity of the new introduced bills. due to both countries political systems, Russia is communist while India is democratic. Both countries have distinct approaches to dealing with it, with India being more open about its digitalization than Russia, which is considering closing its digitalization gate. These two approaches are oddly dissimilar yet comparable at the same time.

The Data Protection Bill has been introduced for the first time in India, hence it is unclear how it will affect our nation. However, the Russian government is not new to this; they already understand how and where the consequences that lead to data breaches occur, as well as how to stop them from happening by enforcing sanctions. Data leaks to countries like the USA, China which may cause a lot of harm to its residents as well as to entire nations, are a problem that both the Russian and Indian governments must deal with.

The enhanced legal document on the data protection procedure, which is to prevent the data from being transferred to data exporters and the importer must be aware of the rules regarding the data protection of that country where the data is intended for, demonstrates the stiffness of the Russian government against data protection laws and the right to privacy. In order to protect and investigate issues involving confidential data outside the country, they have created a special authority to deal with the export of personal data of the nation's citizens. A bill establishing turnover fines for data leaks is anticipated to be introduced by the Ministry of Digital Development, Communications, and Mass Media. (Ministry. (n.d.)[xxxv]. An aggravating or mitigating circumstance can be how much the controller complies with the Personal Data Law.

In India, the Digital personal data protection bill, has been enacted which has mentioned such statutory body, Data protection board to regulate and supervise the adherence of data protection rules, but such board is yet to be notified in India.

With the new changes in mind, it can be said that the modifications made for India are somewhat flexible for a nation that upholds Article 21's prohibition on the invasion of the privacy of its citizens. This is because sharing data with large nations can cause more problems than one might initially think. It can be both a blessing and a curse for our digital market, among other concerns like data breach and challenges with a lack of proper authority to deal with it.

In the case of Russia, the country's government's check and balance on the export of its data may be seen as a touch tough and conservative, but it may also prove to be a useful tool for preventing data breaches at the expense of its own resident's rights to privacy. Even though Russian residents are guaranteed the "Right to privacy under article 19 of the constitution". Acts and revisions of this nature may be problematic for this right and be difficult to address in the future. It is pertinent to note that, Russia lacks judicial precedent with respect to Right to privacy and data protection, it is further found that Russia's check mechanism to be arbitrary and no such particular code of conduct are followed by to see how and what causes the infringement of right to privacy. The banning of several apps and restrictions on streaming contents or conditional use of apps and contents posed to be a rigid form of rules to look over such cases.

Overall, Russia's legal basis for private rights is not as robust as that of many other countries, despite the fact that the government has acknowledged the right to privacy in its Constitution and has addressed privacy issues in certain court rulings. However, the topic remains a hot topic in Russian human rights discourse, and new legal developments may have an even greater impact on the country's privacy laws.

With respect to the *Vasudhaiva Kutumbakam*, One Earth, One Family, One Future, and comparison into the ideology behind both the system of Governance regarding the Data privacy and protection of both of the Nations concludes, India and Russia should take lessons from one another in order to enhance their data protection legislation. India specifically should adopt some rigidity, where it shall focus on creating the Data protection board to regulate and

supervise the adherence of the Digital personal data protection bill, while Russia should adopt some flexibility and curb the arbitrariness concerning the breach of privacy and data protection, as it may cause a hindrance to the human rights law and right to freedom of their citizens.

8. NOTES AND REFERENCE

[i] The Digital Personal Data Protection Bill of 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[ii] The Constitution of India of 1950, Article 21(1950) https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[iii] The Constitution of the Russia Federation of 1993, Rights and Liberties of Man and Citizen, Article 19 http://www.constitution.ru/en/10003000-01.htm

[iv] K.S Puttaswamy v. Union of India, (2017) 10 SCC 1, https://indiankanoon.org/doc/127517806/

[v] Vishalakshi Singh, *An Analysis of Personal Data Protection with Special emphasis on Current Amendments and Privacy bill*,144, 148-151, Volume 4 Issue 1, 2014

[vi] The Constitution of United States of 1788, https://constitution.congress.gov/constitution/

[vii] The Constitution of India of 1950, https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[viii] The Constitution of India of 1950, Article 19 and 21,(1950) https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[ix] The Constitution of India of 1950, Article 21 (1950) https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[x] Campbell, C. (2021). *A Review of Data Protection Regulations and the Right to Privacy: The case of the US and India. CUNY Academic Works*. https://academicworks.cuny.edu/cc_etds_theses/985/

[xi] M.P. Sharma v. Satish Chandra AIR *1954 SC 300*, https://indiankanoon.org/doc/1306519/

[xii] The Constitution of India of 1950, Article 20(1950) https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[xiii] Kharak Singh v. the state of Uttar Pradesh (1963) AIR 1295 1964 SCR (1) 332, https://indiankanoon.org/doc/619152/

[xiv] The Constitution of India of 1950, Article 21 (1950) https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[xv] K.S Puttaswamy v. Union of India, (2017) 10 SCC 1, https://indiankanoon.org/doc/127517806/

[xvi] K.S Puttaswamy v. Union of India, (2017) 10 SCC 1, https://indiankanoon.org/doc/127517806/

[xvii] The Constitution of India of 1950, Article 21 (1950) https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/05/2023050195.pdf

[xviii] Information Technology Act of 2000, No. 21, Acts of Parliament, (2000), https://www.meity.goav.in/writereaddata/files/itbill2000.pdf
[xix] Information Technology Act of 2000, No. 21, Section 72A and 43A, Acts of Parliament, (2000), https://www.meity.goav.in/writereaddata/files/itbill2000.pdf
[xx] The Digital Personal Data Protection Act of 2023,. Https://Www.Meity.Gov.In/Writereaddata/Files/Digital%20personal%20data%20protection%20act%2023.Pdf
[xxi] The Digital Personal Data Protection Act of 2023 Https://Www.Meity.Gov.In/Writereaddata/Files/Digital%20personal%20data%20protection%20act%2023.Pdf
[xxii] Taylor Wessing, *USA, India, China and Russia- where is data processing still possible? (*27/11/2022) (10:00) https://www.lexology.com/library/detail.aspx?g=448e70b4-cf80-4a3e-a671-0af81c4058fa
[xxiii] The Constitution of the Russia Federation of 1993, http://www.constitution.ru/en/10003000-01.htm
[xxiv] The Constitution of the Russia Federation of 1993, Article 23, (1993) http://www.constitution.ru/en/10003000-01.htm
[xxv] The Constitution of the Russia Federation of 1993, Article 24, (1993) http://www.constitution.ru/en/10003000-01.htm
[xxvi] Law in Russia. (n.d.). *DLA Piper Global Data Protection Laws of the World*- https://www.dlapiperdataprotection.com/index.html?t=law&c=RU
[xxvii] Baig, A. (2023, August 5). *What to know about the Russian federal law No. 152-FZ. Security*. https://securiti.ai/russian-federal-law-no-152-fz/
[xxviii] *Comprehensive guide to Russian data protection law* (no. 152-FZ). (2024, February 9). https://secureprivacy.ai/blog/comprehensive-guide-russian-data-protection-law-152-fz
[xxix] Dla Piper (2022). *Data Protection Laws of The World Germany Vs Russia.*
[xxx] Ministry Of It. (2007). The Russian Federation Federal Law No. 149-Fz of July 27, 2006 On Information, Information Technologies And Information Protection. Russian Government. Https://Eais.Rkn.Gov.Ru/Docs.Eng/149.Pdf
[xxxi] Ministry Of It. (2007). The Russian Federation Federal Law No. 149-Fz of July 27, 2006 On Information, Information Technologies And Information Protection. Russian Government. Https://Eais.Rkn.Gov.Ru/Docs.Eng/149.Pdf
[xxxii] Federal Law on Information, Informational Technologies And The Protection Of Information, (2006). Https://Members.Wto.Org/Crnattachments/2015/Ip/Rus/15_2261_00_E.Pdf
[xxxiii] O'Driscoll, A. (2020, November 7). *List of websites and apps blocked in Russia.Comparitech.* https://www.comparitech.com/blog/vpn-privacy/websites blocked-Russia/
[xxxiv] Dubey, S. (2023). *Legality of apps ban in India » open access*.
[xxxv] Ministry. (n.d.). *Ministry of Digital Development, Communications and Mass Media of the Russian Federation*. The Russian Government. Retrieved March 25, 2024, from http://government.ru/en/department/387/events/