Research Article

DOI: 10.48165/tlr.2023.3.2.2

ACS Publisher
www.acspublisher.com

Trinity Law Review

Year 2023, Volume-3, Issue-2 (July-December)

ISSN 2583-3588 (Online)

Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information

Shanaz[1] Asifullah Samim[2] and Mohammad Edris Abdurahim Zai[3]

[1]Research Scholar (Law)Department of Studies in Law University of Mysore
[2,3]Department of Computer Science University of Mysore

ARTICLE INFO

Key words: Data Protection Laws and Regulations, Protecting Personal Information

ABSTRACT

The protection of data is grounded in the doctrine of an individual's right to privacy, which has been explored and enshrined in the constitutions of many developed nations. Concerns for privacy and the protection of personal data became prominent in progressive nations during the 1970s with the advent of computerized systems capable of storing and disseminating large amounts of information. India, as a party to several international instruments, acknowledges privacy protections outlined in the Universal Declaration on Human Rights and the International Convention on Civil and Political Rights. While the Indian Constitution does not explicitly guarantee a right to privacy, the courts have interpreted other constitutional rights, such as the right to life and liberty, as encompassing a limited right to privacy. Although India lacks specific legislation on privacy and data protection, the Information Technology Act, 2000, includes provisions intended to safeguard electronic data, including non-electronic records or information processed electronically. In 2011, the Indian government introduced the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, also known as the Privacy Rules. These rules impose procedures on corporate entities collecting, processing, and storing personal data, distinguishing between "personal" and "sensitive" information.

Introduction

The saying "Data is the new oil" has become popular, drawing parallels between the value of data today and the significance of mineral oil in the past. During the time when oil was a highly lucrative commodity, nearly every nation sought after it. However, data has now taken over as the most valuable commodity in the 21st century. This is evident from the fact that five of the world's most valuable companies, including Amazon, Google, Apple, Microsoft, and Facebook, are all part of the data sector. When closely examining data and oil, we can see that they share similarities. Crude oil, in its raw form, is not useful and requires refining and filtration processes to produce usable products such as petroleum, diesel, kerosene, and gasoline. Similarly, raw information needs to be processed and analyzed to convert it into various types of usable data, such as health information, geolocation data, financial

*Corresponding author.
E-mail address: hajirarashanaz@gmail.com (Shanaz)
Received 10-04-2023; Accepted 05-05-2023

data, browsing data, professional and employment-related information, and more.

Data can be broadly categorized into public data and personal data. Public data is generally accessible to everyone and can be freely shared, while personal data is specific to individuals or organizations and cannot be disseminated without their consent. Personal data includes sensitive information like financial details, family details, browsing history, preferences, psychological characteristics, locations, behavior, abilities, photographs, aptitudes, and so on. It can also involve combinations of these features or inferences drawn from refined data. In the current situation in India, there have been reports of the misuse of personal and photographic data collected by private and government agencies across the country. Therefore, India requires comprehensive legislation on data protection that can establish regulatory mechanisms to safeguard the privacy rights of its citizens. In this article, the author examines the roles of regulatory bodies and government policies regarding electronic surveillance and the collection of personal data.

Balancing Rights and Regulation in the Digital Age

The protection of data is rooted in the doctrine of an individual's right to privacy. Many developed nations have explicitly included or inferred the right to privacy in their constitutions, and the parameters of privacy rights have been explored in various forums. The concern for privacy related to the protection of personal data gained prominence in progressive nations during the 1970s with the rise of computerized systems that could store and disseminate large amounts of information easily through automated processes.

India is a party to several international instruments that contain privacy protections, including the Universal Declaration on Human Rights (Article 12) and the International Convention on Civil and Political Rights (Article 17). While the Constitution of India does not specifically guarantee a "right to privacy," the courts of the country have interpreted other rights in the Constitution, primarily through Article 21 (the right to life and liberty), as giving rise to a limited right to privacy. However, the constitutional right to privacy in India is not inherently strong and is subject to various restrictions.

The fundamental rights enshrined in the Indian Constitution, particularly the right to freedom of speech and expression, come closest to protecting an individual's privacy and freedom of expression. The law of privacy in India aims to strike a balance between these two competing freedoms. The growing violation of the right to privacy by the state, often on grounds that are not always bona fide, prompted the Indian judiciary to play a proactive role in protecting this right.

India does not have specific legislation on privacy and data protection. However, the Information Technology Act, 2000, contains provisions intended to protect electronic data, including non-electronic records or information processed electronically. In 2011, India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, commonly known as the Privacy Rules. These rules impose certain procedures on corporate entities collecting, processing, and storing personal data, including sensitive personal information. The rules differentiate between "personal" information and "sensitive" personal information.

In 2011, India introduced a new privacy package with various rules that apply to companies and consumers. One key aspect of the rules is that any organization processing personal information must obtain written consent from the data subjects before undertaking certain activities. However, the application of this rule is still uncertain. The Information Technology (Amendment) Act, 2008, made changes to the Information Technology Act, 2000, and introduced two sections relating to privacy. Section 43A deals with the implementation of reasonable security practices for sensitive personal data or information and provides for compensation in case of wrongful loss or gain. Section 72A provides for imprisonment and/or fines for disclosing personal information of another person while providing services under the terms of a lawful contract.

Key Regulatory Bodies and Agencies Safeguarding Privacy and Security

Regulatory bodies and agencies in India play a crucial role in regulating different surveillance tools under the supervision of the government. These organizations are responsible for ensuring compliance with laws and regulations related to data protection and privacy. Here are some major regulatory bodies and agencies in India that contribute to this regulatory landscape:

- Ministry of Electronics and Information Technology (MeitY) is the central ministry responsible for formulating policies and regulations related to the use of electronic and information technology in India. It oversees various aspects of data protection, cybersecurity, and surveillance technologies.

- Telecom Regulatory Authority of India (TRAI) is an independent regulatory body that regulates the telecommunications sector in India. It sets policies and guidelines for telecommunication service providers, including regulations related to data privacy, protection, and surveillance.
- Unique Identification Authority of India (UIDAI) is the agency responsible for implementing and managing the Aadhaar program, which provides a unique identification number to Indian residents. UIDAI ensures the security and privacy of personal data collected under the Aadhaar system.
- National Cyber Security Coordinator (NCSC) operates under the Prime Minister's Office and is responsible for formulating and implementing policies and strategies related to cybersecurity. It collaborates with various government agencies to ensure the security and privacy of data in the digital ecosystem.
- Data Protection Authority of India (DPAI) is a regulatory body established under the Personal Data Protection Bill, which is currently under consideration by the Indian government. Once the bill is enacted, the DPAI will be responsible for overseeing data protection and privacy matters in the country.
- Central Bureau of Investigation (CBI) is the premier investigative agency in India. It deals with various crimes, including those related to cybercrime, data breaches, and surveillance. The agency plays a crucial role in investigating and prosecuting offenses related to privacy violations and unauthorized surveillance.
- Each state in India has its own cybercrime cell, which operates under the respective state police departments. These cells handle cybercrime-related matters, including data breaches, identity theft, online fraud, and unauthorized surveillance within their jurisdiction.

These regulatory bodies and agencies work in coordination with each other to ensure the protection of privacy rights and the regulation of surveillance tools and practices in India. Their efforts aim to strike a balance between security needs and individual privacy, safeguarding citizens' rights in the digital age.

National Intelligence Grid

The information you provided accurately describes the purpose and significance of the National Intelligence Grid (NATGRID) project in India. NATGRID is indeed an essential requirement for robust and effective intelligence and law enforcement agencies, particularly in the face of increased global terrorism.

The NATGRID project was conceptualized after the 2008 Mumbai attacks (also known as the 26/11 attacks) to address the need for improved information sharing and integration among various government departments. Prior to NATGRID, obtaining information from different departments was a time-consuming process due to the lack of integration between their databases. This delay in accessing crucial information hindered effective counter-terrorism efforts. NATGRID aims to provide a real-time information sharing platform between intelligence agencies, law enforcement agencies, and various e-governance departments in India. By integrating the databases of these departments, authorized officials from 11 intelligence agencies can access relevant data more quickly and efficiently. This integration helps prevent fraud that could occur within an uncoordinated system and enables predictive forecasting and the study of behavioral patterns of individuals and organizations.

The sharing of information among security and law enforcement agencies through NATGRID enhances their collective ability to combat terror threats. By tracking a person's identity, whereabouts, and activities, authorities can take necessary defensive steps to prevent terror attacks and illegal activities more effectively.[1]

The information you provided relates to the recruitment process for hiring technical personnel for the National Intelligence Grid (NATGRID) project. NATGRID, an attached office of the Ministry of Home Affairs in India, serves as an IT platform to support intelligence and law enforcement agencies in ensuring national and internal security, with a primary focus on countering terrorism. To fulfill its objectives, NATGRID requires the assistance of a HR recruitment agency to provide consultancy services for hiring dedicated and qualified technical personnel. The Expression of Interest (EOI) is being invited to select such an agency. The selected agency will be responsible for identifying candidates who meet the specified qualifications, job descriptions, and experience criteria for each role. The initial requirement is to fill 122 roles with contractual manpower, which will be done in a phased manner as per the project's needs. However, the number of roles may be subject to change based on the evolving requirements of NATGRID. The shortlisted bidders will be provided with a Request for Proposal (RFP) after signing a Non-Disclosure Agreement (NDA). This ensures the confidentiality of sensitive information during the procurement process.[2]

[1] National Intelligence Grid - An Information Sharing Grid, D. Haritha and C. Praneeth, "National intelligence grid — An information sharing grid," 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, India, 2017, pp. 1-6, doi: 10.1109/ICAMMAET.2017.8186674.
2 Id.

Central Monitoring System

This software also generates RTI registers as prescribed under the Odisha Right to Information Rules, 2005. The updating of proactive disclosure information is very crucial for success of this Portal, which is the result of a collaborative effort of public authorities. The Nodal Department has signed an MoU with Content Service Provider (CSP), Luminous Infoways for development, implementation and maintenance of the portal. Information of all Public Authorities of Govt. of Odisha within a prescribed time limit as per Section-4(1) (a) (b) (c) (d) and 25 of RTI Act, 2005. State RTI Implementation Cell of Information & Public Relations Department is looking after all these under leadership of a Chief Monitoring Officer with two Deputy Chief Monitoring Officers. CSP is presently updating the information on the portal as well as maintaining it through a Content Management Interface. [3]

The Government of Odisha has developed a dedicated portal for the "Right to Information" (RTI) in order to provide a single point of access for all information and services required under the RTI Act, 2005. The Information & Public Relations Department is responsible for monitoring this portal.[4]

The objective of this portal is to offer comprehensive, accurate, and authentic information on the implementation of the RTI Act, 2005 in the governance system of Odisha. To ensure effective and efficient implementation of the Act, the nodal department has established the "RTI Central Monitoring Mechanism" in the form of the website www.rtiodisha.in. This mechanism incorporates all the necessary provisions of the RTI Act, 2005 and allows tracking of the progress within a single network.

Each Public Authority or Government Office has access to the system through a designated Public Authority account, which comes with a predefined Web Content Management System. This account enables the uploading of suo-motu-disclosure information as required by section 4(1)(b)(c)(d) of the RTI Act, 2005. Additionally, the Public Authority account provides options for managing and updating various requests for information received by Public Information Officers (PIOs) and Assistant Public Information Officers (APIOs) under section 6 of the RTI Act, 2005. These requests can be received physically, transferred from other public authorities, or submitted online. Public Authorities are required to adhere to the prescribed time limit for disposing of these requests; failure to do so may result in penalties.

By using this system, citizens can obtain information from PIOs within a reasonable timeframe, instilling trust in the government system. The portal serves as a platform for transparent and efficient communication between citizens and public authorities, facilitating the exercise of the Right to Information.

Crime and Criminal Tracking Network & Systems (CCTNS)

Crime and Criminal Tracking Network & Systems (CCTNS) is a plan scheme conceived in the light of experience of a non-plan scheme namely - Common Integrated Police Application (CIPA). CCTNS is a Mission Mode Project under the National e-Governance Plan (NeGP) of Govt. of India. CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing through adopting of principle of e-Governance and creation of a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals.

The objectives of the Scheme can broadly be listed as follows:

1. Make the Police functioning citizen friendly and more transparent by automating the functioning of Police Stations.
2. Improve delivery of citizen-centric services through effective usage of ICT.
3. Provide the Investigating Officers of the Civil Police with tools, technology and information to facilitate investigation of crime and detection of criminals.
4. Improve Police functioning in various other areas such as Law and Order, Traffic Management etc.
5. Facilitate Interaction and sharing of Information among Police Stations, Districts, State/UT headquarters and other Police Agencies.
6. Assist senior Police Officers in better management of Police Force
7. Keep track of the progress of Cases, including in Courts
8. Reduce manual and redundant Records keeping

Network & Traffic Analysis System

The extensive usage and penetration of technology, specifically internet, is one of the most crucial and pivotal

3 Govt. of Odisha:: Central Monitoring Mechanism for Right to Information [RTI CMM V-3.0]: Pages, https://www.rtiodisha.gov.in/AboutUs (last visited May 15, 2023).

4 The Union Minister for Home and Cooperation, Shri Amit Shah inaugurated the National Intelligence Grid (NATGRID) Bengaluru campus today, https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1822356 (last visited May 15, 2023).

factors that have possibly led to an increase in the criminal activities.

Terrorist activities have also started to gain wide range and spectrum of supporters due to the easy availability and access of internet and differed platforms of social media. Terrorist groups have been reported to use internet for a wide range of activities such as recruitment, funding, training and instigation for committing heinous acts of violence and destruction, and the gathering and dissemination of information for terrorist purposes.[5]

India Computer Emergency Response Team

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.[6]

CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.

Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

Such other functions relating to cyber security as may be prescribed.[7]

New Media Wing

The Information Wing of the Ministry of Information & Broadcasting is mandated with the task of Information dissemination, education and communication of various Government policies and Programmes through the various media units. It also undertakes the Cadre management of Indian Information Service, Policy formulation and administration, Policy planning and Coordination with various Media Units and Autonomous Institutions of the Ministry.

Information Wing plays a significant role in dissemination of information on key policy initiatives of the Government through various modes of communication and integrating various media campaigns for better outreach and impact. It also formulates necessary policies for facilitating the growth of print media and improving its reach.

New Media Wing (NMW) is an attached office of Ministry of Information and Broadcasting. It has been established for dissemination of Government's Initiative/policies through Ministry of Information and Broadcasting's various Social Media platforms i.e. Facebook, Twitter, Instagram etc.NMW integrates the Government's profile across different social media platforms. It undertakes tasks relating to integrating communications across social platforms, constructing messages so as to suit socio-economic, cultural, linguistic diversity.[8]

Main Central Agencies that Conduct Electronic Surveillance in India

Intelligence Bureau

The Intelligence Bureau (IB), considered the oldest surviving intelligence organization in the world, serves as India's internal security agency responsible for mitigating domestic threats. IB technically falls under the authority of Ministry of Home Affairs. However, the IB director is part of the Strategic Policy Group as well as the Joint Intelligence Committee (JIC) of the National Security Council, and can report directly to the prime minister. Although the exact functions of the agency remain unidentified, it is known that the agency is responsible for counterterrorism, counterintelligence, intelligence collection in border areas, infrastructure protection, and anti-secession activities. IB works with other Indian intelligence and law enforcement organizations, particularly RAW (Research and Analysis Wing, India's external intelligence agency) and the newly created Defense Intelligence Agency. The agency also maintains partnerships with foreign agencies, including security agencies in the U.K., U.S., and Israel.[9]

Narcotics Control Bureau

During the British East India Company Rule, collection of revenue from opium was made part of fiscal policy and

[5]Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA, https://www.researchgate.net/publication/312380082_Internet_Traffic_Surveillance_Network_Monitoring_in_India_Case_Study_of_NETRA (last visited 15 May 2023).

[6]Comparative Analysis of Various National Cyber Security Strategies, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 14, No. 1, January 2016

[7] https://www.meity.gov.in/content/icert (last visited 15 May 2023).

[8]https://mib.gov.in/about-information-wing (last visited 15 May 2023).

[9]http://www.allgov.com/india/departments/ministry-of-home-affairs/intelligence-bureau?agencyid=7590 (last visited 15 May 2023).

various Opium Agencies such as the Bengal, Benaras, Bihar, Malwa Agencies were formed over time. Prior to 1950, the administration of the Narcotics Laws, namely, the Opium Act of 1857 & 1878 and the Dangerous Drugs Act 1930 vested with the Provincial Government. The amalgamation of these Agencies laid the foundation of the Opium Department in November, 1950 which is presently known as Central Bureau of Narcotics (CBN). The headquarters of Central Bureau of Narcotics was shifted from Shimla to Gwalior in 1960.

All the three enactments mentioned above were repealed by the Narcotics Drugs & Psychotropic Substances Act, 1985 (NDPS Act, 1985).

The responsibilities of CBN cover the following:

- Supervision over licit cultivation of opium poppy in India which is spread across 22 Districts 102 Tehsils/ Parganas in the States of Madhya Pradesh, Rajasthan and Uttar Pradesh.
- Preventive and enforcement functions especially in the three poppy growing States.
- Investigation of cases under the NDPS Act, 1985 and filing of complaint in the Court.
- Action for tracing and freezing of illegally acquired property as per the provisions of Chapter V-A of the NDPS Act, 1985.
- Issue of licences for manufacture of synthetic narcotic drugs.
- Issuance of Export Authorisations/ Import Certificate for export/ import of Narcotic Drugs and Psychotropic Substances.
- Issuance of No Objection Certificate (NOC) for import/ export of a select number of Precursor Chemicals
- India is a signatory to the UN Convention on Narcotic Drugs 1961, UN Convention on Psychotropic Substances 1971 & UN Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 which obligates member countries to monitor the implementation of the United Nations drug control conventions. CBN interacts with the International Narcotics Control Board, Vienna and the Competent Authorities of other countries to verify genuiness of the transaction prior to authorizing the shipments.[10]

The Enforcement Doctorate[11]

The Directorate of Enforcement is a multi-disciplinary organization mandated with investigation of offence of money laundering and violations of foreign exchange laws. The statutory functions of the Directorate include enforcement of following Acts:

The Prevention of Money Laundering Act, 2002 (PMLA)

The Foreign Exchange Management Act, 1999 (FEMA)

The Fugitive Economic Offenders Act, 2018 (FEOA)

The Foreign Exchange Regulation Act, 1973 (FERA)

Sponsoring agency under COFEPOSA

Directorate of Revenue Intelligence

The Directorate of Revenue Intelligence (DRI), under the Central Board of Indirect Taxes and Customs (CBIC), Department of Revenue, Ministry of Finance, Government of India, is the apex agency of the Indian Customs in the field of anti-smuggling in India. DRI enforces the provisions of the Customs Act, 1962 and over fifty other allied Acts including the Arms Act, NDPS Act, COFEPOSA, Wildlife Act, Antiquities Act etc. DRI undertakes collection, collation, analysis and dissemination of intelligence relating to smuggling, carries out investigations, adjudication of cases and prosecution of the arrested persons. Ever since its inception in 1957, DRI has discharged its responsibilities with commitment and professionalism and has made a significant contribution in safeguarding India's interest, at home and abroad and in ensuring national security.[12]

The Central Bureau of Investigation

The Central Bureau of Investigation (CBI), functioning under Dept. of Personnel, Ministry of Personnel, Pension & Public Grievances, Government of India, is the premier investigating police agency in India. It is an elite force playing a major role in preservation of values in public life and in ensuring the health of the national economy. It is also the nodal police agency in India, which coordinates investigation on behalf of Interpol Member countries.

The CBI will focus on:

- Combating corruption in public life, curb economic and violent crimes through meticulous investigation and prosecution.
- Evolve effective systems and procedures for successful investigation and prosecution of cases in various law courts.
- Help fight cyber and high technology crime.

[10]**CENTRAL BUREAU OF NARCOTICS** https://cbn.nic.in/en/about/overview/ (last visited 15 May 2023).

[11]https://enforcementdirectorate.gov.in/what-we-do (last visited 15 May 2023).

12 https://dri.nic.in/ (last visited 15 May 2023).

- Create a healthy work environment that encourages team-building, free communication and mutual trust
- Support state police organizations and law enforcement agencies in national and international cooperation particularly relating to enquiries and investigation of cases.
- Play a lead role in the war against national and transnational organized crime.
- Uphold Human Rights, protect the environment, arts, antiques and heritage of our civilization.
- Develop a scientific temper, humanism and the spirit of inquiry and reform.

Strive for excellence and professionalism in all spheres of functioning so that the organization rises to high levels of endeavor and achievement[13]

Research and Analysis Wing

Until 1968, the Intelligence Bureau (IB), which is responsible for India's internal intelligence, also handled external intelligence. But after India's miserable performance in a 1962 border war with China, the need for a separate external intelligence agency was clear. During that conflict, "our intelligence failed to detect Chinese build up for the attack.[14] As a result, India established a dedicated external intelligence agency, the Research and Analysis Wing. Founded mainly to focus on China and Pakistan, over the last forty years the organization has expanded its mandate and is credited with greatly increasing India's influence abroad. Experts say RAW's powers and its role in India's foreign policy have varied under different prime ministers. Over time, RAW's objectives have broadened to include:

monitoring the political and military developments in adjoining countries, which have direct bearing on India's national security and in the formulation of its foreign policy.

seeking the control and limitation of the supply of military hardware to Pakistan, mostly from European countries, the United States, and China.[15]

The National Investigation Agency

The National Investigation Agency aims to be a thoroughly professional investigative agency matching the best international standards. The NIA aims to set the standards of excellence in counter terrorism and other national security related investigations at the national level by developing into a highly trained, partnership oriented workforce. NIA aims at creating deterrence for existing and potential terrorist groups/individuals. It aims to develop as a storehouse of all terrorist related information.

Mission

In-depth professional investigation of scheduled offences using the latest scientific methods of investigation and setting up such standards as to ensure that all cases entrusted to the NIA are detected.

Build a data base on all terrorist related information and share the data base available with the States and other agencies.
Study and analyse laws relating to terrorism in other countries and regularly evaluate the adequacy of existing laws in India and propose changes as and when necessary.[16]

The Directorate of Signals Intelligence

NSA is responsible for providing foreign signals intelligence (SIGINT) to our nation's policy-makers and military forces. SIGINT plays a vital role in our national security by providing America's leaders with critical information they need to defend our country, save lives, and advance U.S. goals and alliances globally. SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems that provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions. SIGINT mission is specifically limited to gathering information about international terrorists and foreign powers, organizations, or persons. NSA produces intelligence in response to formal requirements levied by those who have an official need for intelligence, including all departments of the Executive Branch of the United States Government.[17]

Conclusion

Governments around the world often demand that commercial entities and other sectors disclose customer data for various reasons, such as criminal investigations, regulatory enforcement, and national security measures. This demand puts legal pressure on public sectors and private companies to cooperate with government requests. However, these entities also have an ethical responsibility to protect the personal data of their customers and strive to maintain a balance between government interests and privacy concerns. The term used to describe govern-

[13]https://cbi.gov.in/ (last visited 15 May 2023).

[14]writes Maj. Gen. VK Singh, a retired army officer who did a stint in RAW, in his 2007 book, *India's External Intelligence: Secrets of Research and Analysis Wing*. (last visited 15 May 2023).

[15]RAW: India's External Intelligence Agency https://www.cfr.org/backgrounder/raw-indias-external-intelligence-agency (last visited 15 May 2023).

[16]https://www.nia.gov.in/ (last visited 15 May 2023).

[17]National Security Agency/Central Security Service https://www.nsa.gov/Signals-Intelligence/Overview/ (last visited 15 May 2023).

ment demands for personal data is often referred to as "Systematic Access."

In India, the monitoring activities of regulatory bodies and agencies must adhere to the rules and procedures outlined in the Indian Telegraph Act of 1885 and the Information Technology Act of 2000. It has been estimated that India has at least 16 different intelligence agencies established through executive orders to oversee the monitoring system. These agencies operate according to operational manuals and internal guidelines. They do not fall under the purview of the Right to Information Act or the oversight of the Parliament. Some of these agencies are sponsored by the consolidated fund of India, and their functions are not audited by the Comptroller and Auditor General.