LAW REFORMS FOR DATA PROTECTION IN INTERNET OF THINGS

Sabrina Bath
Junior Research Fellow, Ph.D. Scholar, Symbiosis Law School, Pune, India, Symbiosis International (Deemed University)

Dr. Amol Sapatnekar
Assistant Professor, Symbiosis Law School, Pune, India, Symbiosis International (Deemed University)

***Corresponding Author:** Sabrina Bath
*JRF, Symbiosis Law School, Pune, India, Symbiosis International (Deemed University)
sabrina.bath@symlaw.ac.in

Abstract

Internet of Things has altered the ways in which data can be collected and processed. With the increasing usage of IoT devices, threats to user privacy and data security such as data theft, data breach, malware have increased. Securing IoT and its supporting systems is becoming crucial in the backdrop of their data collection and potential data processing capabilities. Regarding data protection, risk sharing and breach of liability among the parties involved in the Internet of Things such as device manufacturers, network providers, application developers, regulators, standard organizations and the end users, there are significant legal challenges associated with data security and user privacy. The major issues associated with IoTs include the possibility of unauthorized access of data, the use of personal data for commercial gains and threat to user privacy. These issues require careful attention as IoT devices produce and use a huge amount of personal data, some of which is particularly sensitive (such as private medical information). In consideration of the same, this article looks at the legal implications of the current regulations governing data protection. The authors also analyse whether the Indian legal framework for data protection potentially incorporates the regulating capacities given that the IoTs have the ability to change the paradigm of data collection and processing. Therefore, this article highlights the need to examine whether the data collection through IoTs is covered under the current data protection framework. This article aims at understanding the concept of Internet of Things and the kind of data collected by IoT devices followed by the potential threats to user privacy and data security. The study undertakes an exploratory and comparative approach in analysing the IoT scenario/ dynamics.

Keywords: data protection, data privacy, Internet of Things, law reform, personal data, user privacy.

INTRODUCTION

The term "Internet of Things" (IoT) was used for the very first time in 1999 by Ashton, a member of the RFID development community.[1] With the recent advancements in mobile technology, embedded and ubiquitous connectivity, cloud computing and data analytics, the practical relevance of the IoT sector has increased to a great extent.[2] Even though the phrase "Internet of Things" is used in many different settings, it is generally understood to refer to a network of physical items that are equipped with sensors, software and network connectivity in order to collect and share data.[3] Then, using this data, many processes can be automated and optimized, increasing their effectiveness and efficiency. The IoT sector covers a wide range of devices and applications extending from the consumer sector to the industrial sector where IoTs are incorporated in machinery and substantial infrastructure like smartphones and smart homes to industrial machinery, etc.[4] This allows data to be sent between a wide variety of gadgets and devices without a computer or human-to-computer interface.[5] The goal of the IoT sector is to connect billions of devices to public or private Internet Protocol (IP) networks so they can detect, communicate and share information.

During the recent years, IoTs have experienced an increasing demand owing to its fast expansion, commercial availability, improved accessibility, scalability and interoperability. The IoT market has also developed tremendously with the number of heterogeneous devices estimated to have reached 28 billion by the end of 2020. [6] The development of the IoT sector can be seen in the recent times where the consumers are becoming more interested in the idea of 'smart homes', which offer greater security and energy efficiency owing to the emergence of IoT devices including Internet-enabled appliances, home automation components and energy management gadgets. Other personal IoT devices, such as wearable fitness and health monitoring devices and network-enabled medical equipment, are altering how healthcare services are delivered. A significant amount of data is produced through the IoT sector by smart cities, manufacturing companies, health institutions and government sector, among other sources.[7] According to recent estimates, smart connected devices would analyse 80% of all data by 2025.[8]

[1] Thorsten Kramp et al. *Enabling Things to Talk* (2013).

[2] Esraa Mohamed, *The Relation of Artificial Intelligence with the Internet of Things: A Survey*, 1(1) JCIM. 30-34 (2020).

[3] S. Kumar et. al., *Internet of Things is a revolutionary approach for future technology enhancement: A review,* 6 J Big Data 111 (2019).

[4] Javid Mohd et al., *Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT)*, 2 Sensors International (2021).

[5] Ruth Ande et. al., *Internet of Things: Evolution and Technologies from a Security Perspective,* 54 Sustainable Cities and Society (2020).

[6] Thamer A. Rousan, *The Future of Internet of Things*, 4(1) IJCCIE (2017).

[7] S. Syed et. al., *IoT in Smart Cities: A survey of Technologies, Practices and Challenges*, 4 Smart Cities, 429- 475 (2021).

[8] Bardia Safaei, et. al., *Reliability Side-Effects in Internet of Things Application Layer Protocols*, in proceedings of the International Conference on System Reliability and Safety (2017).

A tremendous amount of data is exchanged between the IoT devices and its users as soon as these devices communicate with each other. With its increased use in our day to day life, it is easier to track the activity of individuals at any time and from any location. This has led to the emergence of new security threats and challenges across all industries and sectors where IoTs have been employed.[9] A few examples of IoT connected devices are mobile GPS devices, fitness trackers, cell phones, tablets, smart automobiles, smart TVs, to name a few. Since all such devices continuously collect data from its users, the users do not have complete control over the data that is being collected through such devices and how the data collected is being used. These devices frequently collect data related to geographic location, biometric data, financial data, medical data, sensor data and user data such as individual purchasing patterns, etc.[10] Given the huge volume of data that is being collected and exchanged, there is a high risk of a data security breach as hackers are continuously working to compromise these systems. Depending on how the data gathered from IoT devices is utilized and shared, IoT has the potential to violate the right to privacy of the users in a number of ways through surveillance, data gathering, data sharing and a lack of transparency on the purposes for which data is acquired. In this article, the authors focus on understanding the concept of Internet of Things and the kind of data collected by IoT devices followed by the potential threats to user privacy and data security. Looking at the legal challenges pertaining to user privacy and data security in the IoT sector, it is important to look at the existing legal framework for data protection and user privacy and ascertain if they provide sufficient protection in relation to user data generated by IoT devices and applications. Data protection laws in five jurisdictions, namely the EU, USA, Brazil, China and India have been discussed to compare the legal framework for personal data protection in the IoT sector in these jurisdictions with India. The comparative analysis has been done to understand the legal lacunae in the Indian legal framework and give recommendations on how India can develop a better legal framework for user privacy and data protection in the IoT sector after analysing the current international best practices.

MEANING AND DEFINITION OF INTERNET OF THINGS

Kevin Ashton, a specialist in digital innovation, has been credited with the coining of the phrase “Internet of Things”.[11] Till date, there is no universally accepted definition of Internet of Things. Various efforts have been made by numerous experts, including academicians, practitioners, developers, researchers and innovators to define the same.[12] All of the definitions given by the experts agree on the basic tenet that the first iteration of the Internet dealt with data produced by people, whereas the second iteration dealt with data produced by things. The best

[9] Phillip Williams et. al., *A survey on security in internet of things with a focus on the impact of emerging technologies*, 19 Internet of Things (2022)

[10] *Id.*

[11] Thorsten 2013.

[12] Somayya Madakam et. al., *Internet of Things (IoT): A Literature Review*, , 3(5) Journal of Computer and Communications 164-173 (2015).

way to describe the Internet of Things is as "an open and extensive network of intelligent devices that have the capability to auto-organize, share information, data and resources with one another."[13] Such devices are all connected, that communicate and share data based on predetermined protocols to achieve smart organization, control and even personal real-time online monitoring.[14]

Internet of Things as defined by the Pew Research Centre is "a catchall phrase for the multitude of gadgets, appliances, cars, wearable material and sensor-laden portions of the environment that connect to each other and pass data back and forth."[15]

IoT has been defined in a number of ways throughout the literature reflecting debates relating to the etymology of the term. While the term 'Internet' alludes to a virtual network-oriented view of technology, 'Things' emphasize the items that can be put into a technological framework.[16] There is a need to move beyond just a technological perspective and redefine the IoT sector as a global infrastructure linking both physical and digital devices.[17] The IoT network helps the devices to communicate with one another and provide useful services to its users automatically.[18] IoT can be described as "intelligent interfaces that are used by virtual and physical 'Things' as part of a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols."[19] These 'Things' have virtual personalities, identities and physical traits through which they can be easily integrated into the information network. Such interconnection of the actuating and sensing devices allows the data to be shared through an unified network across various platforms.[20] This facilitates connection between the things and its

[13] Brend W. Wiltz et. al., *An Integrative Public IoT Framework for Smart Government*, 36(2) Government Information Quarterly (2019).

[14] M. Kheirkhahan et al., *A smartwatch-based framework for real-time and online assessment and mobility monitoring*, 89 Journal of Biomedical Informatics 29-40 (2019).

[15] Lee Raine et al., *The Internet of Things Connectivity Binge: What are the Implications?*, Pew Research Centre, Washington, DC (2017).

[16] Madakam et al. 2015.

[17] B. Dorsemaine et. al., *Internet if Things: A definition and taxonomy* (2015), in proceedings of the 9th International Conference on Next Generation Mobile Applications (2015),

[18] Daniele Miorandi et al., *Internet of things: Vision, applications and research challenges*, 10(7) Ad Hoc Networks 1497-1516 (2012).

[18] Gubbi et al., *Internet of Things (IoT): A vision, architectural elements and future directions,* 29 Future Generation Computer Systems, 645-1660 (2013).

[19] R.V. Kranenburg, *The Internet of Things. A critique of ambient technology and the all-seeing network of RFID,* 2 Institute of Network Cultures (2007).

[20] Gubbi et al. 2013.

users at anytime and anywhere with anyone and anything.[21] Thus, it can be said that IoT is a group of networks that link varied objects and allows for the access and management of data.[22]

Furthermore, it is important to understand the key differences between a computer and an IoT device before discussing the legal, user and data protection issues related to the IoT sector. The Information Technology Act, 2000 defines a computer as "an electronic device that may be programmed to take in raw data as input, process it using a set of instructions (a program), and output the result"[23]. Whereas, IoT devices are physical objects integrated with sensors, software and network connectivity to collect, exchange and process user data. They are also known as connected or smart devices. These gadgets frequently have specialized features and are made for certain specific uses. It includes a wide variety of devices such as wearable technology, environmental monitoring equipment, industrial sensors, smart home appliances, etc. These devices frequently have internet or other network connections, allowing them to interact with other devices, send information to centralized servers, or start operations based on the data acquired. Such devices are made expressly for connection, allowing them to communicate with other IoT devices and centralized systems by transmitting data over the internet or other networks.

The primary differences between computer devices and IoT devices mostly relate to the connectivity, real-time requirements, data sources and the volume of data collected. IoT devices, in contrast to computer devices, which are generally user-centric, are made to gather, share and interpret data from real environments. The data collected by the IoT sector is regularly gathered, analysed and used to drive action by these interconnected devices which offers an extensive amount of data for planning, management and decision-making. The data shared through IoT devices allows them to identify themselves and acquire intelligence by making or facilitating context-related decisions. The types of data that IoT devices collect depends on the particular applications they are used for and the sensors they are equipped with.[24] The data collected through IoT devices can be categorised as real time data which allows for instantaneous generation and transmission of data by using internal sensors or external inputs to gather data about their surroundings.

LEGAL CHALLENGES TO USER PRIVACY AND DATA PROTECTION CONCERNS IN THE IOT SECTOR

IoT has been developing over time with the aim to give its users efficient ways to engage and communicate. This has benefited numerous individuals and businesses. IoT is a cutting-edge and significant phenomena, but it needs to take into account the legal implications of the data

[21] Charith Perera et al., *The emerging Internet of Things marketplace from an industrial perspective: A survey*, 3 IEEE Trans. Emerg. Top. Comput., 585-598 (2015).

[22] Dorsemaine et al. 2015.

[23] S. 1(j) of The Information Technology Act of 2000 (Jun. 15, 2023), available at https://www.meity.gov.in/writereaddata/files/itbill2000.pdf.

[24] Yusuf Perwej et. al., *The Internet of Things (IoT) and its Application Domains,* 182(49) IJCA 36-49 (2019).

protection laws. This sector has been exposed to various dangers and weaknesses as it continues to grow and expand. Some of the notable issues related to the IoT sector are data protection, security and user privacy concerns. Personal data is of utmost importance to an individual. The expansion of the IoT sector allows for different types of personal data to be collected as well as an overall increase in the quantity of data gathered. Therefore, it is essential to address these issues to ensure user trust and security as IoT devices become more widespread in our daily lives and gather and exchange enormous amounts of personal data.

The phrase "Internet of Things" covers a wide variety of continually developing technology and applications, but it lacks a clear legal definition as discussed above. Owing to which it is difficult to determine its exact scope and subsequent data classification. Some legal regulations apply to IoT devices indirectly through the already developed data protection laws. In India, the Information Technology Act, 2000 was passed with the main goals of addressing problems with cybersecurity, data security and electronic transactions.[25] Although it was crucial in creating a legal framework for data protection and e-commerce. But it is insufficient in handling the particular difficulties and complexities that the IoT sector presents. Looking at the data security and user privacy issues in relation to the IoT sector, it is important to look at the current legal framework for data protection and user privacy in India. It is also necessary to see whether the same applies to the IoT sector or not.

In the Indian context, the IT Act's scope is not that broad as it is related to 'data' on the internet rather than data in relation to the IoT sector. The lack of clarity regarding the capabilities and restrictions of IoT to safeguard both customers and service providers is troublesome. IoT usage is promoted by India's Ministry of Electronics and Information Technology (MeitY) to the extent that it examined the potential application of IoT in Indian legal system without offering even the most fundamental principles or laws to control undesirable circumstances and problems associated with it.[26] IoT devices and applications are not specifically governed by laws or regulations in India. However, there may be some protection and oversight provided for certain IoT components within the current rules and regulations, which is not comprehensive in nature. At present, India is one of the few countries in the world that does not have a strong legal framework for data protection, and this is also true for the IoT sector. The government must move swiftly to create a framework that would bring India on an equal footing in the international arena given the growing use of IoT devices.

LEGAL FRAMEWORK FOR DATA PROTECTION IN THE IOT SECTOR

1. Indian legal framework

[25] The Information Technology Act of 2000 (Jun. 15, 2023), available at https://www.meity.gov.in/writereaddata/files/itbill2000.pdf.

[26] Draft Policy on Internet of Things, 2015 (Jun. 20, 2023), available at https://www.meity.gov.in/content/internet-things.

At present, India does not have a comprehensive law that governs the collection and utilization of personal data by the IoT devices. Some of the laws that cover data protection in India are discussed below:

1.1 The Information Technology Act, 2000[27] and the Reasonable Practices and Procedures and Sensitive Personal Data or Information Rules of 2011[28]

The Information Technology Act, 2000[29] and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[30] serve as a nation-wide regulatory framework for data protection and privacy. There are not many comprehensive provisions in the IT Act for data protection for the IoT sector and it only addresses crimes involving personal data.[31]

1.2. Digital Personal Data Protection Act, 2023[32]

In contrast to an earlier cumbersome drafts of data protection bills, the new Digital Personal Data Protection Act, 2023[33] is more narrowly focused on personal data that is collected both online and offline. The Bill has been revised to include stiff penalties for non-compliance, however these penalties are limited. The Act broadens the purview of the proposed law by attempting to regulate both personal and non-personal data. The proposed Bill is grounded in the Apex Courts' ruling in KS Puttaswamy v. Union of India[34], which stated that anything which restricts an individuals' right to privacy must be sanctioned by law and should include procedural safeguards for the same.

1.3. Draft IoT Policy, 2015[35]

A draft of the "Internet of Things Policy" was released by the Indian government in 2015 to encourage the creation of IoT-based technologies, primarily to meet Indian IoT criteria.[36] Eight

[27] The Information Technology Act, 2000

[28] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[29] The Information Technology Act, 2000.

[30] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[31] Section 43 A, Section 72 and section 72 A of The Information Technology Act, 2000 (Jun. 20, 2023), available at https://www.meity.gov.in/writereaddata/files/itbill2000.pdf.

[32] The Digital Personal Data Protection Act, 2023 (Jun. 20, 2023), available at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[33] *Id.*

[34] KS Puttaswamy v. Union of India (2017) 10 SCC 1.

[35] Draft Policy on Internet of Things, 2015.

[36] *Id.*

years since the policy was published, no attempt for has been made to develop a regulatory framework for the IoT sector, despite the technology's widespread adoption.

1.4. Code of Practice for Securing Consumer Internet of Things[37]

It was introduced as a best practice for safeguarding IoT devices in accordance with international standards and best practices. It will help to secure the consumer IoT ecosystem and devices while also mitigating risks.

2. International Legal Framework

2.1. European Union

2.1.1. General Data Protection Regulation (GDPR)[38]

GDPR is EU'S central law for data protection, highlighting the need for uniformity in data protection laws. It is focused on the needs of the consumers and has codified the privacy by design school of thought.[39] It is well written and brought all the members of the year-round agreement with one another over the need to preserve citizen data and privacy.

2.1.2. EU e-Privacy Regulations[40]

The present e-Privacy Directive has been replaced by the new EU regulation known as the e-Privacy Regulation. By granting people more control over their personal data, it strengthens their rights to online privacy. Additionally, it places stronger regulations on businesses that gather or use this data.[41]

2.1.3. EU Cybersecurity Act[42]

Cyber security certification programs for ICT and IoT businesses across Europe have been developed to govern different cybersecurity laws between countries. IoT firms will be categorized utilizing a single set of certification requirements that will range from basic to significant to high, depending on how secure they are. The use of the Internet of Things by businesses is subject to a variety of regulations based on their degree of certification, provided by the European Commission.

[37] Code of Practice for Securing Consumer Internet of Things, 2021, (Jun. 25, 2023), available at https://www.tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf.

[38] EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

[39] *Id.*

[40] IT Governance UK. The EU ePR (ePrivacy Regulation), 2022.

[41] *Id.*

[42] EU Cybersecurity Act 2019/881.

2.1.4. Cyber Resilience Act[43]

It has enacted stricter cybersecurity restrictions for the IoT sector that include severe penalties for manufacturers and software developers who fail to follow the new laws. It aims to set common security standards for connected services and devices.

2.2. USA

The US has developed a sectoral strategy that combines law, regulation and self-regulation. There is no central federal data privacy and security law, instead there are different industry or age focused vertical legislations. State level laws are introduced to overcome the absence of a federal legislation to regulate internet based operations. Eg.- California Consumer Privacy Act (CCPA)[44] focusing on ensuring consumers data privacy on the internet. Efforts are also being made to introduce a federal data privacy law in the US. Eg.- Consumer Data Privacy and Security Act, 2021[45]

2.2.1. IoT Cybersecurity Improvement Act, 2020[46]

It is the first federal statute addressing the security of IoT devices. It seeks to make the IoT devices more secure by linking the IoT devices owned or managed by an agency to a government information system.

2.3. Brazil

2.3.1. General Data Protection Law (Lei Geral de Proteço de Dados, or LGPD)[47]

It is a new privacy regulation which became effective in Brazil on 16 August, 2020.[48] The LGPD is a comprehensive privacy law that offers stern safeguards for the personal information of Brazilian residents and citizens.[49]All entities that handle the personal data of Brazilian citizens and residents must comply with the LGPD.

2.3.2. Brazilian National Plan for the Internet of Things[50]

[43] Regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020.

[44] California Consumer Privacy Act (CCPA), 2018 (Jun. 20, 2023), available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[45] Consumer Data Privacy and Security Act, 2021 (Jun. 25, 2023), available at https://www.congress.gov/bill/117th-congress/senate-bill/1494.

[46] IoT Cybersecurity Improvement Act, 2020.

[47] General Data Protection Law.

[48] *Id.*

[49] General Data Protection Law.

[50] Brazilian National Plan for the Internet of Things.

It is a sector-specific action plan.[51] It was created as a government initiative to encourage the growth of the IoT sector in Brazil.[52] It refers to a set of legislative initiatives and strategies designed to promote the use of Internet-connected devices in Brazilian government, educational institutions and business.

2.4. China

2.4.1. Data Security Law (DSL)[53] & Personal Information Protection Law (PIPL)[54]

These laws aim at protecting the public interest and national security. The PIPL protects the rights and interests of the individuals while handling private data. These laws also provide implementation guidelines for numerous legislative agencies and regulatory authorities.

2.4.2. Guidelines for Building Basic Security Standard System for the Internet of Things ("Draft"), 2021[55]

It aims to provide a framework that will facilitate the creation and implementation of IoT standards. The development of a security standard system for the Internet of Things has been outlined in recommendations published by China's Ministry of Industry and Information Technology.[56]

COMPARATIVE ANALYSIS

European Union

In Europe, privacy and data protection are mainly credited with the commercial feasibility of IoTs. Owing to the low level of security for the IoT devices, the lawmakers introduced regulations on the lines of the GDPR,[57] such as the Cybersecurity Act[58]. A large number of IoT devices are geographically and materially covered by the GDPR owing to its vast geographic extent. It also focuses upon the concept of privacy by design which suggests that when a product is being produced, the data controller must take organizational and technical measures to secure personal data.[59] The Cybersecurity Act establishes a framework for a European cybersecurity certification

[51] *Id.*

[52] Brazilian National Plan for the Internet of Things.

[53] Data Security Law of the PRC, 2021.

[54] Personal Information Protection Law of the PRC, 2021.

[55] Guidelines for Building Basic Security Standard System for the Internet of Things ("Draft"), 2021.

[56] *Id.*

[57] EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

[58] EU Cybersecurity Act 2019/88.

[59] EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

for ICT products, services and processes.[60] The scope of the law would extend to IoT devices only if they are categorized as ICT devices.[61] EU greatly emphasizes the fundamental right to privacy. The protection of EU citizens' rights to privacy in a society centred around the internet was regarded by EU legislators to require a more stringent legislation. As a result the e-Privacy regulations were designed to keep up with changes of a fast developing technological sector. As compared to the GDPR, which governs data security, the new e-Privacy regulations will control the confidentiality of communications. These regulations will focus upon the privacy of electronic communications by making end user permissions mandatory as well as general internet user surveillance. The European Commission is considering the "Trust Label" for IoT which will improve the end-to-end security of personal data in IoT networks.

USA

As compared to the EU, the US falls short of providing the same level of data protection to its subjects. There is also a difference as to who is the subject of the law, the US makes a distinction between US and non-US persons, while the EU offers the same level of data protection to all individuals regardless of their country or place of residence. The US has no federal law governing data protection and relies upon a sectoral approach to privacy protection. It relies both on state legislation and earlier privacy laws to secure the personal data of its citizens. States form their own data privacy laws as there are no direct federal protections for data. Data breach notification rules exist in some form in each of the states. These regulations demand that a business must notify its customers of any data breach when their personal information may have been compromised. Owing to its sectoral approach and the absence of a comprehensive law for data protection, there are many regulatory gaps.

Brazil

Brazil offers incentives, tax reforms and other measures to encourage vendors to provide improved IoT security standards. Although Brazil's General Data Protection Law is still relatively new, it has a solid foundation owing to GDPR's influence. Its governing body, the ANPD, plays a significant role in assisting the law's development and evolution. The LGPD applies to all economic sectors and to every company that collects data in Brazil, regardless of the country from where the data was sourced. Therefore, compliance with the same is mandatory for the IoT sector in Brazil. The law requires the users to provide their permission to organizations for obtaining

[60] Art. 1 of the REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Jun. 15, 2023), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R088.

[61] Art. 2(12) of the REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Jun. 15, 2023), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R088.

their personal data. Users have the right to request access to their data and also its total deletion at any time. Warnings, fines and even a whole or partial suspension of operations are all possible sanctions for disobeying the law, depending upon the seriousness of the offence. The law clearly defines terms like personal data, sensitive personal data and consent by stating the conditions for obtaining consent, re-obtaining consent, proving consent was received and conditions for revoking consent.[62] This consent paradigm is also used by other legislations around the world, including the GDPR.

China

Comparatively to the US, China is now employing a more thorough and coordinated campaign to influence critical IoT standards. Examining the data privacy laws implemented in China is important because of its significance as a technological hub. PIPL is a comprehensive data privacy policy adopted by China.[63] Initially, the country's data privacy laws relied on a patchwork of laws to safeguard its residents. Prior to the adoption of China's comprehensive data regulation, the country's approach to data privacy was very similar to the US, as its citizens were protected by a number of laws that were not directly related to the collection and processing of data.

INDIAN LEGAL FRAMEWORK: LACUNAE?

There are no specific provisions for the IoT sector under the IT Act, 2000.[64] The Act does not cover the vast array of IoT devices, networks and applications. Its primary focus is only on online transactions and e-communications. The complexity of data collection, storage and utilization in the IoT ecosystem may be beyond the scope of the current data protection and privacy rules in the Act. The Act's provisions are insufficient for efficiently safeguarding the privacy rights of individuals given the rampant development of the IoT sector and its potential surveillance and security vulnerabilities. The Act does include some cybersecurity-related regulations, but they fail to address the complex security issues posed by IoT devices. Due to numerous hardware and software components, IoT devices are vulnerable to security threats which could result in unauthorised access and data misuse. The Act also does not clarify the legal accountability and liability structure for the IoT sector.

Thus, there are no explicit provisions that address privacy and data protection under the Information Technology Act, 2000[65] and the Sensitive Personal Data or Information Rules, 2011 (the "Data Protection Rules")[66].

[62] Art. 8 of the General Data Protection Law (Lei Geral de Proteço de Dados, or LGPD), 13709/2018.

[63] Personal Information Protection Law of the PRC, 2021.

[64] The Information Technology Act, 2000.

[65] *Id.*

[66] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

The key issues in the Indian legal framework are discussed below:

- Scope: The primary limitation is that 'personal information' is only defined as information that may be used to uniquely identify a particular person.[67] The existing laws and Rules do not apply to background recording of personal information about others, whether done knowingly or unknowingly, as is the case with IoT devices. The limited definition of sensitive personal data is another limitation**.** Since IoT devices make it simpler to gather data everywhere, more sensitive personal information like location, habits and activities, among others, should be covered by the scope of these Rules.
- Privacy Policy: Organizations involved in the chain of data processing that collect, store, or otherwise deal with or handle 'personal information' have to display a privacy statement on their websites.[68] It describes the company's data processing practices, kinds of personal data collected along with the purpose of its collection, disclosures to third parties and the implementation of reasonable security measures.[69] This only enhances openness but does nothing to combat data misuse.
- Consent: Rules 5, 6, and 7 of the Data Protection Rules mandate that the body corporate must obtain the consent of data sources prior to any data collection, disclosure or transfer.[70] A body corporate should provide information on the purpose and place of data collection and storage, data recipients data. [71] Since these limitations only apply to sensitive personal data which has a narrow definition, a sizable amount of data is processed without prior consent of data providers.
- Lack of categorisation of IoT under the Indian Laws: IoT products and services are not specifically categorized under the Indian law. The scope of the Indian data protection laws only extends to data collected on the internet but not the data collected by internet of things devices. Owing to this, data categorization becomes difficult leading to uncertainty and difficulties when trying to apply the proper rules and legal frameworks to deal with IoT-related concerns. There is difficulty in defining precise regulations for regulatory bodies, users, service providers and manufacturers without a specific legal classification for IoT. Uncertainty in areas like security standards, user privacy and data protection results in a lack of classification. It is crucial for

[67] Rule 2(1)(i) of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(Jun 20. 2023), available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

[68] Rule 4 of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Jun 20. 2023), available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

[69] *Id.*

[70] Rule 5, 6 and 7 of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Jun 20. 2023), available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

[71] Rule 5(1) and 5(3) of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Jun 20. 2023), available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

regulators and legislators to adopt particular legal definitions and classifications for IoT products and services in order to close this gap. By doing this, it would be feasible to create focused rules and guidelines that effectively handle the liability, data security and user privacy and other such issues which are unique to IoT, guaranteeing that individuals are protected and encouraging the development of the IoT sector.

CONCLUSION AND RECOMMENDATIONS

The Internet of Things is a transforming concept. There is a real need for precise regulation for the IoT sector in India, given how constantly it is developing and its integration into our daily lives. With the lack of clear and strict laws governing the IoT sector, it is difficult to determine liability in cases of privacy and user data related violations. It is more difficult to guarantee data privacy in the absence of a specific data protection framework, given the increasing data collection through such devices. It is imperative that a comprehensive data protection framework is created in India that is in lines with the most recent technological advancements in the IoT sector. It should immediately take into account the data protection and user privacy concerns of the IoT sector. The authors have put forth the following recommendations:

Need for data classification: It is difficult to define the scope of the data collected by IoT devices owing to the lack of classification of data collected by such devices. The existing narrow definition of sensitive personal data does not include data such as location, personal habits of users among others, which forms the primary data collected by the IoT devices. This further raises the chances of data misuse. Additionally, it is challenging to precisely determine which industries and devices are covered by the existing Indian data protection rules because there is no comprehensive definition of the term “digital” in them.

Guidelines for creation of standard security guidelines for IoT sector: Due to the absence of universal guidelines and standards for the IoT sector, it is difficult to maintain and secure the data collected by IoT devices. Guidelines and regulations similar to that of the EU should be adopted where IoT devices can be categorised using a single set of certification requirements. There is a need for universal security requirements for IoT devices. Additionally, there should be a governing body like ANPD, the chief data protection authority in Brazil. This would provide for a framework that will facilitate the creation and implementation of IoT standards.

Consent paradigm: There is a need to clearly define terms like ‘consent’ and ‘informed consent’. The conditions for obtaining informed consent of the users of the IoT devices should also be specified. There is also a need for provisions for informing the users that an individual’s data has been breached and their personal data has been sacrificed.

REFERENCES

Ande R. et. al., *Internet of Things: Evolution and Technologies from a Security Perspective,* 54 Sustainable Cities and Society (2020).

Dorsemaine B. et. al., *Internet if Things: A definition and taxonomy* (2015), in proceedings of the 9th International Conference on Next Generation Mobile Applications (2015).

Gubbi et al., *Internet of Things (IoT): A vision, architectural elements and future directions,* 29 Future Generation Computer Systems, 645-1660 (2013).

Kheirkhahan M. et al., *A smartwatch-based framework for real-time and online assessment and mobility monitoring*, 89 Journal of Biomedical Informatics 29-40 (2019).

Kramp T. et al. *Enabling Things to Talk* (2013).

Kranenburg R.V., *The Internet of Things. A critique of ambient technology and the all-seeing network of RFID,* 2 Institute of Network Cultures (2007).

Kumar S. et. al., *Internet of Things is a revolutionary approach for future technology enhancement: A review,* 6 Journal of Big Data 111 (2019).

Mohamed E., *The Relation of Artificial Intelligence with the Internet of Things: A Survey*, 1(1) Journal of Cybersecurity and Information Management 30-34 (2020).

Madakam S. et. al., *Internet of Things (IoT): A Literature Review*, *,* 3(5) Journal of Computer & Communications 164-173 (2015).

Miorandi D. et al., *Internet of things: Vision, applications and research challenges*, 10(7) Ad Hoc Networks 1497-1516 (2012).

Mohd J. et al., *Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT)*, 2 Sensors International (2021).

Perera C. et al., *The emerging Internet of Things marketplace from an industrial perspective: A survey*, 3(4) IEEE Transactions on Emerging Topics in Computing 585-598 (2015).

Perwej Y. et. al., *The Internet of Things (IoT) and its Application Domains,* 182(49) International Journal of Computer Applications 36-49 (2019).

Raine L. et al., *The Internet of Things Connectivity Binge: What are the Implications?*, Pew Research Centre, Washington, DC (2017).

Rousan T.A., *The Future of Internet of Things*, 4(1) IJCCIE (2017).

Syed S. et. al., *IoT in Smart Cities: A survey of Technologies, Practices and Challenges*, 4 Smart Cities, 429- 475 (2021).

Safaei B., et. al., *Reliability Side-Effects in Internet of Things Application Layer Protocols*, in proceedings of the International Conference on System Reliability and Safety (2017).

Williams P. et. al., *A survey on security in internet of things with a focus on the impact of emerging technologies*, 19 Internet of Things (2022).

Wiltz B.W. et. al., *An Integrative Public IoT Framework for Smart Government*, 36(2) Government Information Quarterly (2019).