

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

## **EDITORIALTEAM**

### **EDITORS**

#### **Dr. Samrat Datta**

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*



#### **Dr. Namita Jain**

*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*



*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

## Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*



## Avinash Kumar



*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

## **ABOUT US**

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS  
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

# **IMPLICATIONS, DEVELOPMENT AND ISSUES: AN OVERVIEW ON DATA PROTECTION LAWS IN LOCATION INFORMATION**

AUTHORED BY - K SANKEERTHANA

B.A. LL.B (HONS)

## **ABSTRACT**

Technology is developing quickly as a result of increased internet usage and the removal of obstacles to information flow. Data has become a vital part of our daily lives, with almost every aspect of modern life being connected to some form of data. The Indian Supreme Court declared that the right to privacy, along with the rights to life and personal liberty guaranteed by Article 21 of the Indian Constitution, is a fundamental freedom.

The intersection of multiple legislation for different sectors creates uncertainty and is one of the key reasons of the breach in India, where there has been a significant amount of data loss. Despite having the efficient law making system they have failed to address the issue in the matters regarding location information of a person

In this paper we aim to address the key developments, issues, and implications that is put forward in today's world with a prime focus upon India in data protection laws in location information.

We will be referring to various articles, research papers and the existing provisions from the constitution of India for creating an overall analysis of data protection laws in the field of location information. . By conducting a thorough analysis, we would draft the appropriate suggestions and upshot.

**Key Words:** Data protection, right to privacy, constitution, location information, article 21, Supreme Court

## **1. INTRODUCTION**

The contemporary day, where technology was an important term in every aspect of our lives. The concepts of privacy, data and location information have gained more importance. The rapid advancements in information and communication technologies have lead to unparalleled connectivity and convenience. Data security and privacy worries tied to location information have been highlighted by technological progress' rapid changes, stirring discussion around protecting sensitive user details amid new capabilities.

Privacy, being the fundamental human right to safeguard one's personal details and shield them from unwanted access or disclosure, is of the utmost importance in any just society that values individual autonomy and freedom from overreach. in the automated world, privacy becomes linked with the huge amount of data generated and shared by people daily. These data, which range from location data gathered by smart devices to social media postings and online purchases, are the basis of contemporary technological interactions.

The more information about you that your location exposes, where you consume food, travel, and reside. In particular, location data has particular significance in the context of personal data. Location data is increasingly an important resource for many applications, such as social networking, targeted advertising, and navigation services, because of GPS-enabled gadgets.

The focus of this research study is to look into in detail the intricate relationship that occurs between location, data, and privacy

### **1.1 RESEARCH PROBLEM**

A person has the right to know their location. They have the final say over whether or not to disclose their locations. Taking data security into account is turning into a top privacy concern. The existence of laws pertaining to location information security that are not being applied in the way that is intended is the research problem that we are identifying.

### **1.2 RESEARCH QUESTION**

1. What are the primary privacy concerns with data protection and privacy in location information?
2. Whether the laws and policies provided by government is enough to reassure the protection of location of location information in the data privacy world of our country?

### **1.3 HYPOTHESIS**

The prevailing legislations and statutes are not sufficient in order to overcome the problems faced by the society in data privacy and misuse of location information”

### **1.4 EXISTING LEGAL SITUATION**

**ARTICLE 21<sup>1</sup>**: the article says that every person who is either a citizen or a non- citizen has the right to live with dignity and the right to have personal liberty. There are a lot of components comprised in this article with the growing and development of law. One such component is the right to privacy which was added as a fundamental right and as a component of this article through the justice K.S. Puttuswamy & Anr v. Union of India & Ors<sup>2</sup>

**IT ACT<sup>3</sup>**- Geo-location information is not defined in the personal data definitions under the IT act. But there was a bill introduced which would include a clear definition of geo-location information and its sharing.

**THE DIGITAL PERSONAL DATA PROTECTION ACT (2023)<sup>4</sup>** - The long awaited act is said to be passed by the parliament on 9 august, 2023 which mandates it for the institutions or entities collecting their user’s data for any other purpose. It also acts as a guide to the organizations in handling the personal data provide for their use by their users.

### **1.5 LITERATURE REVIEW**

**1. Should ‘location data’ be considered as ‘personal data’ under Indian privacy laws (2021) Panicker and Panicker Advocates<sup>5</sup>**: this is an article which has arisen a question on the need and necessity to consider or address location data as a personal data. It has made reference to the scenarios in every-day life where location data/ location information becomes useful. The article starts with what is location data which generally just defines location data/ location information. It also deals with the various

---

<sup>1</sup> Article 21, the constitution of India, 1950.

<sup>2</sup> Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

<sup>3</sup> Information Technology Act, 2000(No 21 OF 2000)

<sup>4</sup> The digital personal data protection act, 2023( No. 22 OF 2023)

<sup>5</sup> See article, should ‘location data’ be considered as ‘personal data’ under Indian privacy laws, available at <<https://www.mondaq.com/india/privacy-protection/1128884/should-location-data-be-considered-as-personal-data-under-indian-privacy-laws>>

types of location data and the article concludes by the meaning and understanding of identifiability of location data.

2. **"Location privacy: User Behaviour in the field" Buly Krumm (2007) Researchgate<sup>6</sup>:** Location Information is spreading wider and wider because of the Smartphone, tablets, laptops by GPS which coordinates automatically (Metadata) to share a person location unknowingly or unknowingly like Photo locations which results in concerns especially with parents and this article discusses on information Lifespan, Audience, personal benefits, sender-content relationship, personal context, Tangibility.
3. **Data privacy in India: current outlook and the future (2023) the times of India<sup>7</sup>:** this article begins with the comparison of the data proliferation control in personal data between the western world (Europe) and India. It says that in Europe their government has been making and establishing acts like GDPR<sup>8</sup> from a very long time to secure and safeguard their citizen's data and personal law. But when it comes to India there have been various forms of obligations like contractual or legal obligations. It says about the government trying to implement the data protection laws for its citizens. It is a comparative analysis on the data protection laws in two different places.
4. **"Legal and Ethical Implications of Location Data in Online Social Networks" by Gundecha et al. (2012) Researchgate<sup>9</sup>:** This paper has a unique contribution which combines the ethical and legal implications of social networking sites also recommends and provides for researching on social networking in futures too by giving the fluid nature of social networking Ethics and laws also said that the employees should have limits or boundaries where they should not go beyond the limit by giving warnings. By focusing on future researchers who work on Data privacy should adopt the new changes and examine what social networks are involved in Organisations.
5. **"The Role of Data protection in Marketing" by Kelly D. Martin and Patrick E. Murphy (2016)<sup>10</sup>:** This article is based on data privacy role in marketing. This paper

---

<sup>6</sup> See article, "location privacy: user behaviour in the field, available at <[https://www.researchgate.net/publication/236014201\\_Location\\_Privacy\\_Revisited\\_Factors\\_of\\_Privacy\\_Decision](https://www.researchgate.net/publication/236014201_Location_Privacy_Revisited_Factors_of_Privacy_Decision)>

<sup>7</sup> See article, data privacy in India: current outlook and the future, available at <<https://timesofindia.indiatimes.com/blogs/voices/data-privacy-in-india-current-outlook-and-the-future/>>

<sup>8</sup> The general data protection regulation, 2018, replacement of EU data protection directive of 1995

<sup>9</sup> See article, "Legal and Ethical Implications of Location Data in Online Social Networks" by Gundecha et al., available at <[https://www.researchgate.net/publication/225475733\\_Legal\\_and\\_Ethical\\_Implications\\_of\\_Corporate\\_Social\\_Networks](https://www.researchgate.net/publication/225475733_Legal_and_Ethical_Implications_of_Corporate_Social_Networks)>

<sup>10</sup> See article, "the role of data protection in marketing" by Kelly D. Martin and Patrick E. Murphy, available at <[https://scholar.google.co.in/scholar\\_url?url=https://www.researchgate.net/profile/Kelly-Martin-12/publication/308578866\\_The\\_Role\\_of\\_Data\\_Privacy\\_in\\_Marketing/links/5c473b67a6fdccd6b5c04380/The-](https://scholar.google.co.in/scholar_url?url=https://www.researchgate.net/profile/Kelly-Martin-12/publication/308578866_The_Role_of_Data_Privacy_in_Marketing/links/5c473b67a6fdccd6b5c04380/The-)

examines about data and privacy information is grouped according to privacy's role in society, psychology and in economics. Effects of wide access to consumer's personal information, including fraud, privacy invasions, unwanted communications in marketing, and highly targeted. Privacy role in society also includes ethics of privacy. Psychology of privacy includes consumer privacy concerns, consumer privacy outcomes, consumer privacy enhancing factors personalization and control. Economics of privacy includes organizational privacy models, organizational privacy failures and self - regulation.

- 6. “Current trends and challenges in location based services” by Haosheng Huang and Georg Gartner (2018)<sup>11</sup>:** This article tells about the Location - based data includes in the scientific field like positioning, modelling, communication, applications, evolution and analysis, privacy and ethical issues. Location Based services (LBS) is an application especially a mobile computing application, which provides the information about the location. LBS is an part of positioning and location determination. It is also a key task for LBS. One of the challenges for LBS is privacy issues. Nowadays, LBS became more popular not only in environments( both indoor and outdoor) but it becoming more popular in shopping malls, museums, airports etc. LBS also applicable in emergency services, tourism services, healthcare, social networking, etc.

### **1.5 SCOPE AND OBJECTIVES**

Data privacy which is now becoming the most focused area as we adapted to new technology with digital age where violations of data privacy can infringe upon individuals fundamental rights including Freedom of expression, right to privacy, and non-discrimination which are should be protected by international and national legal systems. The objective of this paper is to understand that how individuals can protect themselves by avoiding registering in unknown/unrecognised website where location and privacy extends beyond the protection of person and provides the scope of improvement in the digital era situation by suggesting better legislation.

---

Role-of-Data-Privacy-in-Marketing.pdf&hl=en&sa=X&ei=Rtk9ZaCBEK6P6rQPrc-EmAk&scisig=AFWwaea2KbSKIOLL4SP-\_xK0zCFo&oi=scholar>

<sup>11</sup> See article, “ current trends and challenges in location in location based services” by Haosheng Huang and Georg Gartner, available at < [https://www.mdpi.com/2220-9964/7/6/199#:~:text=\(6\)%2C%20199%3B-,https%3A//doi.org/10.3390/ijgi7060199,-Received%3A%2023%20May](https://www.mdpi.com/2220-9964/7/6/199#:~:text=(6)%2C%20199%3B-,https%3A//doi.org/10.3390/ijgi7060199,-Received%3A%2023%20May)>

## **1.6 METHODOLOGY**

This research paper addresses the issues faced in data protection of location information in India and the efficiency of law in resolving them. This paper is purely based on literature review of various journals, articles, research papers, and bare acts, dictionaries that talks about or addresses data protection. We have followed analytical mode of research.

## **2. CONCEPT AND CONCERNS OF DATA PROTECTION AND PRIVACY IN LOCATION INFORMATION**

### **2.1 What is data protection and privacy in location information?**

Data protection and insulation in position information is each about keeping individualities information safe from falling into the wrong hands, avoiding unwanted exposure, changes or indeed its complete destruction.

Data protection constantly involves guarding insulation and sensitive information. This information is gathered by companies or government realities. It can include names, addresses, phone numbers, financial data, medical records, or any other data that can be used to identify an existent.

According to Blumberg and Eckersley, location privacy is "*the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use.*"<sup>12</sup>

We gather and store location-based data in a way that fully respects our privacy rights. Our process always adheres strictly to all related laws and regulations.

#### **2.1.1. Anonymization's part in the private**

Anonymization location data is really important for maintaining privacy. Location data is sensitive information that shows where a device or a person is geographically<sup>13</sup>. It can disclose a lot about someone, like their daily habits, their favourite hangouts, and even the locations of their home and workplace.<sup>14</sup>

---

<sup>12</sup>Andrew J. Blumberg and Pete Eckersley , "On Locational Privacy, and How to Avoid Losing it Forever"<<https://www.eff.org/files/eff-locational-privacy.pdf>>

<sup>13</sup> India: Understanding The Process Of Data Anonymisation In The Context Of Data Privacy Laws<<https://www.mondaq.com/india/data-protection/1128820/understanding-the-process-of-data-anonymisation-in-the-context-of-data-privacy-laws#:~:text=In%20India%2C%20'Anonymisation'%20is,the%20framework%20of%20privacy%20jurisprudenc>e.>

<sup>14</sup> See definition of " Anonymization" available at <[imperva.com](http://imperva.com)>

Under Clause 3(2) of the Personal Data Protection Bill, 2019<sup>15</sup>,

*'Anonymization' is defined as " analogous unrecoverable process of converting or converting particular data to a form in which a data star can't be linked, and which meets the morals of irreversibility specified by the Authority."* <sup>16</sup>

Under Article 4(5) of General Data Protection Regulation (GDPR),2016<sup>17</sup>

The term "pseudonymization" refers to the processing of particular data in a way that makes it impossible to link it to a particular data subject without the use of fresh information, handed that the fresh information is stored singly and is defended from identification by organisational and technical safeguards. <sup>18</sup>

In *M. P. Sharma vs. Satish Chandra*, the 8-judge bench of the Supreme Court held that the drafters of the Constitution did not intend to subject the power of search and seizure to a fundamental right of privacy. They opined that the Constitution does not include language similar to the Fourth Amendment of the US Constitution, and found no justification to import the concept of a fundamental right to privacy in search-and-seizures, through what they called a 'strained construction'.<sup>19</sup>

In the case *Kharak Singh v state of Uttar Pradesh*, the decision invalidated a Police Regulation that provided for nightly domiciliary visits, calling them an *"unauthorized intrusion into a person's home and a violation of ordered liberty."* However, it also upheld other clauses of the Regulation on the ground that the right of privacy was not guaranteed under the Constitution, and hence Article 21 of the Indian Constitution (the right to life and personal liberty) had no application. Justice Subbarao's dissenting opinion clarified that, although the right to privacy was not expressly recognized as a fundamental right, it was an essential ingredient of personal liberty under Article 21.<sup>20</sup>

As a component of the right to life and personal liberty, the right to privacy was recognised by the Hon. Supreme Court of India under Article 21<sup>21</sup> of the Indian

---

<sup>15</sup> Clause 3(2) of the Personal Data Protection Bill, 2019

<sup>16</sup> Clause 3(2) of the Personal Data Protection Bill, 2019

<sup>17</sup> Article 4(5) of General Data Protection Regulation (GDPR),2016

<sup>18</sup> India: Understanding The Process Of Data Anonymisation In The Context Of Data Privacy Laws<  
<https://www.mondaq.com/india/data-protection/1128820/understanding-the-process-of-data-anonymisation-in-the-context-of-data-privacy-laws#:~:text=In%20India%2C%20'Anonymisation'%20is,the%20framework%20of%20privacy%20jurisprudenc>  
e.>

<sup>19</sup> (1954) 1 SCR 1077

<sup>20</sup> 1963 AIR 1295, 1964 SCR (1) 332

<sup>21</sup> Article 21, the constitution of India, 1950.

Constitution

. But, In the case of, *Justice K.S. Puttaswamy v. Union of India. (2017)*<sup>22</sup>, also known as “Privacy Judgement. It has been recognised that "informational privacy" is a component of the right to privacy. The court further noted that privacy protection is necessary for both access to personal information and information about an individual.<sup>23</sup>

So, the Right to Privacy is also a fundamental right of an individual and it want to be given more importance.

## 2.2 How is Data, Location, Privacy related?

As the technology shifted to Smartphone which records every location you visit with or without the knowledge of the user if the phones location services are turned on. This can also give the information of the user Home Location, Office location and other locations wherever the user goes. Data and Location which violates the Fundamental Right of right to privacy Under Article 21<sup>24</sup>. However, GPS services provide data while the location Services are active though you turn off your locations services on your devices you are not set free from the long arm. A smart phone tracks the location even if you disable or logged out because the operating system automatically tracks the location of the cell towers and supplies the information to Google automatically. Devices with a cellular data or Wi-Fi connection automatically send the data to Google. Even the unknown individual gets to know the location which he/she may misuse. Social media handles like snap chat which shows the location of a stranger once you quick add and Instagram by posting a picture and adding the location which gives indications that may result in theft.<sup>25</sup>

In the digital age, data, location, and privacy are all intertwined ideas. Data creation, storage, and transport have become increasingly common in today's technologically driven world. Personal information such as names, addresses, contact information, financial information, and much more are included in this massive amount of data. Businesses, government organizations, websites, applications, and any other entity

---

<sup>22</sup> Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

<sup>23</sup> (2017) 10 SCC 1

<sup>24</sup> Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

<sup>25</sup> See article, “ location information is more important than you think” by Sarah Meyer, available at < <https://www.cpomagazine.com/data-privacy/location-privacy-is-more-important-than-you-think/>>

that interacts with humans can gather and keep data. Data location refers to where data is stored, processed, or moved, which might be inside the borders of a country or in other jurisdictions throughout the world.

Individuals' right to regulate the acquisition, use, and dissemination of their personal information is referred to as privacy. It is about safeguarding the confidentiality, security, and integrity of an individual's personal data. Privacy laws seek to establish legal safeguards and regulations that ensure individuals have control over their personal data while also preventing illegal access. The Personal Data Protection Bill 2019 (PDPB)<sup>26</sup>, which is now being debated in Parliament, is India's fundamental legislation addressing data protection and privacy. Furthermore, the Information Technology Act of 2000 (IT Act)<sup>27</sup> and its revisions address several areas of data security and privacy. The IT Act specifies how to deal with unlawful access, disclosure, and misuse of electronic documents, including personal information. Concerning the court's jurisdiction, the PDPB, if passed, is anticipated to establish a data protection authority and adjudicatory process to address data breaches, privacy violations, and other data protection problems. In contrast, the IT Act enables for legal action and sanctions to be enforced by a variety of courts, including district courts, high courts, and the Cyber Appellate Tribunal<sup>28</sup>.

It's crucial to remember that data, location, and privacy are continually shifting legal topics, especially in the context of emerging technology and worldwide data flows. It is recommended to seek legal advice to guarantee compliance with applicable laws and regulations, as well as clarity on specific data protection and privacy issues.

### **2.3 Major concerns regarding location information.**

Location information is provided by location based services like GPS, whatsapp, cellular towers, roadside assistance which include roadside boards etc. There are few advantages but like any other concept it also involves risks. Usually the general location information provided by Mobiles is known as geo location information.

---

<sup>26</sup> The Personal Data Protection Bill 2019, now stands withdrawn

<sup>27</sup> Information Technology Act, 2000(No 21 OF 2000

<sup>28</sup> See article, "location privacy and its application: a systematic study" by Bo Liu; Wanlei Zhou; Tiaqing Zhu; Longxiang Gao' Yong Xiang, available at <  
[https://www.researchgate.net/publication/324177819\\_Location\\_Privacy\\_and\\_Its\\_Applications\\_A\\_Systematic\\_S\\_tudy](https://www.researchgate.net/publication/324177819_Location_Privacy_and_Its_Applications_A_Systematic_S_tudy)>

Usually when some individual installs and opens a particular mobile app it includes asking for several permissions one of which is granting permission to access location. There are multiple data collectors (apps) who make it mandatory to provide access to the system control which already has your personal information and helps the data collector to store your location and other personal information. This might lead to the risk of the following<sup>29</sup>:

- A. Whether their personal data and location data are being used for any other purposes.
- B. With whom the data is being shared?
- C. Is the data of location shared on the app being subject to onward transfer of data?
- D. Is there a specific timeline that the data is stored for?

As said above there are several location based services or the entities that have access to one's location data. Let us dive into who will have access to the location data of an individual.

### **2.3.1 Who will have access to location data?**

A wide range of commercial entities that offer various services possess location data. These entities may include mobile phone carriers, operating systems, businesses that are integral to a device's core functionality, consumer-facing applications etc.

Mobile phone carriers- the mobile phone carriers use the location of the device from where they would direct the phone calls through the cell phone towers. This location can also be enhanced with GPS location data.<sup>30</sup>

Apps and app partners - people generally use apps with location-based features. Where there are provisions of weather alerts, sharing of rides or delivering of purchases made from online stores. The location information is shared usually with the app partners to monetize their services through the app.<sup>31</sup>

### **2.3.2 How is location information collected?**

Generally the data is collected through GPS which can be combined by carriers.

---

<sup>29</sup> See article, "location privacy and its application: a systematic study" by Bo Liu; Wanlei Zhou; Tiaqing Zhu; Longxiang Gao' Yong Xiang, available at <[https://www.researchgate.net/publication/324177819\\_Location\\_Privacy\\_and\\_Its\\_Applications\\_A\\_Systematic\\_Study](https://www.researchgate.net/publication/324177819_Location_Privacy_and_Its_Applications_A_Systematic_Study)>

<sup>30</sup> See article, should 'location data' be considered as 'personal data' under Indian privacy laws, available at <<https://www.mondaq.com/india/privacy-protection/1128884/should-location-data-be-considered-as-personal-data-under-indian-privacy-laws>>

<sup>31</sup> See article, "a closer look at location data: privacy and pandemics" available at <<https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/>>

The most common methods are through GPS, cell towers, Bluetooth beacons and Wi-Fi networks<sup>32</sup> etc. The detailed way of collecting location information is mentioned below:

- a. GPS- a phone's GPS chip is just one sensor among the several that are used by smart phones and other devices to determine location through satellite GPS<sup>33</sup>
- b. Cell towers- cell towers usually connect phone calls. So they will be aware of the location of the cell. There are unique cell tower IDs through which the location can be detected.
- c. Bluetooth beacons- most of the apps are designed in a way that they can detect their proximity to the beacons which are the radio transmitters that sends one way Bluetooth signals
- d. Wi-Fi networks- it generally happens through scanning the Wi-Fi networks available nearby.

### **2.3.3 Is privacy in location information recognised legally?**

Location data is considered as a unique category of data in most jurisdictions means it is subject to additional protection like higher security standards and the need for express consent that is given voluntarily. As per the law the privacy rules in India specifies that SPDI<sup>34</sup> cannot hold the personal information for a period longer than required and for the purpose for which the information may lawfully be used. Right to privacy became a fundamental right through *k. S. Puttuswamy v. Union of India*<sup>35</sup>. This led to the formation of personal data protection laws. Location data is said to be falling in the ambit of personal data and is governed by SPDI rules which only deals with the data and information exchanged in electronic form.

Other legislations by various courts are as follows:

When there is a violation of location privacy, the Indian Penal Code, 1860<sup>36</sup> (IPC) and the Information Technology Act, 2000<sup>37</sup> (IT Act) may also be applicable. The

---

<sup>32</sup> See article, "a closer look at location data: privacy and pandemics" available at < <https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/>>

<sup>33</sup>See article," a closer look at location data: privacy and pandemics" available at < <https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics/>>

<sup>34</sup> Sensitive personal data and information, 2011

<sup>35</sup> Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

<sup>36</sup> Indian Penal Code, 1860 (No 45 of 1860)

<sup>37</sup> Information Technology Act, 2000 (No 21 OF 2000)

IT Act's Section 43A<sup>38</sup> stipulates that failing to secure sensitive personal data, including location data, may result in compensation being given. Sections 354C<sup>39</sup>, 354D<sup>40</sup>, and 509<sup>41</sup> of the Indian Penal Code deal with stalking, voyeurism, and using criminal force to violate a woman's modesty. In rare cases, these crimes may entail violating someone's geographical privacy<sup>42</sup>.

Indian courts have addressed location privacy in a number of rulings and have established rules for its protection.

The Allahabad High Court ruled in *Ritesh Sinha v. State of Uttar Pradesh and Ors.*<sup>43</sup> (2019) “that following someone's position continuously using electronic devices without that person's consent violates their right to privacy”.<sup>44</sup>

In *Sharat Babu Digumarti v. Government of NCT of Delhi and Ors.*<sup>45</sup> (2017), the Delhi High Court held that law enforcement agencies shall not track an individuals' locations without adhering to due process and obtaining appropriate permissions.

### **3. LAW AND PRIVACY IN LOCATION INFORMATION**

#### **3.1 Introduction to the The Digital Personal Data Protection Act (2023)**

##### **3.1.1 History of bill to an act**

By establishing a legal framework that emphasizes the responsibilities and the rights of the “digital nagrik”, the law contemplates the regulation of digital personal data. The draft digital personal data protection bill 2022 got the approval of the union cabinet on July 5, 2022. The GDPR<sup>46</sup> and other personal data protection regulations in other jurisdictions are founded on identical fundamental ideas, which also serve as the foundation for the bill. These include responsibility, integrity, secrecy, lawfulness, fairness and transparency as well as purpose limitation, data minimization, accuracy, and storage limitations. This bill was passed by the parliament on 7 August 2023 and it is act no 22 of 2023<sup>47</sup>.

<sup>38</sup> Section 43A of, Information Technology Act, 2000(No 21 OF 2000)

<sup>39</sup> Section 354C of, Indian Penal Code,1860(No 45 of 1860)

<sup>40</sup> Section 354D of, Indian Penal Code,1860(No 45 of 1860)

<sup>41</sup> Section 509 of, Indian Penal Code,1860(No 45 of 1860)

<sup>42</sup> ibid

<sup>43</sup> (2019) 8 SCC , para 27

<sup>44</sup> ibid

<sup>45</sup> 2016 SCC OnLine SC 1464

<sup>46</sup> General Data Protection Regulation (GDPR),2016

<sup>47</sup> The digital personal data protection act, 2023( No. 22 OF 2023)

### 3.1.2 The Digital Personal Data Protection Act, 2023

The act was enacted by the parliament of India. The act is

*" an act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto"*<sup>48</sup>

Beyond the Information Technology (IT) Rules, the act extends citizens' rights, such as the right to information, the right to redress for grievances, the right to rectification and erasure, and the right to designate a representative in the event of incapacity. It also describes what Significant Data Fiduciaries (SDFs)<sup>49</sup> must do. The Ministry of Electronics and Information Technology (MeitY) states that the Digital India Act (DIA), which will supersede the current IT Rules, would shortly supplement the DPDPA<sup>50</sup>.

The processing of digital personal data inside the borders of India, whether it be offline data gathered and then digitized, is subject to the Digital Personal Data Protection (DPDP) Act, 2023<sup>51</sup>. If processing digital personal data entails delivering products or services to data principals inside India's borders, it also applies to processing such data outside of the country<sup>52</sup>.

The following provisions in the Bill safeguard digital personal data—that is, information that may be used to identify an individual including<sup>53</sup>:

- a) The rights and duties of Data Principals,
- b) or the person to whom the data relates,
- c) the obligations of Data Fiduciaries, or individuals, businesses, and governmental entities that process data,
- d) for data processing, which includes gathering, storing, or any other operation on personal data, and
- e) the financial penalties for violating these rights, duties, and obligations<sup>54</sup>.

<sup>48</sup>See long title of The digital personal data protection act, 2023( No. 22 OF 2023)

<sup>49</sup> SDFs are significant data fiduciaries

<sup>50</sup> See article “ decoding the digital personal protection data protection act,2023” by dr. Lalit kalra available at <[https://www.ey.com/en\\_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023](https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023)>

<sup>51</sup> The digital personal data protection act, 2023( No. 22 OF 2023)

<sup>52</sup> See article “ decoding the digital personal protection data protection act,2023” by dr. Lalit kalra available at <[https://www.ey.com/en\\_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023](https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023)>

<sup>53</sup> See article " salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264>>

<sup>54</sup> See article " salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264>>

The following seven guiding concepts form the basis of the Bill<sup>55</sup>:

- a) the idea of permission, legitimate, and open use of personal information;
- b) the concept of purpose restriction, which states that personal information should only be used for the purposes for which it was collected with consent from the data principal
- c) the data minimization principle, which calls for collecting personal information only to the extent required to fulfil a given objective;
- d) the idea of data accuracy, which is making sure data is current and accurate;
- e) the idea of limited storage (keeping data for as long as it's required for the intended use);
- f) the idea of appropriate security measures; and
- g) The accountability concept (adjudicating data breaches and Bill provisions violations and imposing fines for the breaches)<sup>56</sup>.

The following rights are granted to individuals by the bill<sup>57</sup>:

- a) The right to data deletion and rectification; The right to information access regarding processed personal data;
- b) the ability to file a grievance; and
- c) the authority to designate a representative to carry out rights in the event of incapacity or death<sup>58</sup>

The punishment provision in the DPDP Act is another noteworthy aspect. Data fiduciaries that violate the laws face fines of up to INR 250. Among them are:

- a. Breach of the data principal's obligation to observe up to INR 10,000<sup>59</sup>
- b. Up to INR200 may be lost if the data protection board and the impacted data principals are not notified of a breach involving personal data.<sup>60</sup>

---

<sup>55</sup> See article " salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264>>

<sup>56</sup> See article " salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264>>

<sup>57</sup> See article " salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264>>

<sup>58</sup> See article " salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264>>

<sup>59</sup> See article " decoding the digital personal protection data protection act,2023" by dr. Lalit kalra available at <[https://www.ey.com/en\\_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023](https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023)>

<sup>60</sup> See article " The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act" by shravishta ajaykumar; amoha basrur; vaishnavi Sharma, available at <[https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023/#amp\\_ct=1698763717905&\\_tf=From%20%251%24s&aoh=16987637067786&referrer=https%3A%2](https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023/#amp_ct=1698763717905&_tf=From%20%251%24s&aoh=16987637067786&referrer=https%3A%2)>

- c. Breach of an extra responsibility up to INR 200 with regard to minors<sup>61</sup>

An impacted Data Principal should initially contact the Data Fiduciary to enforce his or her rights. If unsatisfied, the individual can easily file a complaint against the Data Fiduciary with the Data Protection Board<sup>62</sup>.

### 3.2 Criticism of laws and rules relating to privacy in location information

*Under Clause 2(28) of the Personal Data Protection Bill, 2019<sup>63</sup>*

Under this clause the 'personal data' defines as, "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling."<sup>64</sup>

While location data is not specified, personal data is explicitly addressed in this section. The location data is a source for creating an individual profile. It is imperative that location data be treated as personal data in legal modifications. Guidelines protecting location data against de-identification and de-anonymization must be part of this.

*Under Clause 3(2) of the personal data protection bill, 2019<sup>65</sup>*

'Anonymization' is defined as, "in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority."<sup>66</sup>

This section makes it very evident that any identifying information about an individual is being deleted in order to prevent data from being linked to them and to make identification more difficult.

---

F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.orfonline.org%2Fresearch%2Fthe-digital-personal-data-protection-act-2023%2F>

<sup>61</sup> See article "The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act" by shravishta ajaykumar; amoha basrur; vaishnavi Sharma, available at <[https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023/#amp\\_ct=1698763717905&amp\\_tf=From%20%251%24s&aoh=16987637067786&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.orfonline.org%2Fresearch%2Fthe-digital-personal-data-protection-act-2023%2F](https://www.orfonline.org/research/the-digital-personal-data-protection-act-2023/#amp_ct=1698763717905&amp_tf=From%20%251%24s&aoh=16987637067786&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.orfonline.org%2Fresearch%2Fthe-digital-personal-data-protection-act-2023%2F)>

<sup>62</sup> See article "salient features of the digital personal data protection bill 2023", available at <<https://pib.gov.in/PressReleaselframePage.aspx?PRID=1947264>>

<sup>63</sup> Clause 2(28) of The Personal Data Protection Bill 2019

<sup>64</sup> Clause 2(28) of the Personal Data Protection Bill, 2019

<sup>65</sup> Clause 3(2) of the personal data protection bill, 2019

<sup>66</sup> Clause 3(2) of the personal data protection bill, 2019

### 3.2.1 DIGITAL DATA PROTECTION BILL HIGHLIGHTS

An identifiable or identifiable person has a connection to personal data. Personal data is used by businesses and government agencies to provide goods and services. Understanding about individuals is made possible by personal data, and this knowledge is helpful for creating suggestions, tailored advertising, and customization..

Personal data is governed by the Information Technology Act (IT Act), 2000.<sup>67</sup>

In December 2019, the Lok Sabha received the 2019 Personal Data Protection Bill<sup>68</sup>. After being tasked with overseeing the Bill, a Joint Parliamentary Committee produced its findings in December 2021.<sup>69</sup> The Bill was taken out of Parliament in August of 2022. For public comment, a draught bill was made available in November 2022. Parliament received the Digital Personal Data Protection Bill, 2023 in August of that year<sup>70</sup>.

#### Applicability

The applicability of the bill is to processing a digital personal data within India such data is collected by online or offline. It will also applicable outside India if it is providing goods or services in India. Collection, storage use and sharing also included.

#### Consent

The individual voluntarily want to give his data for specified purposes, it includes medical emergency, employment, etc. If the individual is below 18 years , the consent want to be provided by his/ her parent or legal guardian.

#### Transfer of personal data outside of India

The Bill permits the transfer of personal data outside of India, but it will not be allowed for the restricted countries by the central government.

#### Exemptions

It includes,

- (i) prevention and investigation of offences,
- (ii) Enforcement of legal rights or claims.

As Per the ruling of the Supreme Court in 2017, any interference with an individual's right to privacy must be commensurate with the need of the

<sup>67</sup> Information Technology Act, 2000(No 21 OF 2000)

<sup>68</sup> The Personal Data Protection Bill, 2019, as introduced in Lok Sabha

<sup>69</sup> Joint Committee on the Personal Data Protection Bill, 2019, December 2021

<sup>70</sup> Digital Personal Data Protection Bill, 2019, as introduced in Lok Sabha.

interference.

To further goals including state security and public order maintenance, the Bill gives the central government the authority to exclude processing carried out by government agencies from any or all of the restrictions.

### 3.3 Suggestions

1. Delete unused apps, accounts, which you feel unsafe or which violates Individual rights
2. Share less info with apps and services while logging
3. Stop searching or visiting unwanted spots or location
4. Avoid sharing live locations to strangers when you're out of station
5. Use advanced technology for protecting your Data
6. Use strong passwords
7. Keep on updating your device
8. Use secures Connections which does not misuse your Data, location and privacy.
9. Switch to a private space Browser if you feel Unsafe.
10. Avoid sharing Mail id for unrecognised websites

### **CONCLUSION**

In the digital age, location information privacy encompasses efficient laws for individual privacy rights and safety. This research paper tells you the importance of making and maintaining the legal framework effectively to protect the individual privacy in the part of location data. In the world, smart phones and other smart gadgets are tracking and sharing user's locations. The legal framework must want to address a protection for data misuse, surveillance, and unauthorized tracking. The laws are efficiently crucial in safeguarding citizens' fundamental rights. Achieving such efficiency is a task which demands continuous scrutiny, updating and adaptation. The laws are not efficient but it's also more effective in protecting location information privacy. The laws are not only efficient but comprehensive. They should bring a balance between authorizing location information for legitimate uses, including public safety. To protect individuals' rights in the digital era, legislators and policymakers want to keep on drafting and revising legislation that meet the emerging demands of our technology - driven society.

## References

1. Location privacy and its application<[https://www.researchgate.net/publication/324177819\\_Location\\_Privacy\\_and\\_Its\\_Applications\\_A\\_Systematic\\_Study](https://www.researchgate.net/publication/324177819_Location_Privacy_and_Its_Applications_A_Systematic_Study)>
2. Personal data protection laws in India<<https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d#:~:text=Geo%2DLocation%20Information%3A%20Location%20Information,IT%20Act%20or%20IT%20Rules>>
3. The Digital Personal Data Protection Bill,2023<<https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#:~:text=Highlights%20of%20the%20Bill,goods%20or%20services%20in%20India.>>
4. Data Protection Laws In India<<https://blog.ipleaders.in/data-protection-laws-in-india-2/#:~:text=Data%20protection%20safeguards%20sensitive%20data,of%20Justice%20K.S.%20Puttaswamy%20v.>>

