

*Law Audience Journal, Volume 2 & Issue 5, January 2021,
e-ISSN: 2581-6705, Indexed Journal, Published at
<https://www.lawaudience.com/volume-2-issue-5/>, Pages: 130 to 138,*

*Title: Data Protection-Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.*

Publisher Details Are Available At

<https://www.lawaudience.com/publisher-details/>

| Copyright © 2021 By Law Audience Journal |

(E-ISSN: 2581-6705)

*All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (**Law Audience Journal**), an **irrevocable, non-exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute** it in the **Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.***

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

*For permission requests, write to the publisher, subject of the email must be **“Permission Required”** at the email addresses given below.*

Email: lawjournal@lawaudience.com, info@lawaudience.com,

*Phone: **+91-8351033361**,*

Website: www.lawaudience.com.

Facebook: www.facebook.com/lawaudience

Instagram: www.instagram.com/lawaudienceofficial

*Contact Timings: **5:00 PM to 9:00 PM.***

***Law Audience Journal, Volume 2 & Issue 5, January 2021,
e-ISSN: 2581-6705, Indexed Journal, Published at
<https://www.lawaudience.com/volume-2-issue-5/>, Pages: 130 to 138,***

***Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.***

DISCLAIMER:

*Law Audience Journal (e-ISSN: 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in **Volume 2 & Issue 5** are the original work of the authors.*

*Views or Opinions or Suggestions **(if any)**, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.*

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

*Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.*



'Data is a precious thing that will last longer than the systems themselves'

-Tim Berners Lee

I. INTRODUCTION:

India is at its peak of digital revolution owing to government's emphasis on digitisation, availability of high-speed internet and smart devices in abundance at reasonable rates. The country is living through a digital revolution that has triggered extensive development in the financial sector, business processes, healthcare sector, educational sector, etc. India's robustness lies in its growing economy, core tech competencies supported by a strong tech ecosystem and the pace of digital adoption.

The power of technology has led to tremendous opportunities for boosting the country's progress. Moreover, the COVID-19 pandemic has remarkably accelerated the use of the vital technologies. Every sector is getting digitalized in order to remain relevant and to keep up with the times. Terms like machine learning, artificial intelligence, cloud and blockchain have become the topics of ardent discussions around the globe.

However, the risk of data breach has exponentially increased due to advancement of technology followed by poor security practices. Therefore, there is an urgent need to engage effective security practices, because such data breaches not only harm the personal information, but also violates the fundamental rights of an individual guaranteed by the Constitution.

II. MEANING OF DATA PROTECTION:

In the era of digital transformation, people share sensitive personal data on various digital platforms. Most of us simply click on '*I agree with Terms & Conditions*' without reading the Privacy policy, thereby giving access to our personal data and exposing such sensitive data to risk. This security vulnerability leaves millions of users susceptible to various threats. Data

Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.

protection refers to a set of privacy laws that aim at shielding or safeguarding an individual's personal information and regulating the use, collection, storage, modification, and disclosure of the said information. Various countries across the world have different data protection laws.

However, the European Union's General Data Protection Regulation (GDPR) is regarded as a gold standard for data protection all over the world. The fundamental principles of the Indian Personal Data Protection Bill are widely based on the GDPR.

III. NEED FOR DATA PROTECTION:

Data is becoming more and more valuable, leading to its unauthorized use. Keeping the current situation in mind, implementation of strict data protection laws is of utmost importance:

- a. to prevent violation of an individual's fundamental rights,
- b. to safeguard an individual's freedom related to the data,
- c. to ensure fair and consumer-friendly commerce,
- d. to prevent unregulated and arbitrary use of data, and
- e. to ensure that such regulations act as a foundation on which the data-driven innovation and entrepreneurship flourishes.

IV. LEGAL FRAMEWORK IN INDIA:

IV.I FUNDAMENTAL RIGHT:

Indian law has constantly acknowledged the existence of constitutional right to privacy in the scope of other fundamental rights. Data privacy and protection falls under the ambit of Right to Privacy. Right to privacy is a fundamental right under *Article 21 of the Constitution of India*, as affirmed by a nine-judge bench of the Hon'ble Supreme Court in *Justice K.S. Puttaswamy v/s Union of India*¹. In furtherance of the Judgement, the Supreme Court posted a positive obligation upon the government to enact a legislation that protects the right to privacy.

¹ (2017)10SCC641.

IV.II FORMATION OF COMMITTEE:

The *Personal Data Protection Bill* (“PDP Bill”) will be the first comprehensive law on data protection and data privacy in India, as the government is set to bring the data protection laws under a single legislation. Followed by the historical judgement by the Hon’ble Supreme Court in the Puttaswamy case, the Ministry of Electronics and Information Technology formed a committee for making recommendations on the draft Bill on protection of personal data under the chairmanship of Justice B.N. Srikrishna. The Committee submitted the draft Personal Data Protection Bill to the government in July 2018. At present, a Parliamentary Committee is analysing the bill, in consultation with the stakeholders and experts. Much like the General Data Protection Regulation (GDPR) and in-line with the Puttaswamy judgement, the Bill provides for a consent-based approach while processing the data. The Bill also proposes establishment of the Data Protection Authority of India².

IV.III CURRENT LEGAL FRAMEWORK:

At present, India does not have a dedicated legislation dealing with data protection and privacy, however relevant laws dealing with data protection are:

a. The Information Technology Act, 2000³:

Section 43A of the Information Technology Act, 2000 creates a liability on body corporate to pay damages to the affected individual if there is negligence in maintaining reasonable security practices.

Section 72A of the Information Technology Act, 2000 imposes penalty upon an individual, who secures access to material containing personal information and discloses such information without the consent of the person concerned.

b. Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal Data or Information) Rules, 2011⁴ or the SPDI Rules:

² Chapter 9, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

³ <https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf>.

⁴ https://www.prsindia.org/sites/default/files/bill_files/IT_Rules_2011.pdf.

SPDI Rules grant certain rights to the individuals with regards to their personal data and sensitive personal data. The rules make it mandatory for the body corporates to publish an online privacy policy and obtain consent before disclosure of the personal information.

- c. Consumer Protection Act, 2019⁵ and Consumer Protection (E-commerce) Rules, 2020⁶.
- d. Certain rules imposed by the Reserve Bank of India, Telecom Regulatory Authority of India, and Security and Exchange Board of India.

V. THE PERSONAL DATA PROTECTION BILL, 2019-

OVERVIEW:

V.I APPLICATION:

The Bill shall be applicable to processing of personal data that is disclosed, collected, shared, or processed within the territory of India by the State, any Indian company, any citizen of India or body of persons incorporated under the Indian law. The Act shall also be applicable to processing of personal data by data fiduciaries or data processors, who are not present within the territory of India, if such processing is in connection with any such business that is being carried out within India or is in connection with any such activity that involves profiling of the data principles within India. This Act shall not be applicable to processing of anonymized data.⁷

V.II KINDS OF DATA:

The Bill has categorized the data under three heads– Personal Data, Sensitive Personal Data, and Critical Personal Data.

- a. Personal data means data which pertains to characteristics, traits, or attributes of identity of such natural person, which can be used to identify an individual⁸.

⁵ <http://egazette.nic.in/WriteReadData/2019/210422.pdf>.

⁶ <https://consumeraffairs.nic.in/sites/default/files/E%20commerce%20rules.pdf>.

⁷ Sec 2, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

⁸ Sec 3(28), The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

*Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.*

- b. Sensitive Personal data includes the biometric data, financial data, caste, religious or political beliefs, or any other category of data specified by the government⁹.
- c. Critical Personal Data means such personal data as may be notified by the Central Government to be the critical personal data such as military or national security data¹⁰.

V.III OBLIGATIONS OF DATA FIDUCIARY¹¹:

- Personal data shall be processed for lawful and specific purposes only.
- Collection of personal data shall be limited to the extent of such data that is necessary for the purposes of processing.
- The data fiduciary shall provide data principal with all the necessary details at the time of collecting such data. The necessary detail includes- the purpose for which the data is being collected, the category of personal data being collected, the existence of a right to file complaint with the authority, etc.
- The data fiduciary shall ensure that the data being processed is accurate, complete, and not misleading.
- The data fiduciary shall retain the data only till the time it serves the purpose for which it is being processed.

V.IV RIGHTS OF DATA PRINCIPAL¹²:

The Data Principal shall have the right:

- To obtain confirmation whether the data fiduciary is processing or has processed the personal data of data principal.

⁹ Sec 3(36), The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

¹⁰ Explanation to sub-sec 2 of Sec 32, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

¹¹ Secs 4 to 11, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

¹² Secs 17 to 21, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

*Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.*

- To correct the data, if the data being processed is inaccurate, misleading, incomplete, or outdated.
- To data portability.
- To prevent continued disclosure of personal data by a data fiduciary.

V.V GROUNDS FOR PROCESSING DATA¹³:

<u>Personal Data</u>	<u>Personal Sensitive Data</u>
a) On consent	a) On explicit consent
b) For functions of the State	b) For functions of the State
c) In compliance with law or any order of the court/ tribunal	c) In compliance with law or any order of the court/ tribunal
d) For prompt action	d) For prompt action
e) For employment related purposes	
f) For other reasonable purposes	

V.VI EXEMPTIONS¹⁴:

- Processing of personal data shall not be permitted unless authorized by law, in the interest of security of state.
- Processing of personal data shall not be permitted unless authorized by law, in the interests of detection, investigation, prevention and prosecution of any offence.

¹³ Secs 12 to 15, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

¹⁴ Secs 35 to 40, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.

- Processing of personal data shall be exempted from certain provisions of the Act, if such disclosure is necessary for enforcing any legal right or claim or for the purposes of research, archiving or statistical purposes.
- Processing of personal data shall be exempted from certain provisions of the Act if a natural person is processing such personal data for purely personal or domestic purposes.
- Processing of personal data shall be exempted from certain provisions of the Act where such data is relevant to a journalistic purpose.

V.VII PENALTIES¹⁵:

The Act prescribes certain penalties ranging from five crore rupees or two percent of the total worldwide turnover of preceding financial year to fifteen crores rupees or four percent of the worldwide turnover (whichever is higher) for data fiduciaries if they contravene the obligations mentioned in the Act. Data fiduciary shall also be liable to pay a penalty of five rupees per day if he fails to comply with requests of data principal, and if the default continues, he shall be liable to a penalty of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

VI. JUDICIAL ACTIVISM:

Indian judiciary has played an effective role in shaping the concept of data protection across the country. Courts have constantly acknowledged the existence of constitutional right to privacy in the scope of other fundamental rights. Indian media and courts have openly expressed their concerns regarding the issue of data protection and privacy in the country.

In certain notable cases namely, *Kharak Singh vs. State of Uttar Pradesh*¹⁶ and *MP Sharma vs. Satish Chandra*¹⁷, the Supreme court stated that the privacy of an individual needs to be

¹⁵ Secs 57 to 61, The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

¹⁶ 1963 AIR 1295.

¹⁷ 1954 AIR 300.

Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.

protected. In August 2017, the Supreme Court of India delivered the most celebrated judgement regarding data privacy and protection in the case of *Justice K.S. Puttaswamy and Anr. vs. Union of India and Ors.*, whereby a nine-judge bench unanimously held that ‘the right to privacy was an intrinsic element of Article 21 of the Constitution of India.’ Justice Puttaswamy reformed the contours of Indian privacy law, thereby raising the spectre of a robust law on privacy.

The Supreme Court further clarified that if any other law encroaches upon the right to privacy, such law would be subject to constitutional scrutiny and such law shall also fulfil the three-fold requirement for: legality, necessity and, proportionality.

VII. DATA PROTECTION ACROSS THE GLOBE:

The enforcement of the General Data Protection Regulation (GDPR) marked a global shift for data privacy, creating demand for personal data protection, heavier penalties for companies, individuals and governments regulating the technologies that pose a threat to data security. Several US states have passed their own federal laws regarding data protection.

California has recently enacted California Consumer Privacy Act (CCPA) to enhance privacy rights of its citizens and ensure consumer protection. Like India, many countries have now realised the importance of regulating the data and keeping it safe. The State and government machineries are in the process of putting strict legislations in place.

VIII. CONCLUSION:

It is very rightfully quoted by Ronal H. Coase that, ‘If you torture the data long enough, it will confess.’

To put it in simple words, no individual, company, body corporate or even the government can escape the harsh consequences of law, if they compromise with the security of data. India and other countries across the globe have embraced themselves to face the challenge of unlawful

***Title: Data Protection–Indian Outlook,
Authored By: Shivangi Gambhir, Advocate, ILS Law College, Pune,
Author's LinkedIn Profile: <http://linkedin.com/in/shivangi-gambhir-4941a9115>, Email Id: shivangi.gambhir@gmail.com.***

data breaches by enacting strict legislations and making a way for regulating the use of data. The amount of information being processed is growing exponentially each passing minute, and the world is yet to see an effective mechanism to control widespread exploitation of data.

In India, there is an urgent need to engage effective security measures to curb the exploitation of data. Joint efforts of the Parliament and the Technology sector are required to regulate the use of data.

The Personal Data Protection Bill is yet to see the light of the day however, it will surely have huge commercial and political consequences for the country.