



The term Artificial Intelligence coined by American Computer Scientist John McCarthy is a field that deals with Machine Learning and its ability to respond to certain behaviours. Artificial Intelligence aims to make machines do human-like tasks such as visual perception, speech recognition, decision-making, and translation between languages. Artificial Intelligence is an umbrella term that encompasses within itself technologies like machine learning, natural language processing, robotics as well as machine vision. There have been many important developments in the field of Artificial Intelligence. ChatGPT stands for Chat Generative Pre-Trained Transformer is one such development. This is a search engine designed by the Company called 'Open AI' and specializes in providing information in a human-like manner.

This vast accessibility of ChatGPT comes with a vast database of knowledge, so much so that ChatGPT completed MBA exams posted by the Professor of Wharton School of Business.

The application is also equipped to provide well-developed professional e-mails, articles, etc. which otherwise would require an application of mind. But there have been concerns about the amount of personal information that the Bot was accessing while trying to put up the best possible outcome for an individual user.

Currently, India has no specific Laws regulating Artificial Intelligence in India, this article explores the current atmosphere regarding Artificial Intelligence in India, and the need for the required Artificial Intelligence Laws, especially provisions related to Data Security, considering recent developments of AI Chat Bots like ChatGPT.

- What is ChatGPT?
- Data protection laws in India

- Cybersecurity regulations in India and compliance requirements for chatGPT
- The Need for Ensuring Compliance
- Conclusion
- FAQs
- What is India's IT legal framework, and how does it impact ChatGPT?
- What is the data protection law in India, and how do they apply to ChatGPT?
- What are the cybersecurity regulations that ChatGPT needs to comply with in India?

What is ChatGPT?

ChatGPT is a highly powerful Artificial Intelligence Bot developed by "*Open AI*". This is a highly powerful Artificial Intelligence Bot that can understand Human Language and is also capable of producing in-depth writing that is easy to understand. Further, the format of ChatGPT is in the form of Questions and Answers which makes it even more interesting. Moreover, being a free application till date, it has attracted user attention worldwide. Although, a paid version of the application termed ChatGPT Plus has been launched in the USA that can be accessed for US \$20.

Data protection laws in India

Data protection is a complete set of privacy laws, policies and procedures that aims at minimizing the intrusion in one's privacy that is caused by the collection, storage as well as dissemination of personal data. Personal Data refers to the information that can be used to identify an individual, to whom that data belongs, whether collected by the government or collected by any private agency. The Fundamental Right to Privacy has not been granted explicitly in our constitution but the judiciary has interpreted the Right to Privacy to be an integral part of other fundamental rights such as the Right to Life[1] under Article 21[2]. But, unlike European Union's GDPR[3], India does not have personal data protection legislation yet.

Although, recently in November 2022; around the same timeline of unveiling ChatGPT by *Open AI*; Indian Government published the recent draft of the Digital Personal Data Protection Bill, 2022[4]. This was released on 18th November 2022.

In absence of specific Artificial Intelligence laws in India, we must count on enactment of Digital Personal Data Protection Bill, 2022; to bring the required data privacy in India.

Cybersecurity regulations in India and compliance requirements for chatGPT As discussed earlier, concerns regarding the amount of information that ChatGPT collects exist, but users continue to voluntarily provide information to ChatGPT for various purposes, ranging from their need to obtain required information or answers to simply test the application.

Further, it is an important consideration that, one of the primary features of the very application is that it simply studies the behaviour of the user, in order to generate the most appropriate output for them, but the question persists, to what extent the application can avail personal information of a user in order to create or generate the right output for them? And due to lack of proper Data Security Laws, India needs Digital Personal Data Protection Bill, 2022[5]; to be implemented as soon as possible.

Current, legislations in India, that provide somewhat protection include:

1. The Information Technology Act 2000[6]
2. Information Technology (Amendment) Act 2008[7]
3. Information Technology (SPDI) Rules 2011[8]

ChatGPT as of now, needs to comply with the aforementioned set of regulations. In addition, as far as Cyber Security in India is concerned, organizations that choose to use ChatGPT must comply with National Cyber Security Policy, 2013[9].

The Need for Ensuring Compliance

ChatGPT undoubtedly has the potential to revolutionize the communication as well as information exchange in today's world. It can be used for several purposes, to write your e-mails, your exams and even write lyrics for you. A lot of internet giants today are taking interest in AI chatbot technology, like Microsoft and Amazon.

These AI language Chat Bots have revolutionized the industry and are helpful in manifold sectors such as Finance, Healthcare and Education. Although the technology is not perfect, it is known to have provided inaccurate information, and sometimes even offensive responses to users. There is a need to understand that as AI technology gets more sophisticated, it poses future cyber risks and so does ChatGPT.

Hence, first of all, India needs a strict Data Security regime like GDPR[10], and must have regulations to make sure that privacy policy of these companies protect the users and that users are bound by an ethical code, that is not only hard to circumvent but comes with strict punitive actions against the user, which again needs global co-operation and communication considering that a lot of cyber criminals live beyond borders.

Conclusion

We must not inhibit the growth of technology, but it is important to regulate this technology. There must be monitoring of AI platforms to detect suspicious activity. This is because these bots are worthy of the focus of regulators. AI is continuously making utter disruptions in human life, and in the years to come, it shall hold the power to transform individuals, economies as well as societies at large. Hence, it is the need of the hour to bring required and stringent regulations in form of Artificial Intelligence Laws to establish controlled use as well as misuse of AI and ensure Cyber Security in India, especially the data protection laws must be well framed so that valuable personal data of individuals is not compromised.

FAQs

What is India's IT legal framework, and how does it impact ChatGPT?

India has several laws and regulations that govern the IT sector, including the Information Technology Act, 2000 (IT Act), the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Personal Data Protection Bill, 2019 (PDP Bill), which is currently under consideration.

The impact of India's IT legal framework on ChatGPT will depend on various factors such as the nature of ChatGPT's operations, the type of data it collects and processes, and its compliance with the relevant laws and regulations.

ChatGPT may need to comply with data protection requirements, appoint a grievance officer, and implement processes to address user complaints. Failure to comply with the applicable laws and regulations could result in penalties and legal liabilities.

What is the data protection law in India, and how do they apply to ChatGPT?

The vast amount of data that is collected by Artificial Intelligence technology can be potentially used for dangerous purposes such as targeted

advertising, political manipulation and identity theft. The concerns exist around data privacy, protection and bias; as the training data that is used to train the model might consist of sensitive or personal information, and such biases in the data can lead to biased responses from the model itself. ChatGPT applications can store and process data and hence it is highly important that there must be laws for the protection of data. And it is also important to make sure that ChatGPT is compliant with existing laws and regulations. European Union has General Data Protection Regulation (GDPR) in place, which regulates the use of personal data and requires data to be collected for specific purposes only. India is yet to have DPDP Bill be converted into an Act and implemented. Till then, the following laws must be complied with for data protection:

1. The Information Technology Act 2000
2. Information Technology (Amendment) Act 2008
3. SPDI Rules 2011

What are the cybersecurity regulations that ChatGPT needs to comply with in India?

As of now, no existing legislation offers solutions to the cybersecurity threats that ChatGPT poses. Although, National Cyber Security Policy, must be used by organizations that intend to use ChatGPT to help themselves with cyber security. But it is expected that long awaited Digital India Bill, which is a revamp of the, will bring forth solutions for dealing with security concerns regarding AI Platforms like ChatGPT.

[1]Justice K. S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors, AIR 2017 SC 4161

[2]INDIA CONST. art. 21

[3]Regulation (Eu) 2016/679 of The European Parliament and of the Council; No. 27, The European Parliament, 2016 (European Union)

[4]The Digital Personal Data Protection Bill, 2022; (2022)

[5]*Ibid*

[6]The Information Technology Act 2000, No. 21, Acts of Parliament, 2000, (India)

[7]The Information Technology (Amendment) Act 2008, Acts of Parliament, 2008 (India)

[8]Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011; Notification of Ministry of Communication and Information Technology, 2008 (India)

[9]National Cyber Security Policy, 2013,

https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

[10]Regulation (Eu) 2016/679 of The European Parliament and of the Council; No. 27, The European Parliament, 2016 (European Union)

King Stubb & Kasiva,

Advocates & Attorneys

[Click Here to Get in Touch](#)

[New Delhi](#) | [Mumbai](#) | [Bangalore](#) | [Chennai](#) | [Hyderabad](#) | [Mangalore](#) | [Pune](#) | [Kochi](#) | [Kolkata](#)

Tel: [+91 11 41032969](tel:+911141032969) | Email: info@ksandk.com