



Artificial Intelligence and Law in India

Ashutosh Kumar is an Assistant Professor, Amity Law School, Amity University Patna

Abstract

The world has accepted Artificial Intelligence technology use as a major panacea to many problems. It has reduced human suffering and burden and brought a revolutionary change in our modus-Operandi. Today AI (artificial intelligence), is a voice of working ethics in every sector be it agriculture, health, education, banking sector, all are in process of adoption of AI technology. But can AI be deployed everywhere, is it completely safe, this raises the question of ethics and law. AI and cyberspace have raised serious privacy issues along with increasing cybercrimes. In India, AI is being seen as a major game-changer for the economy and progressive development of the region. This paper attempts to cover the legal control of AI in India and regulation concerning artificial intelligence and cyberspace in light of privacy along with digital economy dependence on AI.

KEYWORDS: *Artificial Intelligence, Cyber-Space, Digital economy, Right to privacy.*

Artificial intelligence in India is at a nascent stage as being a developing country the arrival of this technology is late. This technology is attributed to technological advancement in the 21st century where the rise of social networking sites and International multinational corporations investment in India has embarked on research and development in the field of artificial intelligence. As we can see this emerging amazing technology which works on the thinking process of a human being. Today we can see the global application of artificial intelligence in every sector of the economy. It has not only reduce the burden but has also increased the working efficiency based on smart technology. As the Indian government through its policy-making body, Niti Aayog has laid down stress use of artificial intelligence². At present India is

lacking an adequate legal framework on artificial intelligence, but in the indirect form, it is utilizing Information Technology Act 2000, for the application of artificial intelligence control and governance. Recently the government has passed the data protection bill 2019. to give shape to its digital governance and privacy-related issue relating to data as well as cyberspace which will directly include the use of intelligence and ethics attached to it..

² <https://niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>

Relationship between artificial intelligence, digital Governance, and Privacy

India has seen a sharp rise in cybercrime and privacy risk vulnerability with the advent of artificial intelligence and digital governance in absence of concrete data protection law. As use of artificial intelligence, cyberspace and digital governance adoption without data protection law is proving to be heaven for cyber fraud and personal information sharing business. The best example may be explained through an example when you search any commodity or consumer goods or service on the internet you start getting a huge number of calls and emails on your email-id and mobile number. This is an example of an invasion on privacy and personal information. This is how artificial intelligence, read and penetrate in the minds of the user which often make layman a prey to a vulnerable situation such as banking fraud, theft of money from an account. When any person share his personal information on Facebook, Twitter Whatsapp etc. All the information is easily identified by AI and processed in a different form by market operators, which is an attack on digital privacy as well as personal privacy. The relationship between artificial intelligence and digital governance shows that both the variables are linked to Information Technology law. Therefore it can be said that artificial intelligence is one of the aspect of digital governance. This is an apt time that India is moving towards making of regulatory control for activation of its artificial intelligence technology in constructive way. At present, it is very difficult to see that what will be the basic outline for making a regulatory mechanism to bring constructive use cyberspace for controlling the fair use of Artificial Intelligence. No doubt that artificial intelligence is going to revolutionize working efficiency and make humans suffering less by reducing the burden of physical work, be it and health sector, agriculture sector communication sector, and education sector. but at the same time, it has many challenges

in cyberspace and digital governance. Thus it is clear that artificial intelligence is directly related to information technology and part of digital governance.

Regulatory Framework in India

At present Information Technology, Act 2000³ along with Digital Media Ethics Code ⁴ is in force to take care of major privacy online digital and artificial intelligence-based operations in India. As Information Technology Act mandate is primarily directed to provide recognition to electronic commerce and trade under the international obligation of UNCTAD model code⁵ in order give force to digital online e-transaction to be adopted in the market economy to boost trade and commerce. This Model UNCTAD code can be said as a starter to all online banking, trade, commerce across the globe. As a result of which many multi-national corporations and online digital businesses started taking shape and unfolded their wings into operation in transboundary transactions which has no doubt eased the economy and helped in boosting the economy, trade and jobs. But till the early 20th century, nobody knew that this will lead to issue of privacy and cybercrimes. As a result of massive use of advance computing, cloud computing-based application and rise of artificial intelligence-based automated systems and its operations across the globe has made universal entry of AI, which ultimately became ground of privacy threats and made data/information, personal sensitive information on cyberspace more vulnerable. As we all know more challenges are faced by India because of its rising population, which has made it best market economy for investors for online services for the services sector, health sector, banking, trade, etc.

³ Section 43A provides for the protection of sensitive personal data or information ('SPDI') and section 72A protects personal information from unlawful disclosure in breach of contract

⁴ Notification dated, the 25th February 2021 G.S.R. 139(E): the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

⁵ See Preamble of Information Technology Act 2000 Today India has jumped to 10th position in the cyber security index released by ITU⁶ due to its stringent measures on privacy protection policy. But still, India is grappling to bring robust data protection law. As in 2019 it has tabled data protection bill in parliament to deal with the issue of data privacy issues put forwarded by AI and other applications. To cover the risk attached to data protection vulnerability, on the recommendation of Sri Krishna Committee Report⁷ which has highlighted fair use of data principle in digital economy⁸. Thus above-mentioned law is primarily operating to take care of digital governance and privacy-related issues on an online platform which also takes into account the issues of AI⁹. Further sec 65 to sec 79 of IT act specially provides for online misuse of data or crossing the limitation and obscenity use of the online platform. As the word data¹⁰ is defined a set of any information in electronic form. The backbone of data protection and privacy clause is provided in sec 43 A of IT Act that deals with the protection of personal sensitive data¹¹ which directly deals with the major privacy-related issues of online data use such as the use of private/personal sensitive issues dealing with following areas are:

A. Passwords protection and leakage**B. Financial information leak or bank account details sharing by banks****C. Sharing of mental/psychological health condition or making it public without consent****D. The sexual orientation of an individual and disclosing this information without the consent or using it to defame reputation.**

⁶ www.aninews.in/news/world/europe/india-jumps-37-places-to-rank-10-in-global-cyber-security- index20210629201820

⁷ Can be accessed at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

⁸ 2017 Report "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians.

⁹ Sec 67 A Information Technology Act 2000.

¹⁰ Sec 2(0) Information and Technology Act

¹¹ *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. The Rules only deals with the protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to

E. Medical records

All above-mentioned identification constituting personal sensitive information which must be protected and constitute an integral part of the right to privacy as per the Sec 43 A of IT Act, 2000 inclusions, after the amendment has taken care of privacy right protection framework and regulation controlling data and online privacy in India. Further Information Technology Act also provides an intermediary role that is power function and limitation of service providers such that they may not exploit the data or services provided by them and taking advantage¹². Further, the role and function of Intermediaries have been clarified based on liability such as :

A. Intermediaries will ensure encrypted and safe transmission of data.

B. Intermediaries will not make unfair use of personal privacy and the use of data of its customer.

C. Will ensure proper grievance redressal and reporting mechanism in case of data leak or leak of personal information causing unwanted loss

D. Will also be responsible to pay compensation in case of violation of digital media ethics code and as per Sec 79 of IT Act 2000, mandate.

Who is Responsible to protect Online Privacy?

In the Indian republic democratic structure of governance, the state has to protect the privacy of Indian Citizens in all cases be it personal or private, or public information-related citizens. Sec 69 of Information Technology Act provides State utmost sovereign right to intercept pt, intervene and unilaterally subject to exception in the case where sovereignty, integrity, morality, public order, peace, health is at stake state can resort

¹² Sec 79 Of Information Technology Act provides for Intermediaries

to any action to compromise with privacy¹³. As we all know these all exception provides for circumstances that can attract the followings:

- A. Sovereignty
- B. Friendly relations with the foreign state
- C. National security
- D. Public order
- E. Defense

Are highly exceptional situations where a state can resort to any means where no privacy protection will be favored in the above-mentioned reasonable restrictions. Online privacy violations are also fixed in Indian Penal code¹⁴ which provides for stalking and voyeurism, which is a clear case of an attack on the modesty of women and offenses committed online mode which is non-bailable offenses. Further sec 72 provides for breach of online confidentiality which is the essence of privacy and personal agreement between the companies. This shows direct control and regulation of confidentiality clause as well as establishes privacy protection regime. 2008 amendment Act brought a revolutionary change in the privacy regime as it inserted sec 10A to deal with the enforceability of online contract and added several important clauses which are as follows, sec 43 A, sec 66A¹⁵ as this section caused immense misuse by police to arrest any person who expressed freedom of speech and expression as means of fair criticism. As this issue was the real test of conflict between privacy and freedom of speech and expression later on settled in Shreya Singhal case¹⁶.

¹³ Sec 69 of IT ACT 2000.

¹⁴ Sec 354 c ad Sec 354 D, SEC 509 IPC offences related to online crimes agaisnt women

¹⁵ Declared ultra-vires in Case of Shreya Singhal vs Union oF india

¹⁶ (2013) 12 SCC 73

CONCLUSION

As 2008 amendment turned the real application of online digital privacy protection which also checks the AI misuse in India. It highlighted the vulnerable issues of online data theft and cybercrimes related to privacy of Indian citizens and accurately covers fair use of artificial intelligence use in India as AI, inherent part of online application and cyberspace technology which is subject matter of Information Technology Act, 2000. Section 67A¹⁷ Section 67B¹⁸ Section 69A¹⁹ Section 72A²⁰ Section 79²¹, Section 84B²² mentioned provisions proved to be benchmark regulation in the present time that is taking care of online digital privacy administration and framework regulation in India.

Further recommendations of Srikrishna Committee Report (supra) has asked for creation of new separate comprehensive data protection law. In addition Supreme Court has also expressed need for comprehensive welfare based data protection legislation as a reason a bill termed as “**Data Protection Bill 2019**”, was introduced in Lok Sabha, but still it is going through the phase of legislation in process of making²³. As the preamble of the bill provides for details a comprehensive²⁴ law relating to data protection and personal privacy.

¹⁷ Punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.

¹⁸ Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form.

¹⁹ Power to issue directions for blocking for public access of any information through any computer resource.

²⁰ Punishment for disclosure of information in breach of lawful contract.

²¹ Exemption from liability of intermediary in certain cases

²² Punishment for abetment of offences.

²³ <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019>

²⁴ To provide for the protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures in the processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes and matters connected therewith or incidental thereto