PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE: AN INDIAN PERSPECTIVE

By Vatsal Mishra
L.L.M In IPR &amp; Tech. Law
From O.P Jindal Global Law School

By Aakrati Garg
L.L.M In IPR &amp; Tech. Law
From O.P Jindal Global Law School

By Vivek Kumar
L.L.M In IPR &amp; Tech. Law
From O.P Jindal Global Law School

Introduction

Artificial Intelligence (AI) aspires to create a positive paradigm shift in technology by enhancing our digital and physical worlds with new features and tailored experiences. Almost all of our digital services and physical products will be augmented in the future by AI to improve their functionality. However, since developing artificially intelligent models requires a vast quantity of data, it puts user privacy at risk. The growing popularity of AI encourages data collecting, posing a danger to privacy.[1]

While these applications have exploded in popularity recently, the research and development of AI dates back more than half a century: the phrase was created in 1956, while the idea dates all the way back to the late 1700s. The current momentum is being fuelled by the availability of vast quantities of data, inexpensive and accessible processing power, continuing development of statistical methodologies, and the fact that technology has become ingrained in society's fabric.[2] When used correctly, artificial intelligence may be beneficial to society. However, as is the case with the majority of developing technologies, there is a serious possibility that commercial and governmental usage may have a negative influence on human rights. These technologies' applications usually depend on the development, gathering, processing, and sharing of massive quantities of data about both individual and group behaviour. Individuals may be profiled and future behaviour predicted using this data.

The report defines essential technical terms to help understand the argument and examines how AI affects the right to freedom of speech and the right to privacy, as well as highlighting major concerns. It then discusses the present state of AI governance, examining several existing legal, technological, and corporate frameworks, as well as industry-led AI projects addressing issues of free speech and privacy. Finally, the author makes preliminary recommendations for rights-based solutions that civil society organisations and other stakeholders might explore in their AI advocacy efforts.

[1] DH. Autor, *The skill content of recent technological change: an empirical exploration* 118(4) THE QUARTERLY JOURNAL OF ECONOMICS 1279, 1312 (2003).
[2] S. Chatterjee, *Artificial Intelligence and Human Rights: From Socio-Legal Perspectives*, INTERNATIONAL CONFERENCE ON LAW AND TECHNOLOGY [ICLT 2019] SCHOOL OF LAW, THE UNIVERSITY OF PETROLEUM & ENERGY STUDIES (2019).

Effect of AI on Privacy

The emergence of artificial intelligence (AI) has added to the complexity. Consumers are confronted with long and complicated user agreements that they must approve quickly. They do, however, accept the user agreements without recognising the extent of privacy rights they may be giving up. Whatever information people disclose these days ends up in massive databases that are mined for a variety of purposes, such as purchase suggestions, marketing possibilities, or other comparable activities. Data retrieved by voice recognition or face recognition programmes is capable of monitoring all of our movements in real time. Several smart appliances and equipment, such as motion-sensing electrical devices, thermostats, and smart TVs that continually gather data, may also follow your activities in real time.[3]

These instruments offer critical services, but they also pose additional concerns. AI requires massive amounts of data, giving third-party platform owners even more motivation to follow, analyse, and profile people and their habits. In conjunction with other AI applications, facial recognition may be utilised for more and deeper monitoring. These developments present various privacy issues for customers.[4]

Is it Possible to Protect Privacy?

The use of artificial intelligence in promoting prejudice is extensively established and is one of the most contentious subjects in contemporary ethical debates. Privacy is a basic human right that is necessary for maintaining human dignity. Additionally, the right to privacy bolsters other rights, such as the freedom of speech and association. Numerous countries and localities already view data protection as a basic right. Data protection is mainly concerned with safeguarding any personally identifiable information about you. It is inextricably linked to the right to privacy, and may even be considered a subset of it under the UN human rights framework. AI systems are often taught by gaining access to and analysing large data sets.[5] Additionally, data is gathered to provide feedback mechanisms and to allow calibration and continuous modification. This data collecting infringes on individuals' rights to privacy and data protection. The analysis of data by AI systems may disclose private information about persons, which counts as protected information and should be regarded as such, even if it is obtained from large data sets fed by publicly accessible data. For instance, researchers have created machine learning models capable of reliably estimating a person's age, gender, employment, and marital status only based on their mobile phone location data. Additionally, they were able to forecast a person's future position based on their prior behaviour and the

[3] *Ibid* at 102.

[4] S. Chatterjee, *Emergence of AI and its implication towards data privacy: From Indian legal perspective*, INTERNATIONAL CONFERENCE ON JUSTICE EDUCATION: ARTIFICIAL INTELLIGENCE AND ITS LEGAL IMPLICATION (2019).

[5] MD. Prasad, *The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law* 28(1), INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 1, 13 (2020).

location data of their acquaintances. To preserve human rights, this information must be handled similarly to other personally identifiable information.[6]

In the lack of a clear statute, India's data protection laws are made up of a patchwork of judicial and legislative decisions. 'Reasonable security methods' for 'sensitive personal data or information' are detailed in the IT Act, 2000, which deals with cybercrime and e-commerce, under section 43A.[7] These regulations restrict the ability of organisations to acquire, use, keep, and disclose the personal data of people and require them to have a privacy policy. The disclosure-with-consent provision is rendered ineffective when the information sought comes from a government entity, therefore these regulations are not without their flaws. They only apply to corporations. As a result, people have very limited control over their personal information since the IT Rules exclude the government from its scope. Laws in India were re-evaluated after a 2012 petition alleging that the Aadhar system violated the right to privacy was filed. 'Right to privacy' was recognised a basic right of all people by the Supreme Court in the historic Puttaswamy decision in May 2017. A data protection framework for India was drafted by an expert group headed by Justice BN Srikrishna after the Indian government realised the need of protecting personal information.

Puttaswamy Judgement and Lack of Foresightedness

A chilling effect might be had on our capacity to take full use of current technology because of the tests they've laid out and the restrictions they've set in the landmark judgement of KS Puttaswamy v. UOI. Justice Sanjay Kishan Kaul and Justice D.Y. Chandrachud, both of whom advocate for balancing the advantages of data mining with the person's right to privacy, propose a framework for protecting individual autonomy based purely on permission. However, although they seem to be aware of the advantages that big data might offer us, they tend to be oblivious to the chilling impact that a stringent notice and consent-based structure can have on these businesses.[8]

Because of its reliance on precedent, the common law system has a flaw that may be exploited by those who are not familiar with the system. As a result, they are unable to come up with ideas for the future that are not tied to the past. This is why a common law judge is so terrible at coping with disruptions. Unprecedented disruptive transformation is taking place right now. Previously, it was sufficient to protect personal privacy by restricting the collection of data, but as the number of devices and systems that continually collect information from us grows, consented collection is entirely infeasible.[9] Additionally, we are able to benefit from emerging technologies that

[6] *Ibid.*

[7] J. McCarthy, *Privacy is Fundamental Rights* (2017) NPR, https://www.npr.org/sections/thetwo-way/2017/08/24/545963181/indian-supreme-court-declares-privacy-a-fundamental-right (Last accessed on November 7, 2021).

[8] N. Gruschka, V. Mavroeidis, K. Vishi, and M. Jensen, *Privacy issues and data protection in big data: A case study analysis under GDPR*, IEEE Int'l Conference on Big Data 5027, 5031 (2018).

[9] Prasad *(n* 5).

utilise the power of data in order to improve our quality of life. In order to perform their magic, many of these new technologies rely on big data and machine learning, which in turn need access to massive data sets. If data controllers are required to limit themselves by proportionality and purpose, this might have a chilling impact on emerging business models.

The 'Arogya Setu' App fiasco and similar cases

Following a large public outcry, the government addressed the legality and usage of the ***Arogya Setu app*** on a best effort basis in the context of privacy by the government. The lack of Bluetooth technology requirements, algorithms and artificial intelligence systems, and no indication of the private parties participating in the app's creation is glaring. Before the app's debut, there was no statutory framework in place. If any of the registered user's contacts test positive for Covid-19, the app claims to be able to determine the user's risk of infection based on complex factors. We don't know what "advanced parameters" are since technology systems of this sort are still under development.

An inadequate demonstration of the privacy-first system that would safeguard the sensitive personal data of users via encryption and security has been provided. The app's implementation committee did not include any public health professionals. App's functionality and architecture are being challenged since the app lacks a sufficient legal policy framework, and its firewall is built in a public-private collaboration, raising concerns about its data security.

Notably, privacy has also been used as a justification in the well-known instances of the reading down of Section 497 of the Indian Penal Code and the ruling of Section 377 of the Indian Penal Code as unconstitutional. [10] After the Puttaswamy judgement, the domain of privacy has expanded exponentially. The decision was seen as a leveller of privacy rights versus the rest of the globe. However, in this age of technological boom and data dynamics, privacy enforcement against non-state actors has been woefully inadequate. The present legislation, such as the Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011, have proven mechanically inadequate in protecting our privacy.

With the type of technological change, we're seeing and the increased monetary value placed on data, India's privacy legislation is in disarray. In some ways, privacy has become a fantasy right with a corporate perspective. Structured enforcement is urgently needed. The State should fulfil its affirmative commitment and, in order to expedite its approach, pass the long-delayed Personal Data Protection Bill, 2019.[11]

At the moment, the nation is operating in a legal vacuum, with only precedents to guide us and no specific legislation addressing finer conceptions of privacy. The Committee of Experts on Non-Personal Data Governance Framework recently issued its report, which

[10] D. Joshi, *Personal Data Protection Bill strikes a discordant note on 'non-personal data'* (2020) The Indian Express,< http://14.139.58.147:8080/jspui/handle/123456789/1511 >(Last accessed on November 7, 2021).

[11] Autor *(n* 1) 1279, 1312 .

proposed that a separate statute be drafted to control non-personal data via a new regulatory organisation. The government's start in this direction is commendable, but efforts must produce results.[12]

Personal Data Protection Bill vis-à-vis Artificial Intelligence and Transparency

While the Personal Data Protection Bill confers important rights and safeguards on people, it also makes exercising these rights more complex. By giving people more control over their personal data and the ways in which it is used, as well as by making structural reforms targeted at organisations that utilise personal data, the Bill significantly reduces the impact of automated judgments. Furthermore, the Bill provides people with a limited right to access and correct personal data, which includes inferences for profiling purposes. As a result, profiling is described as "any processing of personal data that analyses or forecasts characteristics of a data principal's behaviour, qualities, or interests." Thus, the Bill explicitly addresses profiling of persons by automated processing and enables some degree of control over such profiling for individuals. There are certain precautions against profiling and decision-making, but they are only applicable to personal data judged to be "sensitive," allowing the Data Protection Authority to designate specific "additional measures" against profiling.

It is imperative that we strengthen our defences against automated judgments in order to be effective in this new age of "AI". Due process is a legal tradition that assures that judgments affecting persons have certain procedural guarantees that are crucial to guaranteeing that they are fair and non-arbitrary. One means of expanding such protection would be to draw from it. As a part of these protections, citizens have a right to know why a decision was made, as well as access to material used in making the decision. They also have the right to challenge or appeal a judgement. Automated decision-making should be subject to substantial human monitoring if there are no legislative protections in place for people's rights in the absence of such safeguards.

However, putting the task of rebutting judgments squarely on the shoulders of affected persons would not suffice. To alleviate this burden, data privacy legislation such as the PDP Bill might include structural safeguards that guarantee automated profiling is both fair and transparent. These safeguards may include, but are not limited to, regular audits of the data and procedures used in profiling to guarantee their robustness and prevent systematic prejudice. Additionally, the logic or rules governing automated data processing for the purpose of proofreading must be visible by default. Different degrees of protection may be provided in different situations, depending on the possible damage to the decision's subject. The primary difficulty after the adoption of PDPB will be to transform legislative concepts into technical execution utilising current technology. The most difficult aspect of developing a data protection framework is translating legislative responsibilities into a technology platform. Numerous stakeholders, including legal experts, law enforcement agencies, software architects, developers, requirement analysts, and security and privacy specialists, are involved in the endeavour. They must work together

[12] *ibid* (*n*11).

toward a common objective of achieving data protection privacy by design. There is a strong conflict between the way products are developed in the software sector and the legal precepts of the data protection framework. Numerous constraints and obstacles exist in the legal framework, making implementation challenging.[13]

Conclusion and Findings

Over the last several years, India's IT industry has seen enormous expansion. Along with the IT industry, the usage of social media has grown at a rapid pace. Not only that, but the current administration is eager to expand the IT industry and has launched programmes such as Digital India, Digital Cloud for Citizens, Smart Cities, and so on. People in the globalisation period use ICT through the internet. The majority of individuals access the internet through computers or smartphones. When Indian customers are requested to disclose their personal information to service providers in order to enjoy continuous and free internet services and access to certain social media sites or applications, they willingly do so. All of these personal records are being maintained on servers outside of Indian territory, which is causing concern for the Indian government. In this day and age, when information technology is moving at breakneck speed, there is always the risk of foreign firms misusing data.[14]

The security of personal data has become a big problem. The government's choice to propose such a measure has long-term consequences. It has both advantages and disadvantages. As a result, soon after the law was tabled in parliament, it drew a slew of complaints from a variety of quarters. Though it has certain positive elements, as indicated by the government, this law allows the government to access private or government agency data at any moment for reasons of sovereignty or public order. This might have serious consequences. It may infringe on the right to privacy. Given the importance of data privacy as a basic right of citizens and the economic consequences of possible data breaches, the government should evaluate all of the pressing problems listed above. A strong personal data protection legislation is urgently needed. Public awareness, greater implementation and regulation, and quick grievance redressal must all be prioritised.[15]

Recommendations

Data analysis, employment, healthcare, IoT, transportation and so on are all domains where AI algorithms are increasingly being used. This means that the AI will have much easier access to Personally Identifiable Information (PII) (PII). A better understanding of prospective customers' tastes would be gained as a result. It demonstrates the degree to which AI has affected PII. Analysis of data is being performed by AI for several socially beneficial applications. However, the ease with which AI may access personal data raises wider worries about privacy. For this reason, it is imperative that a comprehensive framework and policy be developed to handle

[13] R. Govind Singh, S. Ruj, *A Technical Look at the Indian Personal Data Protection Bill* (2020), https://ui.adsabs.harvard.edu/abs/2020arXiv200513812G/abstract (Last accessed on November 7, 2021).

[14] Prasad (*n* 5).

[15] *Ibid.*

the privacy issues associated with AI. In light of the Supreme Court of India's recent decision, this issue has grown more urgent.

India's regulatory authorities need to strike a delicate balance between protecting residents' privacy and promoting the use of AI technology, in order to counteract the current threat to the country's economy. If this balance isn't achieved, it might either harm the privacy of people when it comes to their personal data, or it could harm India's technical advancement, resulting in a slowdown in the country's overall economic progress. As a result of a lack of effective jurisprudence in India, it is expected that in the near future appropriate, comprehensive, executable and simple enactments and policies will be formed so that through increased use of AI applications the technological growth can reach its apex of success without compromising on data privacy issues.

*****