National Journal of Advanced Research
www.multidisciplinaryarticle.in
ISSN: 2455-216X
Received: 14-05-2023, Accepted: 29-05-2023, Published: 14-06-2023
Volume 9, Issue 1, 2023, Page No. 31-36

The intersection of law and technology: Online privacy and personal data protection

Aastha Singhal, Ashish Guwalani
Advocate, Rajasthan High Court, Jaipur, Rajasthan, India

Abstract

"Law and technology produce, together, a kind of regulation of creativity we've not seen before."

~ Lawrence Lessig

The interplay of law and technology has carved a path towards revolutionizing of Ideas but at the very same time it has become a critical issue that needs to be addressed in the modern era of data-driven technologies. The advent of the internet has revolutionized the way we share, store, and process information. However, this new era of technological advancement has come with significant risks to individuals' privacy, security, and data protection. In order to combat the repercussions associated with this heinous medium, the government have passed laws and regulations aimed at protecting personal data and online privacy requiring organizations to obtain explicit consent from individuals before collecting and using their personal data and to implement measures to ensure the security of this data. The purpose of this paper is to make people aware of the dark side of technology which can be a threat to not only individuals but also the nation as a whole. This paper further houses as to how the law regulates the online privacy protection to the individuals and the organisations, the absence of check and balance and proper implementation with its implications of violation of digital privacy on women, the challenges faced by the society at an individual level and the steps to be taken to overcome these challenges.

Keywords: data protection, right to privacy, digital technology

Introduction

In today's digital age, the internet and digital technologies have transformed the way we live, work, and interact with others. While these technologies have brought numerous benefits, they have also given rise to concerns related to online privacy and personal data protection.

Online privacy refers to an individual's right to control the collection, use, and disclosure of their personal information on the internet. Personal data protection, on the other hand, involves protecting individuals' personal information from misuse, unauthorized access, and other forms of abuse.

The increasing use of technology and the internet has resulted in an explosion of personal data being collected and shared online. This has led to growing concerns about how this information is being used and who has access to it. Online privacy and personal data protection have therefore become critical issues that need to be addressed to ensure that individuals have control over their information, can make informed decisions about sharing their information, and prevent any potential harm.

Online Privacy is serious concern not only for individuals but also for governments, companies, and society as a whole. The protection of personal data is essential to safeguard privacy, prevent identity theft, fraud, and other forms of cybercrime. As such, governments and companies need to take steps to protect personal data and promote responsible data use, while individuals need to be aware of the risks and take steps to protect their own privacy.

Online privacy refers to the ability of individuals to control the information they share about themselves on the internet, and to prevent that information from being misused or mishandled by others. This can include personal information such as names, addresses, phone numbers, email addresses, and financial information, as well as sensitive information such as health and medical records, political views, and other private details.

Online privacy is becoming increasingly important in today's digital age, as more and more people are using the internet to communicate, shop, and conduct their daily lives. Without adequate online privacy protections, individuals may be at risk of identity theft, cyberbullying, online harassment, and other forms of privacy violations. Therefore, it is essential for individuals to be able to control the information they share online and to be aware of the risks and potential consequences of sharing personal information on the internet.

Personal data protection refers to the measures and processes used to safeguard the privacy and confidentiality of individuals' personal information. This can include data such as names, addresses, phone numbers, email addresses, financial information, health and medical records, and other sensitive information.

Personal data protection is essential in today's digital age, where personal information is often collected and processed by companies and organizations for various purposes. Without proper protection, personal data may be vulnerable to theft, misuse, or mishandling, which can lead to identity theft, financial fraud, reputational damage, and other forms of harm to individuals.

To ensure personal data protection, many countries have implemented laws and regulations that require organizations to collect, store, and use personal data in a responsible and transparent manner. These laws may require organizations to obtain informed consent from individuals before collecting or processing their personal data, to implement appropriate security measures to protect the data, and to provide individuals with access to their personal data and the ability to request its deletion or correction.

Overall, personal data protection is essential for safeguarding individuals' privacy and ensuring that their personal information is used in a responsible and ethical manner.

While the terms "online privacy" and "personal data protection" are related, they are not interchangeable and refer to different aspects of data privacy.

Online privacy refers to the ability of individuals to control the information they share about themselves on the internet and to prevent that information from being misused or mishandled by others. This can include personal information such as names, addresses, phone numbers, email addresses, and financial information, as well as sensitive information such as health and medical records, political views, and other private details. In other words, online privacy is about protecting an individual's personal information from being accessed or misused by others, especially when using the internet.

On the other hand, personal data protection refers to the measures and processes used to safeguard the privacy and confidentiality of individuals' personal information. This can include data such as names, addresses, phone numbers, email addresses, financial information, health and medical records, and other sensitive information. Personal data protection is about ensuring that an individual's personal data is collected, processed, and used in a responsible and ethical manner, and that appropriate security measures are in place to protect the data.

In response to these concerns, many countries around the world have implemented laws and regulations aimed at protecting personal data. For example, the European Union's General Data Protection Regulation (GDPR) is one of the most comprehensive data protection laws in the world, and it gives individuals greater control over their personal data.

Similarly, in the United States, the California Consumer Privacy Act (CCPA) has been enacted to provide consumers with certain rights over their personal information, including the right to know what personal information is being collected, the right to request that their personal information be deleted, and the right to opt-out of the sale of their personal information.

However, despite these laws and regulations, there are still many challenges to ensuring online privacy and personal data protection. For example, many companies continue to collect and use personal data without obtaining proper consent or providing clear explanations of how the data will be used.

In addition, the rise of artificial intelligence and machine learning technologies has created new challenges for data protection, as these technologies often require access to large amounts of personal data in order to function effectively.

Legal measures for ensuring online privacy protection

In India, there are several laws and regulations related to online privacy and personal data protection. Some of the Laws mentioned below

1. **The Information Technology Act, 2000:** This is the primary law governing online privacy and personal data protection in India. It includes provisions related to the unauthorized access and interception of electronic data, the misuse of computer systems, and the protection of sensitive personal information.

2. **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:** These rules were enacted under the Information Technology Act, 2000 and prescribe the reasonable security practices and procedures to be followed by companies and organizations while collecting, storing, processing, and transferring sensitive personal data or information.

3. **The Aadhaar Act, 2016:** This is a law that governs the use of Aadhaar, a biometric identification system used in India. The act includes provisions related to the protection of personal information collected under the Aadhaar system, the use of the system for authentication and verification purposes, and the penalties for misuse of the system.

4. **The Consumer Protection Act, 2019:** This is a law that seeks to protect the interests of consumers in India and includes provisions related to the protection of personal data and privacy of consumers while availing of goods and services.

5. **The Personal Data Protection Bill, 2019:** This is a draft bill that has been introduced in the Indian Parliament and seeks to regulate the collection, use, storage, and processing of personal data in India. The bill proposes the establishment of a data protection authority, the classification of personal data into different categories, and the imposition of penalties for non-compliance with the law.

Salient features of the PDP bill.

a. **Obligations of data fiduciary:** The bill outlines that data fiduciaries, who decide the means and purpose of processing personal data, must comply with certain purpose, collection and storage limitations. They must process personal data only for specific, clear and lawful purposes and undertake transparency and accountability measures, such as implementing security safeguards and instituting grievance redressal mechanisms. They must also verify the age and obtain parental consent when processing sensitive personal data of children.

b. **Rights of the individual:** The bill grants certain rights to the individual or data principal. These include the right to obtain confirmation from the data fiduciary on whether their personal data has been processed, seek correction of inaccurate or incomplete personal data, have personal data transferred to any other data fiduciary in certain circumstances, and restrict continuing disclosure of their personal data by a fiduciary if it is no longer necessary or consent is withdrawn.

c. **Grounds for processing personal data:** The bill allows processing of data by fiduciaries only with consent from the individual. However, personal data can be processed without consent in certain circumstances, including if required by the State for providing benefits to the individual, legal proceedings, or to respond to a medical emergency.

d. **Social media intermediaries:** The bill defines social media intermediaries as those that enable online interaction between users and allow for sharing of information. All such intermediaries with users above a notified threshold, whose actions can impact electoral democracy or public order, have certain obligations, including providing a voluntary user verification mechanism for users in India.

e. **Data Protection Authority:** The bill sets up a Data Protection Authority to protect the interests of individuals, prevent misuse of personal data, and ensure compliance with the bill. It will consist of a Chairperson and six members with at least 10 years of expertise in the field of Data Protection and Information Technology. Orders of the Authority can be appealed to an Appellate Tribunal, and further appeals from the Tribunal will go to the Supreme Court.

f. **Transfer of data outside India:** Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the Government can only be processed in India.

g. **Exemptions:** The Central Government can exempt any of its agencies from the provisions of the Act in the interest of security of state, public order, sovereignty and integrity of India, and friendly relations with foreign states. Processing of personal data is also exempted from provisions of the bill for certain other purposes such as prevention, investigation, or prosecution of any offense, or personal, domestic, or journalistic purposes. However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.

h. **Offences under the Bill:** Offences under the bill include processing or transferring personal data in violation of the bill, failure to conduct a data audit, and identification and processing of identified personal data without consent, punishable with fines or imprisonment.

i. **Sharing of non-personal data with Government:** The Central Government may direct data fiduciaries to provide it with non-personal data and anonymised personal data for better targeting of services.

j. **Amendments to other laws:** The bill amends the Information Technology Act, 2000, to delete provisions related to compensation payable by companies for failure to protect personal data.

The regulatory landscape is constantly evolving, and new laws and regulations may be enacted in the future to address emerging issues and challenges in this area.
There are several problems and challenges that we are facing in the area of online privacy and personal data protection which are:

Gender-specific implications
The issue of online privacy and personal data protection has important implications for women, and there are several gender-specific aspects to consider. Some of the points which needs to be to consider:

- Women are more likely to be the target of online harassment and abuse, which can result in the exposure of personal data. Women often face a greater risk of being subjected to doxxing, cyber stalking, and other forms of online harassment, which can lead to the exposure of their personal information.
- Women's personal data is often used for targeted marketing and advertising. Companies
- may collect and use women's personal data to tailor marketing and advertising campaigns to them based on their gender and personal characteristics.
- Women's health and reproductive data is particularly sensitive and can be used to discriminate against them. Women may be hesitant to share information about their reproductive health and other sensitive health information due to the fear of discrimination or stigma.
- Women are often the primary caregivers and may share personal data about their children online. Women may share information about their children online, such as photos and personal information, which can also be at risk of being exposed.
- Women may face greater challenges in protecting their personal data due to social and economic factors. Women may have less access to resources and education on how to protect their personal data, particularly in marginalized communities.

Overall, the protection of online privacy and personal data is an important issue for women, and it is essential to consider gender-specific aspects when developing policies and regulations. It is important to ensure that women's privacy rights are protected in the digital space and that they have access to the necessary resources to protect their personal data.

Challenges & its remedies to online privacy
There are several problems and challenges that we are facing in the area of online privacy and personal data protection are:

a. **Data breaches:** Data breaches are a major threat to online privacy and personal data protection. When sensitive personal information is stolen or compromised in a data breach, it can lead to identity theft, financial fraud, and other types of harm.

b. **Lack of awareness and education:** Many people are not aware of the risks associated with sharing personal information online or the steps they can take to protect their privacy. There is a need for greater education and awareness-raising efforts to help individuals understand the importance of online privacy and personal data protection.

c. **Data monetization:** Companies often collect and use personal data for commercial purposes, such as targeted advertising. This can lead to concerns about the monetization of personal data and the lack of transparency around how data is being used and shared.

d. **Government surveillance:** Governments around the world have increased their surveillance capabilities in recent years, which can have implications for online privacy and personal data protection. There is a need to balance the legitimate needs of law enforcement and national security with the protection of individual privacy rights.

e. **Emerging technologies:** Emerging technologies such as artificial intelligence, biometrics, and the Internet of Things (IoT) can pose new challenges for online privacy and personal data protection. These technologies may collect large amounts of personal data and present new risks for data breaches and other types of harm.

These are just a few of the problems and challenges that we are facing in the area of online privacy and personal data protection. Addressing these challenges will require a multi-stakeholder approach that involves individuals, governments, and the private sector working together to develop effective policies and practices that protect privacy while promoting innovation and economic growth.

Challenges faced by digital era

In recent years, there has been a significant tussle between WhatsApp (owned by Facebook) and the Indian government over privacy issues, online privacy, and personal data protection. The Indian government, concerned about the potential misuse of social media platforms for illegal activities and the spread of fake news, proposed new regulations for intermediaries and social media platforms. These regulations were primarily aimed at strengthening online privacy and personal data protection.

WhatsApp, being one of the most widely used messaging apps in India, found itself at odds with the government's proposed regulations. The government's regulations required messaging platforms to trace the origin of flagged messages and provide decrypted information when required by the authorities. However, WhatsApp argued that complying with such requirements would undermine end-to-end encryption, which is a crucial aspect of user privacy and security on their platform.

WhatsApp claimed that breaking end-to-end encryption to trace messages would weaken the overall security of the platform, making it vulnerable to hackers and malicious actors. They also expressed concerns about the potential infringement on users' privacy if their messages were to be accessed by third parties, including the government.

As a result, WhatsApp refused to comply with the government's demands and engaged in discussions and negotiations to find a middle ground that would address the government's concerns while preserving user privacy. The standoff between WhatsApp and the Indian government led to public debates and discussions about the balance between privacy and law enforcement.

The clash between WhatsApp and the Indian government over privacy issues sparked widespread attention and raised questions about the right to online privacy, personal data protection, and the role of social media platforms in ensuring user security. The issue highlighted the ongoing global debate on how to strike a balance between security measures, law enforcement, and individual privacy rights in the digital age.

Remedies

a. **Stronger data protection laws and regulations:** Governments can enact and enforce stronger laws and regulations related to online privacy and personal data protection. These laws should require companies and organizations to obtain explicit consent from individuals before collecting and using their personal data, and impose penalties for non-compliance.

b. **Improved data security measures:** Companies and organizations can take steps to improve their data security measures to prevent data breaches and protect sensitive personal information. This can include implementing encryption, two-factor authentication, and other security measures.

c. **Education and awareness-raising efforts:** Individuals need to be educated about the risks associated with sharing personal information online and the steps they can take to protect their privacy. This can include developing educational campaigns, providing training, and raising awareness about the importance of privacy.

d. **Data minimization:** Companies and organizations can practice data minimization by collecting only the minimum amount of personal data necessary for their operations. This can help reduce the risk of data breaches and limit the potential harm caused by a breach.

e. **Ethical data use*:*** Companies and organizations can practice ethical data use by being transparent about how they collect, use, and share personal data, and ensuring that they use data in ways that are consistent with individuals' expectations and rights.

f. **Collaboration and stakeholder engagement:** Collaboration among stakeholders including government, industry, civil society and academia, can help ensure that policy and regulations are effective, balanced and future-proof. Engagement with individuals, civil society, and other stakeholders can also help to ensure that privacy concerns are adequately considered in innovation and policy-making.

Comparative analysis of Indian government and foreign government

Data Protection Laws

Indian Government: The Indian government introduced the Personal Data Protection Bill, which aims to provide a comprehensive framework for protecting personal data. It includes provisions related to data processing, consent, data localization, and individual rights.

Foreign Governments: Different countries have varying data protection laws. For example, the European Union's General Data Protection Regulation (GDPR) sets stringent standards for data protection and empowers individuals with rights over their personal data.

Government Surveillance Measures

a. **Indian Government:** The Indian government has implemented various surveillance measures, such as the

controversial Aadhaar system and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, which require platforms to trace the origin of flagged content.

b. Foreign Governments: Foreign governments have also implemented surveillance measures, such as the USA PATRIOT Act in the United States and the Investigatory Powers Act in the United Kingdom. These laws grant surveillance powers to government agencies for national security and law enforcement purposes.

c. Transparency and Accountability Frameworks
Indian Government: The Indian governmet has been working on establishing a framework for transparency and accountability in data processing. The Personal Data Protection Bill includes provisions for the establishment of a Data Protection Authority and mandates periodic audits by data fiduciaries.

Foreign Governments: Foreign governments have varying frameworks for transparency and accountability. Some countries require businesses to publish transparency reports, disclosing requests for user data by government agencies, while others focus on data breach notification and penalties for non-compliance.

d. Cross-Border Data Transfers: Indian Government: The Indian government has proposed provisions in the Personal Data Protection Bill that require critical personal data to be stored locally, to ensure data sovereignty and prevent unauthorized access.

Foreign Governments: Different approaches exist, such as the European Union's adequacy decisions that enable data transfers to countries with similar data protection standards, or the use of standard contractual clauses or binding corporate rules for cross-border transfers.

e. Role of Regulatory Authorities: Indian Government: The Personal Data Protection Bill proposes the establishment of a Data Protection Authority (DPA) responsible for overseeing the implementation and enforcement of data protection laws in India.

Foreign Governments: Regulatory authorities, such as the Information Commissioner's Office (ICO) in the UK and the Federal Trade Commission (FTC) in the US, play a vital role in enforcing data protection laws, investigating data breaches, and ensuring compliance.

It would delve into the complexities and challenges faced by both governments in effectively implementing and enforcing laws related to online privacy and personal data protection.

Right to privacy: a fundamental right brought into existence with judicial activism

Article 21 of the Constitution of India guarantees the fundamental right to life and personal liberty. This article has been interpreted by the Supreme Court of India to include the right to privacy, which is an integral part of personal liberty. The scope of Article 21 in respect of online privacy and personal data protection is significant as it provides the legal basis for protecting individuals' privacy rights in the digital age.

The Supreme Court of India has recognized the importance of privacy rights in the digital age and has held that the right to privacy is a fundamental right that is protected by the Constitution. In the landmark judgment of Justice *K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court held that the right to privacy is a fundamental right under Article 21 of the Constitution, and that privacy includes the right to control one's personal data.

The scope of Article 21 in relation to online privacy and personal data protection is therefore significant as it provides a constitutional basis for individuals to claim their privacy rights in the digital space. The Supreme Court has also recognized that the right to privacy is not an absolute right and can be limited by law in the interests of the sovereignty and integrity of India, national security, public order, morality, and health.

Therefore, the scope of Article 21 in respect of online privacy and personal data protection provides a legal framework for balancing individuals' privacy rights with the legitimate interests of the state and society. It is important for governments and companies to recognize the scope and importance of Article 21 in relation to online privacy and personal data protection and take necessary steps to ensure that individuals' privacy rights are protected in the digital age.

In the case of *Gobind v. State of M.P.*, the Supreme Court declared that the right to privacy
includes the protection of personal intimacies such as the home, family, marriage, motherhood, procreation, and child-rearing. However, this right is subject to "compelling state interest."

Similarly, in the case of *People's Union for Civil Liberties (PUCL) v. Union of India*, the Supreme Court extended the right to privacy to communications while considering the issue of telephone tapping. The court held that telephone tapping is a serious invasion of an individual's privacy.

In the case of *Selvi v. State of Karnataka*, the Supreme Court recognized the distinction between bodily/physical privacy and mental privacy. The court held that subjecting a person to techniques such as narco-analysis, polygraph examination, and the brain electrical activation profile (BEAP) test without their consent violates their mental privacy.

Further, in the case of *Unique Identification Authority of India v. Central Bureau of Investigation*, the CBI sought access to the database of the Unique Identification Authority of India for investigating a criminal offense. However, the Supreme Court, in an interim order, held that the Unique Identification Authority of India should not transfer any biometric information of any person who has been allotted an Aadhaar number to any other agency without the written consent of that person.

These cases demonstrate that the right to privacy is a fundamental right in India and that it encompasses various aspects of an individual's life. As such, it is essential that this right is protected and respected by all.

Conclusion

In conclusion, online privacy and personal data protection are important issues that need to be addressed in the digital age. With the increasing use of technology and the internet, the risks associated with sharing personal data online have become more significant. Protecting personal data is essential to ensure that individuals have control over their information, can make informed decisions about sharing their information and prevent any potential harm.

Governments, companies, and individuals all have a role to play in protecting online privacy and personal data. Governments can enact and enforce stronger laws and regulations, while companies can implement better data security measures and practice ethical data use. Individuals can also take steps to protect their own privacy by being aware of the risks and taking steps to safeguard their personal data.

It is also essential to recognize that addressing the problems related to online privacy and personal data protection will require a collaborative and multi-stakeholder approach. The involvement of all relevant stakeholders including individuals, governments, the private sector, civil society, and academia is necessary to develop effective policies and practices that protect privacy while promoting innovation and economic growth.

We live in a digital world where the internet has become an integral part of our daily lives. With the increasing use of online services, the issue of online privacy and personal data protection has become more important than ever before.

As legal professionals, it is our responsibility to ensure that the rights of individuals are protected and that their personal data is not misused or mishandled by organizations. This is especially important given the increasing number of data breaches and cyber-attacks that we have witnessed in recent years.

In conclusion, the issue of online privacy and personal data protection is one that is crucial in our digital age. As legal professionals, we must remain vigilant and continue to advocate for strong privacy protections and data security measures, both at the national and international levels. Ensuring online privacy and personal data protection is crucial in the digital age, and the adoption of measures to protect privacy rights should be at the forefront of policy-making and technology development.

References

1. Dwork C. “Differential Privacy: A Survey of Results,” in Theory and Applications of Models of Computation, ser. Lecture Notes in Computer Science, M. Agrawal, D. Du,
2. Duan Z, Li A. Eds. Springer Berlin Heidelberg, 2008, 1–19.
3. Kindt E. Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, ser. Law, Governance and Technology Series. Springer Netherlands, 2013.
   a. Narayanan, Shmatikov V. “Robust De-anonymization of Large Sparse Datasets,” in 2008 IEEE Symposium on Security and Privacy, 2008, 111–125.
4. Barbaro M, Jr TZ. “A Face Is Exposed for AOL Searcher No. 4417749,” The New York Times, 2006.
5. Dean J, Ghemawat S. “MapReduce: simplified data processing on large clusters,” Communications of the ACM,2008:51(1):107–113.