

REVIEW ON DATA PROTECTION LAWS IN INDIA- Parthvi Patel¹**Abstract**

The growth of recognizing oneself's privacy has also led to the need for protecting this privacy. Although the parameters of privacy and data protection are somewhat difficult to set, the importance to set them is dire, especially in this modern era where the line defining privacy is getting blurred each passing day. Privacy is a changing notion, and there should be requisite means of protecting it. It is this author's whim to make an encapsulated review on exiting data protection safeguards of India and has drawn a comparative study with the legislation of developed countries, ie., United States of America and United Kingdom, in particular.

1. Longest battle in history: Defining 'Privacy'

Somewhere between 343 to 335 BC, Aristotle in his book "politics" coined the term privacy, wherein he divided privacy into public nature associated with a person's political life, and private sphere like, family, and domestic life.

The gold standard for the language of law, otherwise known as Black's law dictionary defines privacy as the "*right to be left alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned*".²

But this definition is vague and doesn't fully cover the notion of privacy.

In India, about the same time as Aristotle, Chanakya³ elaborated the need for privacy by building homes at a sufficient distance from other homes, and to cover windows and lock doors. Coming back to the present time, "Privacy" as stated in our Preamble, is considered to be one of our fundamental rights, but India's Constitution does not define this term. Dimensions of Privacy are

¹ Student at United World School of Law

²"Privacy" Black's Law Dictionary.

³Arthashastra

ever changing, and so even if we define or make laws, they can only ever be partially inclusive of what we entail as privacy unless they evolve too, with the changing times.

Privacy is a basic need of every individual, which allows life to be leadwith dignity and honour. An individual's choice to consent the use of any information that has active or passive implication on them, all of it would fall under the purview of privacy. And as you can tell, this is why protecting these information from unauthorised access is so important. This is data protection comes in.

2. What is Data Protection?

Also known as data security, the term 'data protection' is comprised of the tools, mechanism, and policies that secures data from unauthorised access by a third entity. Like privacy, data protection also, hasn't been defined under any legislations but as per a general understanding, any legally enforceably notion to protect an individual or a groups's privacy would constitute as data protection. The reality of today's world is that almost every single activity of an individual involves a form of data transaction, from one device to another, which is why protecting this data is imminent, now more than ever, and this need will only go uphill from here.

3. Need for Data Protection

India holds the rank of enduring the second highest cases of data breach in the first half of 2022 itself⁴.

Recently, on 3 August 2022, Bob Diachenko⁵, tweeted:

"[BREACH ALERT] 280M+ records in this Indian database, publicly exposed. Where to report? @IndianCERT?"

The Ukrainian cybersecurity researcher claimed that about 288 million (!!!), and another IP with 8.4 million data records - publicly published personal records, including full names, gender, marital status, date of birth, bank account number, UAN⁶, Employment status bank account number and nominee information of the Employees' Pension Scheme holders, and the Employees' Provident Fund Organisation (EPFO), were exposed for an accounted length of time before he pointed it out. It is his finding that both IPs "were Azure-hosted and India-based"

⁴Surfshark VPN, Dutch Cybersecurity Firm

⁵Ukrainian cyber threat intelligence director and journalist, SecurityDiscovery.com

⁶ Universal Account Number

Any data, especially the ones in the digital sphere will only grow. There's no stopping of the digital growth, but there is a serious need to start regulating this data and its usage, especially from companies that fetch these personally identifiable data from its customers.

Along with the number of users, the industrial value of their data will also increase. Data protection ensures the security of this personal data and regulate the storage, use, transfer, and disclosure of the said data.

4. Existing Legislatures, Rules and Regulations

- Constitution of India, 1950
- Indian Penal Code, 1860
- Information Technology Act, 2000
- Copyright Act, 1957
- Indian Contract Act, 1872
- Consumer Protection Act, 2019
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Consumer Protection (E-Commerce) Rules, 2020
- Rules by the Telecom Regulatory Authority of India
- Rules made by the Reserve Bank of India
- Rules by the Insurance Regulatory and Development Authority of India
- Rules imposed by the Securities and Exchange Board of India
- Unified Licence Agreements pursuant to the National Telecom Policy, 2012, issued by the Department of Telecommunications
- Judicial precedents from Indian courts

5. Overview of these Data Protection Laws

5.1 Constitution of India, 1950

Currently, India lacks a reasonably sound legislation for data protection. Modern day understanding and governance of privacy and data protection can be derived from judicial proceedings, in particular, i.e., the decision laid by the Supreme Court on 24 August 2017, in *K. S. Puttaswamy vs*

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

Union Of India. In this case, Supreme Court unanimously changed the contours of Indian privacy law, and held right to privacy as an intrinsic element of Article 21 of the Constitution, under which all citizens have a negative right not to violate someone's right to privacy and a positive right to take necessary actions to protect this right, crafting a positive obligation on the Government to enact laws that protects its citizen's right to privacy.

Supreme Court relied on Article 21, and the word "Liberty" in Preamble to declare Right to Privacy as a fundamental right, which, under its umbrella, views Data infringement as a threat, and any unauthorised access of someone's data, without their explicit consent, directly amounting as infringement of Right to Privacy, for which a person can straightaway take the matter to the Hon'ble Supreme Court of India, under Article 32.

The issue arises, when there is no parameter surrounding "privacy" given in the constitution. And so, even though the need of protecting privacy is duly highlighted, the power to decide what falls under breach of privacy is left unto the judicial proceeding, and consequent judgment.

*R Rajagopal and Ors v. State of Tamil Nadu*⁷, recognised tortious liability for breach of privacy and the enabling the court to draw damages for invasions of privacy.

In USA, Right to Privacy is a judicially recognised right, under tort law as well. Victim can bring a lawsuit against the tortfeasor under "Invasion of Privacy" upon infringement of their right to privacy, or upon disclosure of their private information.

5.2 Indian Penal Code, 1860

- Theft⁸ -when an unauthorised person gains access or copy any private data of any individual, and is punishable with imprisonment up to 3 years or fine or both.
- Extortion⁹ - person induces fear into another person to deliver any vitally private documents or data to him, and is punishable with imprisonment upto to 3 years or fine or both.
- Forged document¹⁰ -using a forged document or e record which infringes the privacy of any individual, as real or genuine shall be punishable with imprisonment up to 2 years or fine or both.

⁷ Writ Petition (Civil) No. 422 of 1994

⁸Section 379, Indian Penal Code

⁹Section 383, Indian Penal Code

¹⁰Section 471, Indian Penal Code

It is pertinent to note that, is good that some parameters are drawn and its punishment isn't left unto the judicial decisions however, the punishment are outdated. The damage caused by the infringement can be much more severe and may have caused a lot of damage, yet the maximum punishment would only be for a very short period of time, and a fees thats near to negligible in this era.

5.3 Information and Technology Act, 2000

This Act, specifically deals with the Cyber Crimes and enables Cyber Security, with provisions aiming to curb crimes under the cyberspace, Data Protection and conserving Privacy,

- *Hacking*¹¹ - an unauthorised access to a computer resource or data without it's owner's consent, which causes injury to the image of that person or goodwill of a body corporate as defined under Section 43A, and is punishable with imprisonment upto 3 years or with fine
- Identity Theft¹² - fraudulent use of the e signature, password or any other unique identification feature of any other person.Punishable with imprisonment up to 3 years and fine up to rupees 1 lakh.
- Impersonation¹³ - ie cheats by personation, by means of any communication device or computer resource. Punishable with imprisonment up to 3 years and fine up to rupees 1 lakh.
- Punishment for violating of privacy¹⁴ - intentionally or knowingly captures, publishes or transmits the image of a private area of any person without their consent. Punishment imprisonment up to 3 years and fine up to rupees 1 lakh. Here, private data only includes "naked or undergarment clad genitals, public area, buttocks or female breast"

As you can see, all 3 of them - Identity Theft, Impersonation and Violation of privacy have the same punishment as if all of them were offences of similar nature except they aren't. They have widely different implications and consequences faced by victim to the crime. Even the 2009 amazement, did not fix this obvious loophole.

Section 67 is in regards topublishing or transmitting obscene material via any electronic form, and

¹¹Section 66, IT Act 2000

¹²Section 66C, IT Act 2000

¹³Section 66D, IT Act 2000

¹⁴Section 66E, IT Act 2000

Section 67A constitutes this offence containing sexually explicit via electronic form, punishable up to five years with fine up to ten lakh rupees. But this also, only regards privacy as privacy of “sexual material” there is no component of mental, emotional or economical privacy whatsoever.

Fourteenth Amendment of the US Constitution, has recognised family, marriage, procreation and motherhood, and child rearing under the general ambit of privacy.

5.4 Copyright Act, 1857

This Act mainly protects the literary, dramatic, musical and artistic works of the author, during their lifetime and sixty years after their death. The Act provides Civil and Criminal Remedies, if anyone copies, replicate or uses the creation of an author, without their explicit permission for commercial gain or publishing, circulating or transmitting, and so infringes the private rights of the author. The punishment however is imprisonment up to 3 years and a fine of 1 lakh.

Mr Hefner published Marilyn’s unsolicited pictures for his 1st issue. If he were Indian, he’d be in prison for only 3 years where he can sit and count the millions he made, and pay 1 lakh as fine.

5.5 Indian Contract Act, 1872

Is not an explicit safeguard, but allows to form agreements relating to the Privacy and Data Protection, and so allows a partial protection of Right to Privacy and Data, in India.

6. Bill in Draft

6.1 Baijayant Panda, in 2009 tabled- The Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill. The aim of this Act was to prohibit unsolicited telephone calls by business promoters or individuals to persons who hadn’t signed up for these calls, and didn’t wish to receive them. The goal of the act was to ensure every citizen isn’t deprived of its right to privacy, and hence the right to without unwarranted infringement. This bill also had an elaborated definition as to what constitute as privacy and its breach.

6.2 Data (Privacy and Protection) Bill, 2017- was Mr Panda’s another futile attempt, for reasons that aren’t his fault, to ensure right to privacy amongst this country. In December of 2019, the Ministry of Electronics and IT tabled in this bill Lok Sabha and on the same day, it was referred to a Joint Parliamentary Committee. This committee drew a report 2 years later, in December 2021.

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

<https://www.ijalr.in/>

The bill would affect big technology companies like Google and Meta, would increase their compliance burden, data storage requirements and restrict cross-border flow of data, hence limiting the ongoing unwarranted use of people's data.

7. Nothing goes without a hitch

Manish Tewari, rightfully pointed out an intricate limitation of this Bill, which was that if this Bill were applied, it would create *“two parallel universes — one for the private sector, where it would apply with full rigour, and one for the government, where it is riddled with exemptions.”* meaning, the breach of privacy if done by government, would be far easy to exempt, which also poses a threat.

Forth Amendment in the US Constitution, acts as an immunity for the people from unwarranted and arbitrary search and seizures by the State Authorities, for which people can hold the related government responsible in the court of law and also claim compensation for said breach.

PM Narendra Modi and his subsequent political party, took varied steps to protect data with tech companies. They decided to extend their powers of censorship over to social media, and started hiding certain post but is it to question how those post were going to breach a citizen's privacy, unless there was a link attached under it, that acted in favour of cyber terrorism¹⁵.

They also made WhatsApp set some private messages “traceable”to government if the government believed the content is a threat national security. Again, framework around “National Security” has always remained dazed and confused. It takes away the right, not directly though, to question the actions of the ruling government.

But as said by Apar Gupta, *“It's not about getting a perfect law, but a law at this point. Each day lost causes more injury and harm.”* Which is true to core. The longer we wait to bring a perfect bill, the list of victims would only grow and the criminals will go freely without facing any liability for their actions.

8. Drawing Inspiration from Laws of Developed Countries

In the UK, there were no existing laws protecting the Right to Privacy. But Human Rights Act enactment in 2000, that Right to Privacy essential in the UK, and includes several remedies for the

¹⁵ IT Act, 2000

breach of the such. This Act incorporated Article 8 of European Convention on Human Rights, which covered Right to privacy, along with bodily liberal and family rights.

With the help of General Data Protection Regulation, companies like Meta and Google would have to get specific permission for usage of a person's data, and has eased the process of erasing such personal data.

General Data Protection Regulation replaced the 1995 Data Protection Directive. GDPR's aim is to focuses on newer areas like Privacy rights, data security, data control, and governance. To simplify regulatory framework for businesses and give more power to the citizens to protect their personal data. It would also protect web related data like IP address and cookies. One important category that they bought in was the protection of political opinion, sexual orientation, health and genetic data, biometric data, and racial or ethnic data.

Failing to comply would result in a fine of up to EUR 20 million or 4 percent of the company's total global revenue for the preceding fiscal year, whichever is higher. A fair step in regulating its citizen's privacy and sustainable growth of a business.

9. Conclusion

India is yet in its developmental state, the need for privacy has surged but more importantly, the need to safeguard this privacy has grown too. We constitute 1/7 of world's total population, and obviously the data generated is huge and so should be the concern of protecting this data. We cannot sit and wait for a perfect Bill to come across, whenever it does and hope for the best until then. It could at least start by amending existing laws, and also not ending the discussion after pointing out the flaws in draft bills but actually rigorously working towards bettering them. Right to privacy, is rightfully, a fundamental right and it is about time said is taken as seriously - not just by the judiciary, but equivalent effort in making legislations too.