VOLUME 2 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CHANGING DATA PRIVACY LANDSCAPE IN INDIA

- Shreya Goswami & Atri Chattopadhyay[1]

ABSTRACT

This paper discusses the concept of privacy and lays special emphasis upon the issue of data privacy, highly relevant in the current era of rampant digitalisation. This paper also delves into the legislative landscape regarding privacy around the world with a focus on the Indian context and also analyses two notable incidents of privacy breach, along with the practice of surveillance. Throughout this paper, the primary focus has been given to the understanding and legal framework surrounding privacy in India and a case has been made out through this paper in support of the formulation and implementation of a robust data protection regime and machinery in India.

INTRODUCTION

Privacy for long been regarded as a basic human right and the Right to Privacy has been a contentious issue in jurisdictions around the globe. People have long demanded for the protection of their private self from scrutiny by governments and organizations and several legislations and regulations have also been enacted in this regard, apart from a growing recognition and understanding about the importance of privacy laws and the need for strengthening of safeguards to protect citizens against infringement of their personal data and information. Violations of privacy even by authorities is being increasingly denounced and a collective call for stringent, comprehensive and effective privacy laws has become a characteristic feature of the contemporary times.

Various nations around the world have enacted numerous legislations and legal frameworks to safeguard the data privacy of their citizens and to form a comprehensive mechanism to deal with privacy violations.

[1] 1st year students of Shyambazar Law College and WBNUJS respectively

In the United Kingdom., the Data Protection Act of 2018 incorporates the EU General Data Protection Regulation (GDPR) and supplements its provisions. It focuses on data subject rights, "special category" personal data, data protection fees, data protection offences, consents received from children and the enforcement of all these areas of preservations, giving the data protection mechanism in the UK a holistic structure.

In the United States of America, a sectorial approach to data privacy is followed which relies on a patchwork of sector-specific laws and state laws. The "California Consumer Privacy Act (CCPA) provides four distinct rights to the residents of California. They include the right to notice, right to access, right to opt-in or out and right to equal services. Apart from these governmental interventions on matters of data protection, reliance is also placed upon a "combination of legislation, regulation and self-regulation". This results in smooth working of the legal machinery and protects one from getting his/her right of privacy violated.

However, India has no specific legislation on privacy and data protection. Unlike the Fourth Amendment in the US Constitution, privacy as a concept is also not explicitly defined in the Indian Constitution. India's data privacy legislation is based on various other laws and acts in the absence of any specific legislation in this regard. Privacy lacks the position of a recognised concept in India and this makes it difficult for Indians to obtain proper legal recourse when a violation does take place.

Through the course of this paper, right to privacy as a field of law will be studied, with special emphasis over its status and the legal scenario concerning it in India, apart from a look at government surveillance through the lens of privacy laws and an analysis of the recent Pegasus fiasco. The field of study shall mainly concern the domain of India with occasional reference to other Western nations.

PRIVACY IN INDIA – A STUDY

Privacy has always been a translucent subject in the Indian legal framework, even more so amongst the general populace who are mostly ignorant about the laws in place as a result of which, privacy has seldom found its place amongst legislation and regulations up until the advent of the 21st century, when the government brought into force the *Information Technology Act* in 2000 which paved the way for serious discussions on privacy issues. Until

then, cases such as *Kharak Singh v State of Uttar Pradesh* had provided only narrow definitions of the right to privacy, even which did not address the issue of information privacy and left a scope for ambiguous interpretations.

Article 21 of the Constitution of India provides the right to life and post the landmark judgement in the case of *K.S. Puttaswamy v. Union of India* in 2017, the right to privacy was also recognised as a valid Fundamental Right and a part of the larger concept of the Right to Life under Article 21, for the right to life includes a right to live with dignity and personal freedom, including the freedom to be 'left alone'. Privacy was held as being worthy of the same level of protection as the rights enshrined under Part III of the Constitution of India, paving the way for better public consciousness about privacy.

Data protection laws are also a big void in the Indian context, which is quite ironic considering India's dominant position in the Information and Communication Technology and Business Process Outsourcing sector throughout the globe. Culturally, privacy has always been an elusive concept in the Indian society, with joint families being a characteristic part of households, the average Indian family consisting of 5 members, and Indian ranking consistently low on the Individualism Index (IDV) which measures the extent of a society's emphasis on individuality. Statistically, Indians are less concerned about identity theft, possess less knowledge of privacy laws, and are less aware of technology's impact upon privacy, leaving them highly vulnerable to exploitation.

The legislative framework regarding the protection of privacy in India is still not much developed and the latest advancement in this regard has been the enactment of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, apart from the existing Information Technology Act and although these kind of guidelines are positive steps towards enhancing data security in India, some crucial gaps still remain to be addressed adequately such as rules governing the collection, retention and disclosure of data. Proactive measures need to be taken to effectively strengthen the legal mechanism and steps such as the establishment of independent bodies such as a Privacy Commission can also go a long way in preventing the risks of privacy breaches and abuses due to the limitations of the existing legal regime.

SURVEILENCE - VITAL OR VIOLATIVE?

Surveillance means the close observation of a specific person or a group of people, especially of those who are under some suspicion.

With the growth of the Information Technology (IT) sector, several new age surveillance technologies have also been introduced such as internet surveillance, CCTV surveillance, telephone and e-mail surveillance. This growth gained widespread public attention in 2013, after the major leak of sensitive data from and the allegations of unethical surveillience against the National Securities Agency of USA by whistleblower Edward Snowden. In India, surveillance activities are carried out under the purview of two legislations: Section 5(2) of the Telegraph Act, 1885 and Section 69 of the Information Technology Act, 2000 which authorise the interception of both calls and electronic communication.[2]

Some of the legislations which facilitate surveillance in India are section 26 of the Indian Post Office Act, 1898, allows governments to intercept postal articles and Rule 138A of the Central Motor Vehicles Rules, 1989 mandates the installation of radio frequency identification ("RFID") tags on vehicles to facilitate their identification and monitoring. Some private organisations and commercial entities take the reason of 'quality purposes' to engage in mass scale collection of of digital data of their users, but this collection, sometimes even undertaken without adequate consent of the user or without providing the user with a real and free choice, bear the risk of leading to a rampant breach of data privacy breach. One of the striking examples of these kind of organisations is Microsoft, which watches all the messages and violates the privacy of every individual on Skype.[3] Additionally, even the update to the Terms of Service of popular messaging app WhatsApp in 2021 was met with heavy public outcry and a report on respected technology site, Ars Technica, revealed that WhatsApp is forcing people to accept its sharing of personal data such as their phone number and profile name with Facebook, something they could opt out of previously.

Several specialised organisations have also been set up for the exclusive function of carrying out surveillance activities, such as the National Intelligence Grid and the Central Monitoring System and exceptions in laws such as Rule 4 of the Information Technology (Procedure and

[2] Maria Xynou, CENTRE FOR INTERNET AND SOCIETY (CIS) BLOG, Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles.Available at https://cis-india.org/internet-governance/blog/policy-recommendationsfor-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-inindia-and-the-necessary-and-proportionate-principles.pdf

[3] Soumya Patnaik, QUICK HEAL BLOGS, Are Your messages on Skype are private? July 1, 2016.

Safeguard for interception, monitoring and decryption of information) Rules, 2009 allows governments to delegate the authority of intercepting, monitoring and decrypting digital information to any agency which it deems fit. It has been asserted that although surveillance can be essential and required under certain circumstances, it must be executed in a lawful manner without violating the principles and standards laid down by provisions and precedents. The act of surveillance is lawfully allowed when it follows the guidelines of Rule 419A of the Telegraph Act, as noted in *Public Union for Civil Liberties v Union of India* (1996).[4]

Although courts have even relied upon American cases such as *Griswold v Connecticut* and *Roe v Wade* for clearly determining the scope and ambit of right to privacy and the subsequent legality of government surveillance, some ambiguity and confusion still persists and due to a lack of concrete constitutional provisions, a lot of reliance has to be placed upon juridical precedents, which leaves a scope for variations in interpretation, leading to no definite legal position on the validity of surveillance and allied activities with respect to the right to privacy. Still, privacy as a component of law has become much defined now and judicial review of interceptions which were accused of being motivated by mala fide intentions have been carried out, sending out the assertion that although surveillance can be essential and required under certain circumstances, it must be executed in a lawful manner without violating the principles and standards laid down by provisions and precedents.

THE PEGASUS FIASCO

Pegasus is a spyware developed by an Israeli surveillance company NSO, which caused a massive commotion when it was revealed that it had been allegedly used to carry out unauthorised snooping and spying over notable personalities all around the globe including political dissidents, leaders, journalists and lawyers. Pegasus is designed to infiltrate devices

[4] Shashwat Singh, LEGAL SERVICES INDIA, Survellience in India Post the Right to Privacy Judgement. Available: https://www.legalserviceindia.com/legal/article-2273-surveillance-in-india-post-the-right-to-privacy-judgment.html

running on all major operating systems like Android, Blackberry, iOS and Symbian and turn them such devices into instruments of round the clock surveillance.

Pegasus can also be installed over a wireless transceiver located near a target, or, as stated in the NSO Brochure, simply manually installed if an agent can steal the target's phone. It exposes all the vulnerabilities of a person and leaves him with no option to protect himself.[5] The involvement of sophisticated technology like this, which employs a 'zero-link technology' mechanism raises serious concern over the ethics of government surveillance as the advanced mode of this spyware made it immune to scrutiny under the present laws. According to a report by Kaspersky, it is a modular malware that can initiate total surveillance on the targeted device, without the user not even guessing about its existence, making it even more dangerous and invasive on privacy.

In the Indian context, the delay in the implementation of the Personal Data Protection (PDP) Bill has left citizens susceptible to illegal privacy breaches and this also seeks to endanger the aim of Digital India as these kinds of threats would severely impair the growth and adoption of digitalisation of India. The PDP bill still awaits being passed by the Parliament and qualify as an Act, thus leaving the Indian citizens exposed to privacy breaches like this. Provisions of The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, notified under the Information Technology Act, 2000 can act as safeguards against spyware like this, apart from sections of the IT Act itself, such as Section 43A which creates liability for negligence in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, and section 72 of the Act, which provides for penalty for breach of confidentiality and privacy.[6]

The IS 17428 standard issued by the Bureau of Indian Standards is also an important mechanism for privacy assurance of individuals, its Sub-clause 3.2 highlighting the importance of consent as "Data subject's freely given, specific and informed agreement to the processing of their personal information." Although not explicitly under the domain of Criminal Law, section 403 of the Indian Penal Code, which mentions the offense of dishonest

[5] David Pegg and Sam Cutler, THE GUARDIAN, Explained: The Pegasus Project, July 18,2021. Available on: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

[6] Ajay Chawla, SSRN, Pegasus Spyware – 'A Privacy Killer', August 9, 2021. Available: https://dx.doi.org/10.2139/ssrn.3890657

misappropriation or conversion of "movable property" for one's own use, is sometimes applied in cases like this of data security breach.[7]

Modern spyware methods such as Pegasus enhance the call for plugging in the gaps in the current privacy laws and present a strong case for expediting the process of the implementation of a robust data protection regime, and the augmentation of existing measures such as Computer Emergency Response Teams (CERT) and initiatives like the Cyber Swachhta Kendra to bring into action the recognition of the Right to Privacy as a Fundamental Right.

LEGAL STATUS OF PRIVACY IN INDIA

While consciousness over privacy is still limited in India, the high growth in the business process outsourcing sector and the increasing amounts of personal information being accumulated from other countries has lead to "India becoming one of the more challenging contexts for privacy protection", according to a recent report by the London-based Privacy International. India has a "large presence in the outsourcing economy," but arguably the people of India are not equally concerned about privacy issues, making them highly vulnerable to become the victims.[8]

India presently does not have any express legislation governing data protection or privacy, in the absence of which, the most relevant law in India dealing with data protection is the Information Technology Act, 2000. A codified law on the subject of data protection is likely to be introduced in India in the near future. However till then, the personal details of millions of people stand at a great risk of being compromised with.

The public disclosure of certain kinds of information can also be mandated by law, and in such cases, privacy protection cannot be claimed. Examples are the disclosure of medical conditions and the obligation to reveal information about diseases and disease symptoms, as was prevalent during the initial stages of the COVID pandemic when people were mandated to disclose their medical history, conditions, travel history etc. to authorities whenever asked

[7] THE PIONEER, Pegasus affair is an assault on privacy, July 26, 2021. Available: https://www.dailypioneer.com/2021/columnists/pegasus-affair-is-an-assault-onprivacy.html

[8] PRIVACY INTERNATIONAL, Explained: Privacy Law In Asia: Final Report Of Scoping Project 21, November 2009, Available: http://www.privacyinternational.org/issues/asia/privacy_in_asia_phase_1_report.pdf

for. These are all instances of privacy breaches in the common understanding, but all these cases might escape prosecution due to these being instances of protected privacy infringements which are often allowed and even encouraged by governments. These kind of limitations prove to be a hindrance in the enactment of an efficient and strict data privacy mechanism and while the kind of strict data protection laws in place in the European Union have their disadvantages too, such as playing a role in the crash of Germanwings Flight 9525 which was deliberately caused by a suicidal co-pilot whose condition was unknown to his employers due to german laws preventing employers from accessing their employees' medical records, to ensure the safeguarding of privacy from unauthorised and mala fide surveillance, certain amendments to the existing laws on surveillance are usually proposed, to bring them in line with the National Privacy Principles and the International Principles on the Application of Human Rights to Communications Surveillance. Amongst the proposed changes is the non adoption of rule 419B of the Indian Telegraph Act 1885 which provides for disclosure of call data records to law enforcement agencies bears potential for abuse. Changes to certain licence agreements are also suggested, such as modification of clause 2.2 of the ISP License Agreement, which provide data encryption facilities above 40 bits to users only upon disclosure of private encryption keys and the obtaining of explicit written permission from service providers.

There are also provisions for setting up of review committees and scrutiny of interception orders to ensure the genuineness of directions and orders of surveillance in case the orders violate the surveillance guidelines as laid down in *People's Union for Civil Liberties (PUCL) v Union of India*, then the collected information can be ordered to be destroyed.

These recommendations, if properly implemented, would pave the way for India's data protection mechanism to become at par with other developed countries and would lead to the prevention of the flourishing of technological advancements at the cost of private data and information of individuals that they hold dear and deem secure.

CONCLUSION

While privacy as a concept has remained a bit elusive, especially in India, it has been continuously deliberated upon and has developed and progressed with the passage of time and successive judicial decisions. With all the advancements in this field, some pertinent

issues still remain unattended, which leave the citizens vulnerable to privacy breaches. Surveillance by governments is one such way of infringement of privacy which if not done in the proper and ethical way, can seriously compromise the legitimacy of a government and the trust and faith of the people upon the political machinery. Governments should be accountable for their scrutinising activities and must justify its measures against the laid down criteria, to maintain transparency. Exceptions in existing regulations and statutes which provide a blanket shield to governments and its functionaries against liability in case of data infringements must be reviewed and rationalised to prevent arbitrary actions. The draft Personal Data Protection Bill pending with the Parliament should be adopted in its final version at the earliest to bring about a comprehensive protection regime, which can address the current shortcomings. With modernisation and rapid technological progress, advanced modes of surveillance are vast becoming available, which although efficient, must be utilised in a regulated manner and should not violate clearly laid down guidelines by exploiting grey areas in existing regulations. To foster the growth of digitalisation and mass adoption of technology in developing nations, public confidence must be built, which can only be achieved through an efficient and effective data protection regime. The right to privacy is a fundamental basic human right and should be preserved and respected by governments under all circumstances, in order to ensure good governance and prevent misuse of authority, for as rightly said by American actor and political activist Marlon Brando Jr.,

"*Privacy is not something that I'm merely entitled to, it's an absolute prerequisite.*"

BIBLIOGRAPHY

1. Maria Xynou, CENTRE FOR INTERNET AND SOCIETY (CIS) BLOG, Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles.Available at https://cis-india.org/internet-governance/blog/policy-recommendationsfor-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-inindia-and-the-necessary-and-proportionate-principles.pdf

2. Soumya Patnaik, QUICK HEAL BLOGS, Are Your messages on Skype are private? July 1, 2016.

3. Shashwat Singh, LEGAL SERVICES INDIA, Surveillience in India Post the Right to Privacy Judgement. Available: https://www.legalserviceindia.com/legal/article-2273-surveillance-in-india-post-the-right-to-privacy-judgment.html

4. David Pegg and Sam Cutler, THE GUARDIAN, Explained: The Pegasus Project, July 18,2021. Available on: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

5. [1] Ajay Chawla, SSRN, Pegasus Spyware – 'A Privacy Killer', August 9, 2021. Available: https://dx.doi.org/10.2139/ssrn.3890657

6. [1] THE PIONEER, Pegasus affair is an assault on privacy, July 26, 2021. Available: https://www.dailypioneer.com/2021/columnists/pegasus-affair-is-an-assault-onprivacy.html

7. PRIVACY INTERNATIONAL, Explained: Privacy Law In Asia: Final Report Of Scoping Project 21, November 2009, Available: http://www.privacyinternational.org/issues/asia/privacy_in_asia_phase_1_report.pdf