DE JURE NEXUS LAW JOURNAL

Author:

Aashna Arora

Lloyd Law College, Noida

3rd Year, BA LL.B.

ERA OF DIGITALISATION AND HUMAN PRIVACY RIGHTS PRESERVATION

"Privacy is dead and social media holds the smoking gun."

– Pete Cashmore

Abstract:

Some call its freedom; some call it privacy. All the countries around the globe are going through phase of profound societal change, almost a technological shift which has brought on rapid expansion of digital communication infrastructure and exponential adoption of the digital technology. The digital revolution began around 1980 with the concept of internet and after with mobile devices, social networking sites, computing clouds and so on with an unlimited list on inventions. Technology has always presented itself with the two dimensions of being either a boon or a bane in every human's life.

This research is all about studying in detail how the increased branches of technology has violated the privacy rights of individuals in the Indian contexts.

Keywords:

Technology, Human Rights, Privacy, Constitution of India

Introduction:

We live in an era when we no longer need to stand in long queues to get the bus or train tickets, or the banking services and putting up an online order is as simple as blinking an eye. All the doorstep facilities are just a click away. No human being is born with physical privacy. All humans are blessed with an excellent sense of wellbeing which has with the blast of technology benefits also posed a question on preservation of human privacy. The question of privacy being a fundamental right has always been a hot debated discussion rolling upon the judicial bars. In 2019 there were 5.112 bn mobile users, 4.388 bn internet users and 3.484 bn active social media users. All of these groups have grown by between 2 and 9% since 2018 and are expected to continue to grow throughout 2020[1]. The globalization along with the digital and information communication technology has signified a whole new era for human rights, featured by new tensions, challenges, and posing risks for human privacy rights. With the advanced digital technology privacy has become need of the hour.

Defining 'Privacy':

"Privacy on internet? That's an oxymoron"

[1] https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

- *Catherine Butler*

Privacy has been categorised under one of the human rights. Human rights are the rights which we have simply just because we exist as humans. The pace of technology evolvement is ever increasing eagerly embracing the people. The term "Privacy" is notoriously a very wide term to define and cannot be understood as one-dimensional concept. It has constantly been dynamic with the advancements and progress of technology in every corner of world. Privacy has been acknowledged as the wildest increasing crime; it is projected that in every 79 seconds an identity is stolen.[2] It has been considered from different disciplines of study like sociology, psychology, law and philosophy. Being a multidisciplinary domain, privacy looks easy concept to understand but a difficult concept to define. Just clicking one option of ordering an item online and next day or within hours the phone's notifications, Instagram, Facebook is all flooded with the same deal displaying continuously. Is it what we call real privacy?

International instruments on right to privacy:

Right to privacy is an important concept under the human rights principles. It has always been a part of human life since the inception of human history. It is the most cherished right of any civilised society. International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy. The right to privacy is enshrined by the:

Universal declaration of human rights:

Article 12 of UDHR states, "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[3]

International Covenant on Civil and Political Rights:

Article 17 of International Covenant on Civil and Political Rights (to which India is a party) states, *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honor and reputation".*

Convention on the Rights of the Child:

Article 16 of Convention on the Rights of the Child states, *"Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health."*[4]

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families:

Article 14 of International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families states, **"***No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."*[5]

Right to Privacy – Indian Status Quo:

In the context of rapidly growing and omniscient digital growth the concept of privacy has almost been an evaporating concept. Privacy, in its simplest sense, allows each human being to be left alone in a core that is inviolable. Though, the overarching presence of state and non-state entities regulates the aspects of social

[2] https://www.bartleby.com/essay/Technology-and-the-Invasion-of-Privacy-FKJ6QWAZTC
[3] https://privacy.sflc.in/universal/
[4] https://www.ohchr.org/en/professionalinterest/pages/crc.aspx
[5] https://www.ohchr.org/Documents/ProfessionalInterest/cmw.pdf

existence which bear upon the freedom of the individual which is why the judgement of *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors*[6] comes in as a breath to fresh air. Privacy values have been categorised as one of the fundamental pillars of our democratic society. Article 21 of the Indian Constitution states that "*No person shall be deprived of his life or personal liberty except according to procedure established by law".* The day of 24th August,2017 is considered to be a red-letter day in the history of Indian Legal Jurisprudence. It was for the first time in independent India the nine-judge bench delivered an overarching landmark judgement on right to privacy concluding that has fundamental right to privacy enshrined under right to life, as fundamental right under Article 21 of the Indian Constitution which is an intrinsic element of Part III of the Constitution and considered to be the heart and soul of the Indian Constitution. Although, there have been no provisions made in the Indian Constitution but the net effect of Judgement pronounced on 24th August,2017 lead to a net effect conclusion of anyone being the citizen of India has Right to privacy. Prior, to this judgement there were three stages of development of Right to Privacy Act.

STAGE 1: BEFORE 1975 - RIGHT TO PRIVACY NOT EXPRESSELY RECOGNISED

The attorney general of India urged the existence of fundamental right of privacy is in doubt to view to the two decisions - *M P Sharma v/s Satish Chandra*[7], the 8-judge bench of the Supreme Court held that drafters of the Constitution did not intend to include the subject of power of seizure to be a fundamental right of privacy. They proposed that Constitution does not include language similar to the Fourth Amendment of the US Constitution.

And in the second case of *Kharak Singh v/s State of Uttar Pradesh*[8], Kharak Singh was arrested for dacoity but was released due to a lack of evidence. The right to privacy was invoked by the accused to challenge the surveillance by the police during mid-night under Chapter XX of the Uttar Pradesh Police Regulations. Kharak Singh then challenged the constitutional validity of Chapter XX as it violated his fundamental rights under **Article 19(1)(d) (right to freedom of movement)** and **Article 21 (protection of life and personal liberty).** The 6-judge bench hence held that domiciliary visits at night was unconstitutional, but upheld the rest of the regulations on the justification that right of privacy is not a guaranteed right under the Indian Constitution.

STAGE 2: DURING 1975-2000 - RIGHT TO PRIVACY IMPLICIT IN ARTICLE 21 OF INDIAN CONSTITUTION

In the case of *Govind v/s State of Madhya Pradesh*[9] Govind challenged the validity of the Madhya Pradesh Police Regulations related to surveillance, including domiciliary visits. He alleged false accusations put against him on the basis of which he was put under surveillance by the police. The Supreme Court dismissed the petition but advised reforms to be made in in the Madhya Pradesh Police regulations and observed that they were 'verging perilously near unconstitutionality'. Justice Mathew, accepted the right to privacy to be a product of Article 19(1) (a), (d) and Article 21, but simultaneously also held privacy not to be an absolute right. Also, in the other case of Smt. Maneka Gandhi v/s Union of India & Anr., the supreme court held that the term 'personal liberty' under Article 21 shelters many terms like

STAGE 3: 2000 TO PRESENT - RECGONITION AND SAFEGUARDSALONG WITH REASONABLE RESTRICTIONS TO THE RIGHT TO PRIVACY

In **Directorate of Revenue v. Mohd Nisar Holla**[10], the court held that an individual who does not break any law is entitled to enjoy his life and liberty which includes the right of not to be disturbed. Right to be let alone is recognized to be a right under article 21.

The **Aadhar case**, popularly known as Aadhar case laid the foundation of Right to Privacy in the Indian Society. This landmark case has widened the scope of fundamental rights of individuals.

Judicial Approach – Aadhar Case:

[6] Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161
7 1954 AIR 300, 1954 SCR 1077
[8] 1963 AIR 1295, 1964 SCR (1) 332
[9] 1975 AIR 1378, 1975 SCR (3) 946
[10] (2008) 2 SCC 370

BACKGROUND

In January,2009, Aadhar scheme was launched by the Government with the aim to create world's largest unique system in which every citizen was provided unique 12-digit code with biometric data and demographic data identifications. Statutory authority named Unique Identification Authority of India (UIDAI) was responsible for handling of the data. Although, the objective with which the scheme was created was to help the government distributing subsidies and implementation of schemes but adversely the issue of privacy was raised up stating the violence of right to privacy by collecting the sensitive information. The case has been brought into the limelight by retired High Court Judge K S Puttaswamy against the Union of India.

PARTIES TO THE CASE:

- Petitioner: Justice K. S. Puttaswamy (Retired)
- Respondent: Union of India; Planning Commission, Government of India; Unique Identification Authority of India; The State of Andhra Pradesh; The State of Assam; The State of Arunachal Pradesh; The State of Bihar; The State of Chhattisgarh; The State of Gujarat; The State of Goa; The State of Haryana; The State of Himachal; The State of Jharkhand; The State of Jammu and Kashmir The State of Karnataka; The State of Kerala; The State of Madhya Pradesh; The State of Maharashtra; The State of Manipur; The State of Meghalaya; The State of Mizoram; The State of Nagaland; The State of Orissa; The State of Punjab; The State of Rajasthan; The State of Sikkim; The State of Tamil Nadu; The State of Tripura; The State of Uttarakhand; The State of Uttar Pradesh; The State of West Bengal; The Union Territory of Daman and Diu; The Union Territory of Dadra and Nagar Haveli; State of National Capital Territory of Delhi; The Union Territory of Andaman Nicobar Islands; The Union Territory of Lakshadweep; The Union Territory of Chandigarh; The Union Territory of Puducherry.

ISSUES RAISED

Whether the right to privacy is a fundamental right under Part III of the Indian constitution,1950.

HELD

On 26th September,2018 the court pronounced its verdict that had finally put an end to Aadhar Dilemma. The court had multiple views on privacy:

Justice Chandrachud, writing a multiplicity opinion stated privacy is not an alien to other fundamental rights under Part III of the constitution. It can be classified as an unchangeable natural right which is mandatory to maintain human dignity. Also, he urged that due to fast developments in the country sooner or later there'll be a need for a data protection law.

According to **Justice Chelameswar**, "Right to privacy comprises of three facets, namely repose (freedom from unwarranted Stimuli), sanctuary (protection from intrusive Observation) and intimate decision (autonomy to make personal life decisions)"

Justice Nariman stated that right to privacy is divided into three categories namely, i) that which involves trespass to person by state's invasion ii) Unauthorized uses of information and iii) individual autonomy over fundamental personal choices.

Justice Bobde is of the opinion that fundamental rights have two facets- firstly, to limit the legislative powers and secondly to provide rights in order to flourish the conditions for dignity of individuals.

On the other hand, **Justice Sapre** majorly focuses his opinion restricted to importance of preamble of the Constitution. He asserted how an individual can connect his right to privacy with the principles of liberty. Dignity and fraternity.

Permissible restrictions on Right to Privacy

Privacy intrusion might be made on the following instances:

(1) Law-making Provision

(2) Managerial/Decision-making request

(3) Court Orders.

(4) Administrative or authority movement concerned and it must consist of admiring the assurances and status of the case.

Concerns and Difficulties

Who has authority to collect personal data?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[11] India's regulatory mechanism revolves around the data protection and privacy in the Information Technology Act, 2000 ("the IT Act") and its corresponding Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("the IT Rules").

Section 43A of the IT Act imposes liability on corporates that retains, deals or handles any sensitive personal data or information in computer resource they own, control or operates to pay damages caused by the way of compensation, to the person affected if there is any wrongful loss or wrongful gain because of the negligence in implementing and maintaining reasonable security practices and procedures to protect the information of the person affected.

Nature of data protected by the Indian legislature

Since the Indian culture is still climbing the stair of data protection mechanism, the primary act dealing with data protection is the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011. Under the IT Act and Rules, what is primarily prioritised to be protected is personal data and sensitive information, i.e., password-related information, financial information such as bank account or credit card or debit card or other payment tool details, physical, physiological and mental health condition, sexual orientation, medical records and history.

Almost all the us, use fitness apps/ gadgets like Fit bits and the many Mi Bands or must have searched health information online, or signed up for a free diagnostic check-up or may have claimed health insurance. Each time when we do any of these, we do have to share our sensitive data related to our health with various entities and the sites. The IT Rules only protect a limited set of information but major part of health data is left uncovered. Also, Multiple apps such as like Facebook, Google, Life360 - Family Locator, mSpy, FamiSafe, Spyzie, Instagram can track our locations on the go. In the absence of any specific provision preventing the dissemination of location information, these apps can easily trade our location information with third parties which can be severe threat to privacy of any individual.

Extend to which personal data can be shared with third parties

Any corporate body that retains, deals or handles any sensitive personal data or information in computer resource they own, control or operates, receiving the information may be allowed to disclose sensitive personal data or information to any third party with prior authorization received from the provider of such information, or there should be an agreement for such disclosure between the recipient and the information provider, or where disclosure is necessary to comply with a legal obligation.

However, no such approval is required from the information supplier is required if in case the information is shared with government organizations mandated by legislation to acquire information including sensitive private

[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

data or information for identity verification purposes, or to prevent, detect, investigate, including cyber occurrences, prosecute, and punish offenses.

Conclusion

Privacy is a new born right in today's era and probably an item of current western law. Ever since the Internet sector has bloomed, everything is connected to the Internet that depicts a clear need for privacy laws because everything is connected with the Internet and especially on sites like Facebook, Twitter, Instagram, LinkedIn, and many other sites like Paytm, PayPal, MobiKwick, our credit card or debit card or net banking information is saved, this can a threat because anything can be hacked on sites like these. All these developments demand a desperate requirement for Right to Privacy in this digital age. Need of hour is 'A right to Privacy Act' defining each and every corner of privacy in a detailed manner so that there are no loopholes left for breach of privacy of any individual.