HAS THE DIGITAL WORLD COME OF AGE, WITHOUT A LEGAL FRAMEWORK?

By *Gayatri Dabir & Aishwarya Ganesan*
From *Symbiosis Law School & VIT Law School, respectively*

THE INFORMATION AGE:

With nearly 450 million Internet users and a growth rate of 7-8%, India is well on the path to becoming a digital economy, which has a large market for global players.[1] The internet has removed geographical boundaries to a number of activities and hence has made electronic transactions a necessary part of our everyday lives. It has given birth to entirely new markets: those dealing in the collection, organisation, and processing of personal information and other related data, whether directly or indirectly. With electronic transactions on the rise, there is also an increase in data processing activities in both, public and private sector and cybercrime activities like data-theft, hacking, identity theft to name a few. Data protection has therefore become an issue which needs urgent attention. India is still at a nascent stage when it comes to data protection regulations, as compared to other jurisdictions like the European Union. The European Union gave effect to the provisions of the General Data Protection Regulation (hereinafter referred to as "**EU GDPR**") from May 25, 2018.

As of 2018, In India, data protection and all the matters relating to the storage, collection, disclosure and transfer of such data in the electronic form is covered under Information Technology Act, 2000 (hereinafter referred to as "**IT Act**") and the rules framed under the same. With respect to personal data, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter referred to as "**SPDI Rules**"), lay down procedures and measures to be undertaken by all those entities which deal with sensitive personal information. But with the efforts being put to digitise the economy, increase in the activities over the internet and right to privacy being recognised as a constitutional right [2], the existing data protection framework seems to be insufficient to address all the issues surrounding data protection.

Therefore in order to further strengthen the regulations surrounding data protection and privacy, a Committee of Experts under the chairmanship of Justice, Shri B. N. Srikrishna was formed to daft a Data Protection Bill. The Committee accordingly on November 27, 2017 released White Paper of The Committee of Experts on a Data Protection Framework for India (hereinafter referred to as "**White Paper**"). The draft after a number of delays is now set to be submitted to the Government. The draft will later be introduced in the Parliament, subject to the Government's agreement on the same.

This article firstly tries to put forward a judicial approach of the Indian courts

[1] Arushi Chopra, Number of Internet users in India could cross 450 million by June: report', LiveMint (2 March 2017), http://www.livemint.com/Industry/QWzIOYEsfQJknXhC3HiuVI/Number-of-Internet-usersin-India-could-cross-450-million-by.html

[2] *See* Justice K.S. Puttaswamy (Retd.) vs. Union of India & Ors. 2017 (10) SCALE 1.

towards privacy. Secondly, it covers comparative approach between the EU GDPR, the IT Act and Rules and the White Paper and then concerns that may arise with these rough and non- demarcated lines of privacy.

JUDICIAL RESPONSES TO PRIVACY CONCERNS IN INDIA

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

- Marlon Brando[3]

Debates about this extremely complex subject took their pilot opening with the phrase 'the right to be left alone' coined by Cooley [4] and adopted by Warren and Brandeis in a shaping and decisive Harvard Law Review [5] article which has been held as providing the basis for the origin and development of the law in this area.

Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner."[6] The fundamental rights, enshrined in Part III of the Constitution, are inherent and cannot be extinguished by any constitutional or statutory provision. Any law that therefore abrogates or abridges such rights would be violative of the basic structure doctrine. The actual effect and impact of the law on the rights guaranteed under Part III has to be taken into account in determining whether or not it destroys the basic structure. [7] The Hon'ble Supreme Court has added to the already wide ambit of Art.21, and to imply certain rights there from, has looked to perceive and interpret Art.21 along with international charters on human rights. In PUCL v UOI,[8] the court has derived and deduced the right to privacy from Art.21 by construing it in conformity with Art.12[9]of UDHR, 1948[10]and Art.17[11]of ICCPR, 1966. [12] This kind of judicial approach has been observed in a number of cases.[13]

International instruments have therefore assisted jurisprudence and offer important interpretative tools to Art.21 and the right to privacy. *Informational privacy is a facet of*

[3] American Motion picture and stage actor, 1924-2004.

[4] Cooley, Torts, 2ndEdn. , 1888.

[5] Samuel D. Warren and Louis D. Brandeis, "The Right To Privacy", Harvard Law Review, Vol. 4, December, 1890. p. 193-220. Para. 193.

[6] *See* Ram Jethmalani and Ors. vs. Union of India (UOI) and Ors.,2011(4)ALLMR(SC)815.

[7] *See* Dharam Pal vs. State of Haryana and Ors.,MANU/SC/0118/2016.

[8] *See* PUCL v UOI AIR 1997 SC 568

[9] Art.12 of UDHR, 1948- "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."

[10] Universal Declaration of Human Rights, on 10 December 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights.

[11] Art.17 of ICCPR, 1966

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks

[12] International Covenant on Civil and Political Rights, 1966, entered into force on 23rdMarch 1976.

[13] Visakha v. State of Rajasthan, AIR 1997 SC 3011, D.K Basu v. State of W. B., AIR 1997 SC 601, Chairman Railway Board v. Chandrima Das, AIR 2000 SC 988

the right to privacy[14], rightly said by the Hon'ble Supreme Court in *Justice K.S. Puttaswamy*, laying the foundation to a future with a digitally secure India.

COMPARATIVE APPROACH

A brief comparison of the two existing legislations and one proposed regulatory framework for data protection could be summarised as under:

- **Application:**
  Several jurisdictions have deliberated on the applicability of the data protection law differently. The EU GDPR only applies to 'natural persons' whereas the IT Act covers natural as well as body corporate under its ambit. The White Paper seeks to cover only natural persons under the framework.
- **Processing:**
  Data protection laws across the globe have tried to keep the definition of 'processing' as broad as possible to ensure that there is always room to incorporate new operations in the existing definition with changing times. Under the EU GDPR any operation performed on personal data, manually or electronically constitutes processing. The White Paper identifies three main operations of processing, namely, collection, use and disclosure of data but this is not exhaustive. Processing would include electronic as well as manual processing.
- **Consent:**
  Informational privacy can be broadly understood as the individual's ability to exercise control over the manner in which her information may be collected and used[15] hence consent becomes an integral part of the same.[16]

  Article 6 of the EU GDPR talks about the requirement of consent. For such consent to be valid, the consent must be freely given, specific, informed and unambiguous for processing of personal data. When the data is sensitive, the Regulation requires an explicit consent. Similar to the aforementioned, Rule 5 of the SPDI Rules mandates the requirement of consent in written form for sensitive information. Keeping the importance of consent in mind, the White Paper also makes the requirement of consent a mandatory one; for collection and use of personal data.

  The EU GDPR and White Paper also cover child's consent. Any child who is below the age of 16 and 18 respectively, would require parent's consent for data processing.

- **Purpose Specification Principle:**
  Purpose Specification is an essential first step in applying data protection laws and designing safeguards for the collection, use and disclosure of personal data.[17]
  Article 29 of the EU GDPR mandates the data controller to collect data for specified, explicit and legitimate purposes, and once the data is collected, it must not be processed further in a manner that is

[14] *See* Justice K.S. Puttaswamy (Retd.) vs. Union of India & Ors. 2017 (10) SCALE 1.

[15] Adam Moore, Toward Informational Privacy Rights', 44 San Diego Law Review 809 (2007)

[16] Jerry Kang, Information Privacy in Cyberspace Transactions', 50 Stanford Law Review 1193, 1202-03 (April 1998).

[17] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation', European Commission (2 April 2013), http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files

incompatible with the original purpose. Rule 5 of the SPDI Rules, 2011 also states that data can only be collected for a lawful and specific propose. The White Paper suggests some standards and guidelines to be enacted to govern the data controller's actions and that individuals should be able to retain the control of data provided by them.

- **Cross Border Data Flow:**
With disappearing geographical borders due to technological advancements and increase in cross border transactions on the Internet, it becomes important for data protection laws to cover such transactions.
All three frameworks mandate for an adequacy test (the IT Act doesn't specifically use the term) i.e. the access to personal data to not be permitted in other countries unless the countries are deemed to have an adequate level of data protection. Furthermore, the White Paper suggests for an additional comparable level of protection test. It also suggests for an establishment of Authority that will actively monitor developments of this law around the world.

- **Individual Participation:**
Processing of personal data must be transparent to, and capable of being influenced by, the data subject and hence to ensure the adherence to the same, it becomes important for individual participation.[18]
The EU GDPR grants an individual the right to access his personal data including the right to confirm the processing of such data. He can also seek rectification of his data, subject to certain conditions. Furthermore, he has the right to object processing of his data on certain grounds and the right to request data controllers to erase any data from the system. The IT Act lacks any such provision. The White Paper, just like the EU GDPR seeks to provide an individual with the right to confirm access and rectify his personal data once it has been collected by a party. The Paper also recognises the right of an individual to controllers to erase any data from the system, better known as the right to be forgotten.[19]

- **Penalties:**
Civil Penalties act as a sanction as well as act as deterrence for those who violate the obligations under data protection law.
Under the EU GDPR, an administrative fine can be imposed up to EUR 20,000,000 or up to four percent of the total turnover of the preceding financial year, whichever is higher. The IT Act under Section 43 A provides for compensation on failure of data protection by body corporate involving a fine not exceeding five crore rupees. The Act also provides for a residuary penalty under Section 45. As per the White Paper, there has to be a Data Protection Authority established that shall have the power to impose civil penalties on the defaulting parties.

WHERE DOES OUR CONCERN BEGIN?

In light of the judicial pronouncements that have been laid down, it is clear that it is the right of every citizen to obtain information from a public authority.[20] Information has been further defined to constitute, *"any material in any form, including records,*

[18] Lee Andrew Bygrave, Data Privacy Law: An International Perspective' 2, 2014

[19] Sri Vasunathan vs. The Registrar General, 2017 SCC OnLine Kar 424

[20] See § 3, Right to Information Act,Act No. 22 of2005.

documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force."[21]

While the terms '*data material to be held in any electronic form'* has been mentioned within the section, it is not an easy task to differentiate information or segregate it into sensitive, personal information or just information considering that there is no law in place for the same purpose. As the objective of "White Paper" is clearly stated, as to ensure growth of the digital economy while keeping personal data of citizens secure and protected; it keeps in mind and refers to the obiter of this Hon'ble court in *Justice K.S. Puttuswamy v. UOI,*[22] *which states "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state."* With this growing realisation the government, felt it was instrumental to have a legal framework for data protection, to facilitate India's digital growth. The courts have however opined and realised that, *"Formulation of data protection was a complex exercise which needs to be undertaken by State after a careful balancing of privacy concerns and legitimate State interests, including public benefit arising from scientific and historical research based on data collected and processed."*[23]

While the Supreme Court of India has recognised a general right to privacy, no general right relating to personal data protection has been developed to date.[24] Although the IT Act attempts to address the issue of protecting privacy rights, it fails to meet the objective as it only protects privacy rights from government action. In fact, SPDI Rules only apply to bodies corporate or persons located in India.[25]

The Calcutt Committee used as its working definition:
The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.[26]

Furthermore, it is also submitted that in today's era a lot of information that could be considered 'personal' has been expended out

[21] See § 2(1)(f), Id.

[22] *See* Justice K.S. Puttuswamy v. Union of India, 2017 (6) MLJ 267.

[23] *Id*., at ¶481.

[24] The judgement rendered by this hon'ble court in the *Puttuswamy* case was only recognizing a constitutional right to privacy and did not provide clarity to what information falls under this.

[25] Stephen Mathias & Naqeeb Ahmed Kazia, *Data Protection in India:Overview,* WESTLAW INDIA, (Jan 13, 2018) Available at: https://content.next.westlaw.com/Document/I02064fb41cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true.

[26] *See*The Calcutt Committee, Report of the Committee on Privacy and Related Matters, 1990, p. 7.

by the very person the information could stand to bring harm to. This has led to a problem in ascertaining what all comes under the ambit of personal information and therefore strict adherence cannot be made to any of the definitions under the Indian law.

A similar line of thought rendered by this Hon'ble court in the case of *State of Uttar Pradesh v. Raj Narain*[27], wherein on the matter of informational privacy the court stated that *"In a government of responsibility like ours, where all the agents of the public must be responsible for their conduct, there can be but few secrets. The people of this country have a right to know every public act, everything that is done in a public way by their public functionaries. They are entitled to know the particulars of every public transaction in all its bearing. Their right to know, which is derived from the concept of freedom of speech, though not absolute, is a factor which should make one wary when secrecy is claimed for transactions which can at any rate have no repercussion on public security".*[28]

The Supreme Court of Pennsylvania has expressly stated that once an individual's information becomes a matter of public record, the right to privacy with respect to that information ceases. [29] Further with a similar holding, the courts in the case of *R. Rajgopal v. State of Tamil Nadu*[30] *stated, "Every citizen has a right to safeguard the privacy of his own. However, in the case of a matter being part of public records, the right to privacy cannot be claimed."*[31] It is submitted that reference should be made to the opinion made by S. A. Bobde, J., in the case of *Justice K.S Puttuswamy v. UOI*[32] wherein he states the importance of a case to case decision making when it involved such a premature right.[33]

§ 6A of the IT Act prescribes that the government may for the efficient delivery of services to the public through electronic means authorise, by order, any service provider, which includes agency that has been granted permission to offer services in accordance with the policy governing that area.

Rule 3(3) Information Technology (Electronic Service Delivery) Rules, 2011 prescribes that the appropriate Government may determine the (sic) of encrypting sensitive electronic records requiring confidentiality while they are electronically signed, which thereby proves that if the government felt the necessity it could have issued protection on the information that the Service providers are to maintain its confidentiality.

After adverting to the evolution of the doctrine of privacy in the US from a right

[27] *See* State of Uttar Pradesh v. Raj Narain , 1975 AIR 865.

[28] *Id*., p.27, ¶1.

[29] *See* Naglak v. Pennsylvania State University., 133 F.R.D. 18 (M.D. Pa. 1990).

[30] *See* Rajgopal v. State of Tamil Nadu, 1995 AIR 264.

[31] Id., ¶26.

[32] *Supra* No. 3.

[33] According to S.A. Bobde J., *"No legal right could be absolute and every right has limitations. Such aspect of the matter was conceded at the bar. Therefore, even a fundamental right to privacyhas limitations. The limitations are to be identified on case to case basis depending upon the nature of the privacyinterest claimed ... Thus, it is critical that such standard be adopted with some clarity as to when and in what types of privacyclaims it is to be used. Only in privacyclaims which deserve the strictest scrutiny is the standard of compelling state interest to be used."*

associated with property [34] to a right associated with the individual [35], Chief Justice Lahoti[36] referred to the penumbras created by the Bill of Rights resulting in a zone of privacy[37] leading up eventually to a "reasonable expectation of privacy"[38] Post *Maneka Gandhi v. Union of India*,[39] the Supreme Court expanded the phrase "personal liberty" in its interpretation of A.21 to the widest amplitude.[40]

The word "personal" means appertaining to the person; belonging to an individual; limited to the person [41] and would be information, in any form, that pertains to an individual.[42]

Therefore information is in relationship to a public activity and will not be an intrusion on privacy.[43]

Hence, with the advancements in digital age and with the emergence of big data analytics, the need to protect privacy has only increased. The right to privacy is an inalienable fundamental right of all natural persons indispensable to the preservation of human dignity, personal autonomy and the exercise of constitutional liberties.[44]

It is therefore the need of the hour to put in place an effective regime to safeguard the crucial fundamental right to privacy of all natural persons and their personal data. An establishment of a data protection law and a Privacy Commission to look after the matters related to privacy like from surveillance of natural persons and interception of communications, etc. to name a few and for matters connected therewith and incidental thereto is the first step that our country now needs to take.

*****

[34] *See* Boyd v. United States, 116 US 616 (1886).
[35] *See* Olmstead v. United States, 277 US 438 (1928).
[36] *See* District Registrar and Collector, Hyderabad v Canara Bank (2005) 1 SCC 496.
[37] *See* Griswold v. State of Connecticut, 381 US 479 (1965).
[38] *See* Katz v United States, 389 US 347 (1967).
[39] Hereinafter referred to as the 'Maneka Gandhi case'.
[40] *See* Pathumma and Ors.v. State of Kerala and Ors. AIR 1978 SC 771.
[41] BLACK'S LAW DICTIONARY,567 (4th ed. 2011).
[42] *See* Rajagopal v. State of Tamil Nadu, MANU/SC/0056/1995 : AIR 1995 SC 264.
[43] *See* Rakesh Kumar Gupta vs. The Public Information Officers MANU/CI/0087/2009.
[44] *See* Justice K.S. Puttuswamy v. Union of India, 2017 (6) MLJ 267