CREATION OF DATA PROTECTION REGIME IN INDIA

By *Mervyn Vivek Tamby*
Advocate

PRIVACY AS A MATTER OF RIGHT

In this contemporary period, privacy is a basic right of each and every individual. There are plethora of legal instruments and court decisions which recognise privacy as a fundamental right, almost in every country. Especially, in the world engulfed with technologies and in internet activities, there is a high chance of violation of privacy rights of an individual. Here, it is important to draw our attention to some of the prominent international legal instruments which recognise the concept of right to privacy. The Universal Declaration of Human Rights[1]; The International Covenant on Civil and Political Rights[2]; as far as European Union is concerned, the European Union Charter of Fundamental Rights[3] and the Treaty on the Functioning of European Union[4] are the primary instruments which recognise the privacy rights of the Europeans. Therefore, it becomes obligatory for the signatory parties to recognize the right of privacy, under the rules of public international law.

For India, it took approximately 67 years from the date, the Constitution of India came into effect, to firmly consider privacy as a part of the fundamental right of the Constitution. Prior to this, the validity of right to privacy was like a tumult situation. Finally, the Hon'ble Supreme Court in the case of **Justice K.S. Puttaswamy & Anr. V. Union of India & Ors**[5]., held, unanimously that ***"the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution"***. Most of the countries in the globe legislated the Data Protection laws, particularly among them, the General Data Protection Regulation, 2016 (GDPR)[6] of the European Union has been a wake-up call for rest of the countries who didn't have an adequate or a properly legislated statutory material, particularly dealing with the subject of privacy law in view of information technology.

In India, the privacy law referred as the Information Technology Act (IT) 2000, is the prevailing law. Nevertheless, there is no vacuum in India in the area of data protection, but the aforesaid law and its rules remains to be infirm under many aspects for the people, do not contain the stamina to tackle the modern privacy issues and indeed lack proper protection and regulation. In the age of internet, one's privacy right could be easily and evasively transgressed. There are colossal of people who are still flummoxed about their rights and obligations of the data fiduciaries in view of the prevailing IT law.

[1] *See,* Article 12 of the UDHR, *available at https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf.*

[2] *See,* Article 17 of the ICCPR, *available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf.*

[3] *See,* Article 8(1) of the EUCFR, *available at https://www.europarl.europa.eu/charter/pdf/text_en.pdf.*

[4] *See,* Article 16(1) of the TFEU, *available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.*

[5] *See,* K.S. Puttaswamy & Anr. V Union of India & Ors., W.P. (CIVIL) NO 494 OF 2012, *available at https://indiankanoon.org/doc/127517806/.*

[6] *See,* GDPR EU 2016/679, *available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.*

Let's see some of the significant features of the new data privacy Bill which has been introduced in Lok Sabha[7]

INTENT OF THE BILL

First let us, explore the object and purpose of the bill. For the sake of easy understanding, I have mentioned below the actual intent of the bill in the following seriatim.

1. To protect the privacy of the individuals in respect of personal data.
2. To bring to the individual's knowledge about the purpose or usage of the collection of the data.
3. To construct trust between the actors i.e., the individual and entity which process the data.
4. To protect the individual's rights in this context.
5. To establish a regulatory framework for organisational and technical measures.
6. To lay down norms for social media and cross border transfer of data.
7. To make the processing entities accountable.
8. To sanction and lay down the remedies in case of unauthorised and harmful processing of the individual's data.
9. To appoint a Data Protection Authority to monitor and undertake the activities under the bill.

On the whole, the Bill's main purpose is to protect, safeguard and provide remedies when an individual's right is jeopardized.

SCOPE OF THE BILL

Under the Bill, an individual is referred as "Data Principal" and the information relating to that individual is referred as "Data". The scope of the Bill can be divided into Territorial scope and Material scope

a) Territorial scope

The scope of application of the bill is not limited to the processing of personal data within the territory of India, it also extends to cover the activity of processing of personal data by the data fiduciaries or processors who are outside the territory of India, but the processing is be done in relation to services or goods provided to the data principal within India, or includes profiling such as analysing the behaviour, attributes or interests of the data principal, taking place in India.

b) Material scope

When it comes to material scope, the bill applies when the processing is done by the following persons: -

(i) Citizen of India

(ii) Company incorporated under the Indian Companies Act (Includes both Public & Private company).

(iii) State has defined under Article 12 of the Constitution.

(iv) Other persons or body of persons incorporated under the Indian law.

(v) Data fiduciaries or processors includes any company, any person, any juristic person outside India and also includes a foreign state.

The purpose of processing must be lawful with proper consent and should be in consonance with Chapter II of the Bill. The Bill also proposes some circumstances in

[7]*See*, The Data Protection Bill, 2019, *available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.*

which the consent is not a prerequisite[8]. It is pragmatic, to have few exceptions for the purpose of processing of personal data without consent in certain circumstances so as to ensure, the functions of the sovereign are not impeded, because as we all know *"Too much of anything is good for nothing".* For instances, providing a service to the public, for compliance with court judgments, for rendering rescue operation in times of any disaster etc., in all such cases, the consent of the data principal is not at all required because requiring consent in those cases, obviously seems to be ridiculous and nonsensical. Further, the exemption is applicable in employment services, but the data fiduciary cannot gain the shelter if, the processing contains sensitive personal data of the data principal. Moreover, the Bill says, it is open for the Authority to extend the exemption by way of regulations.

The combination of both the scopes, may result for example, if a foreign company, in the process of doing business with an individual in India collects the personal data of that individual, the company has to comply with the Data Protection law of India.

As a result of bare reading of the bill, it could be inferred that the law once enacted, may come in aid not only for the citizens of India but also to the other citizens residing within the territory of India.

RIGHT TO ERASURE AND RIGHT TO BE FORGOTTEN – *The crux of the Bill*

The concept of right to be forgotten was well established **in the case of *Google Spain***[9] by the European Court of Justice (ECJ). In this case, the ECJ held that the interpretation of Article 12(b) read with Article 14 of the Directive 95/46 has given birth to the principle of "right to be forgotten" which the data subject acquires through, the protection of privacy right guaranteed under Articles 7 and 8 of the fundamental rights Charter and the ECJ also took into account that the principle of right to be forgotten would have an overriding right not only to the economic interest of the operator of the search engine but also to the interest of the public. However, in order to determine the overriding effect of the right of the data subject, the court applied the preponderance test, the privacy right of the data subject on side and on the other, the interest of the general public. On the whole, this principle was expressly incorporated under Article 17[10] of the GDPR regulation 2016 with some exceptions as provided in Article 17(3) of the GDPR.

In India, the principle of Right to be forgotten was first recognised **in the case of *Registrar General of Karnataka High Court***[11]. The petitioner in this matter, prayed for veiling of his daughter's name which appeared in the order of a compromised case between his daughter and her husband. The

[8] *See,* Chapter III of the Data Protection Bill, 2019.

[9] *See,* Google Spain & Google Inc.V Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, *available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.*

[10] *See,* Article 17 of GDPR EU 2016/679, *available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.*

[11] *See,* Karnataka High Court, The Registrar General on 23 January, 2017, *available at https://indiankanoon.org/doc/12577154/* .

daughter of the petitioner was worried that as a result of her name search in a search engine such as google; yahoo, etc., her name could be easily be available in the public domain. The petitioner's daughter apprehended that it would badly affect her family relationship and reputation in the society. Therefore, the petitioner approached the court for an order directing the registrar general to anonymise her name. The court ordered and held by stating that the western doctrine of right to be forgotten could be applied in highly sensitive cases involving woman as a party, in order to shield her image in the society.

In the matter of *Zulfiqar Ahman Khan V. M/S Quintillion Business Media Pvt.Ltd. And Ors*[12], the defendant published in its online platform, an article containing a baseless and frivolous harassment allegation against the plaintiff. Aggrieved by this article, the plaintiff filed a suit in a trial court and the court ordered in favour of the plaintiff. The defendant complied the order and removed the article published. Then, the article was republished by another news agency platform. On noticing this, the plaintiff approached the High Court of Delhi, to remove from all other sources. The High Court of Delhi, by considering the reputation of the plaintiff in the realm of his professional and personal life, ordered for erasure from all sources including, the search engines thereby, protecting and recognising the plaintiff's Right to privacy and its species, the "Right to be forgotten" and the "Right to be left alone", respectively.

Since the Data protection Bill is very much akin to the GDPR, this principle was included in section 20 of the Bill. The language of this section elucidates, *inter alia* that the right to be forgotten could be effectuated only on the application made to the Adjudicating officer and the enforcement of the right depends on the discretion of the Officer who is bound to follow the factors enumerated in sub clauses (a),(b),(c), (d) and (e) of section 20(3) whilst, arriving at a conclusion. Unlike GDPR, right to erasure is an absolute right which can be invoked under section 18(1)(d), where the personal data is no longer necessary for the purpose for which it was processed. In this connection, it is important to draw a distinction between the right to be forgotten under GDPR and the Bill. In accordance with GDPR, right to erasure could also be known as right to be forgotten because both the rights are not absolute and subject to the exceptions laid under the chapeau of Article 17 of the GDPR. But in the Indian Bill, it is obverse, as both rights are dealt with separate sections. Precisely, in pursuant to the Bill, right to erasure could be claimed as an absolute right and right to be forgotten is a right subject to some restrictions by virtue of structural interpretation of the Bill. In my point of view, the right to erasure and to be forgotten shall be more beneficial when compared with other rights in the Bill.

SANDBOX FEATURE – *Striking a balance between privacy right and innovation*

The sandbox is a great step taken by the government to encourage innovation in the field of emerging technologies for the benefit of the public, the intention behind this feature is not to render this Bill as an obstacle for

[12] *See*, Delhi High Court, Zulfiqar Ahman Khan V. M/S Quintillion Business Media Pvt.Ltd. And Ors on 9 May 2019, *available at https://indiankanoon.org/doc/172009054/* .

innovation in the field of artificial intelligence, machine learning and other emerging technologies. This feature would be useful for start-ups and other companies working for interest of the public. As novelty is an essential tool which contributes to the country's social and economic development, it becomes indispensable for a country's growth and the welfare of its people. Hence, in order to strike a balance between individual's privacy and innovation, this feature has been inserted as an exception in section 40 of the Bill.

Section 40 which deals with sandbox creates a ***"safe zone"*** in which the data fiduciary engaged in the technological innovation in the public interest can make use of this space as per the terms and conditions prescribed by the data protection authority to experiment their innovative products, to put it in other way, it is like an experimenting phase for the innovation using personal data of the data principals under the surveillance of the data protection authority. A significant responsibility lies on the data protection authority to ensure that this feature shall be made available to innovators only, who work solely in public interest. Regarding the procedure concerning for the inclusion in the sandbox, the data fiduciary should mention the period for enjoying the sandbox's benefits, however such period must not be beyond twelve months; usage of the technology; information in respect of participating data principals and other information as may be provided in the regulation, to the data protection authority. On the other end, the data protection authority has the obligations to mention the period; to specify the safeguards, terms and conditions bearing in mind, the purpose of processing; limitations on the collection of personal data and restriction on holding the personal data.

Thus, it can be deduced that sandbox is not an ordinary exception, it is a regulated feature in which both the data protection authority and data fiduciary should act cautiously, like walking on a tightrope, by finding a balance between innovation and privacy right of the individuals. But at the same time, there may be a chance for partiality when a government as a data fiduciary applies for the sandbox, as the exemption is granted by a public authority.

FINDING BALANCE BETWEEN DIGITAL JOURNALISM & DATA PROTECTION LAW

Journalism and privacy are mirrored as right to freedom of expression and right to privacy, under Articles 19(1)(a) and 21 of the Indian Constitution, respectively. The question of prevailing right among the rights (*supra)*, in case of repugnancy, is enshrouded by various conflicting decisions of the courts. However, one can witness, based on the interpretation of the Hon'ble Supreme Court of India, in cases involving the question of prevailing right under Part III of the Constitution, the court usually employs the test of proportionality or balance as warranted by the facts and circumstances of each and every case. Here, I would like to narrow my discussion to digital journalism; data privacy and social media. In technological world, one can easily transmit or pass the news, article, etc. from one side of the country to another, even it can be swiftly transferred across the world. So, in the event of violation of privacy right, the ramification would be on a large scale. On the other hand, each and every individual has the "right to know" which is

an offspring of right to freedom of speech and expression, is also a *sine qua non* for the application of such right. Hence, the courts have to look the matter in issue through microscopic eyes to find an equilibrium between those rights.

In the case of *M.L. and W.W. V. Germany*[13], two applicants requested before a regional court of Hamburg for the anonymization of personal data regarding their conviction and the result of their application for a retrial in a murder case which appeared in the archive of a radio broadcaster. The regional court ruled in favour of the applicants. The Court of Appeal upheld the regional's court judgment by holding that based on the test of proportionality, privacy right of the applicants well outweighed the public interest as the public were well informed about the news.

Furthermore the case was appealed in the Federal Court of justice which overturned the decision by taking into account that ***"blanket prohibition on access or an obligation to delete any reports concerning offenders named in an Internet archive would result in the erasure of history and in wrongly affording full immunity to the perpetrator in that regard"***. The Court also noted that the media's act is within the remit of media privilege and they could not be deprived of their work which subsequently, affects Article 11 – ***"Freedom of expression and information"*** of the Fundamental Rights of the European Union.

The case reached its final stage when the European Court of Human Rights affirmed the views and assessment of the Federal Court of justice and held that there was no infringement of the applicant's right to respect for their private life.

In my perspective, this case might be an eye opener for the inclusion of section 36(e) in an elaborated form under Chapter VIII of the Bill which says that, the processing of personal data has to comply with the code of ethics issued by the Press Council of India or by any media self-regulatory organisation. Indeed, it envisages an unequivocal intention of the government to prescribe or specify the limits of journalism in cases involving privacy issues of an individual, nonetheless, this provision might arise a question of interpretation in the Hon'ble Supreme Court of India when it is in conflict with data privacy issues as aforesaid, the provision has to be construed according to the facts and circumstances of each case.

SOCIAL MEDIA UNDER THE BILL

The Bill captions social media which are engaged in offering services like online interaction among its users, creating, uploading, disseminating, modifying and sharing information to its users as social media intermediaries, explicitly negates intermediaries providing commercial

[13] *See*, ECHR, M.L. AND W.W. v. GERMANY, 2018, *available at https://hudoc.echr.coe.int/eng#{"fulltext":["Ml%20v%20germany"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-183947"]}*.

transactions, search engines, email services, on-line encyclopaedias, on-line storages services and internet service provider. The Bill empowers the central government in consultation with the data protection authority to label the social media intermediaries "*whose action have, or are likely to have huge impact on the electoral democracy, security of the State, public order or sovereignty and integrity of India*[14]*."* as significant data fiduciaries and makes them to act according to the additional obligations as laid down in the Bill. The language of the provision tends to be broad and seems to discourage the social media intermediaries' growth because today most of the people use these platforms as a conduit to express their opinion, expression and voices, in addition, this provision may provide the government to tacitly control the dissenting voice of the user, which is consider as a safety valve of the democracy by the apex court in the ***Bhima koregaon case***. Sec 28(3)&(4) directs the social media intermediary to be tagged as a significant data fiduciary and to make the registered users of their service who are from and in India to voluntary verify their accounts. The users who underwent such process will be given an identification mark which can be seen by other users. Albeit, India is a first country to introduce such measure, these kinds of provision make the social media intermediaries burdensome.

DATA PRIVACY AND BANKING COMPLAINCE- *Head to Head*

The Bill is likely to hit the banking sector as the Bill remains silent regarding the processing of personal data of the customers of banking and financial institutions including online payment or money transfer platforms such as Google pay, Paytm, Phonepe, Amazon pay, etc. The concept of Know Your Customer (KYC) is in direct conflict with the privacy Bill. The master circular issued by the Reserve Bank of India[15] mandates the banks and financial entities to comply with KYC and due diligence procedures for the sake of preventing money laundering and other tax evading activities. Therefore, it is going to be cumbersome for the banks to comply with the data privacy bill as they have colossal of personal information relating to customers such as passport number, pan details; address proofs – electricity bill, telephone bill; pay slips; ration cards, email address, property details in case of availing loans etc., for the compliance and effective banking purposes. So, as per the data privacy bill, the banks and financial institutions are bound to acquire prior consent for using or processing the personal data of their customers. Their duty doesn't stop here, their role as a data fiduciary makes them obligatory to provide access to their customers to all documents and matters relating to their personal information.

Coming to recovery of debt action and privacy issue, the apex court in **Ram Jethmalani & Ors V. Union of India**[16], observed that, ***"The revelation of details of bank accounts of individuals, without establishment of prima facie grounds to accuse them of wrongdoing, would be a violation of their rights to privacy. Details***

[14] *See*, sec 26(4)(ii) of the Data Protection Bill, 2019.
[15] *See*, RBI KYC compliance circular, *available at https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607*.

[16]*See*, Ram Jethmalani & Ors V. Union of India 4 July 2011, *available at https://indiankanoon.org/docfragment/1232445/?formInput=privacy%20violation%20by%20bank*.

of bank accounts can be used by those who want to harass, or otherwise cause damage, to individuals."

Since, the recovery of debt comes under the exceptions category it may not be necessary for the banks and financial institutions to obtain the consent of the data principals. But it cannot be left alone like this, because this kind of exception may subject the customers to harassments. Thus, in my point of view, based on the conjoint reading of the data privacy Bill and the above-mentioned case, to recover a debt, mere existences of debt should not be encouraged, unless the fact of existence of debt is substantiated with sufficient material evidence in order to claim the shelter under section 14(2)(f).

CONCLUSION

The government of India has brought this robust Data Protection Bill with the aim to protect and safeguard the individuals from invasion of their privacy rights. Apart from the above-mentioned rights, the Bill proposes other rights such as right to confirmation and access, right to correction, right to data portability in case of cross border transfer of data and special rights relating to persons below the age of 18, it is obligatory to get the consent of the parent or guardian. Thanks to the Justice B.N. Shrikrishna Committee, which played a significant role for the construction of this Bill. India, at present, suffers from lack of strong privacy law which leads to violation of privacy right in the world of technologies. In my opinion, this Bill is well structured except some chance of favouritism towards government because, as we have seen, it also includes government as a data fiduciary and allows the major gaps in the Bill to be filled by the government through regulation as and when required. It's like framing rules for themselves. Apart from this, once it is enacted would surely fill the grey areas left by the prevailing information technology law and tends to streamline the present situation which is flummoxed, in the field of data privacy in India. On the other hand, the Bill opens the doors for employment opportunities in the field of Data protection managers or officer in many sectors. Overall, this Bill is a panacea of rights in which, the individuals could find a solution in a timely fashion. It's also good to see the flexibility of the Bill, so as to counter any future developments because this area is like a wave subject to frequent changes and modifications.

*****