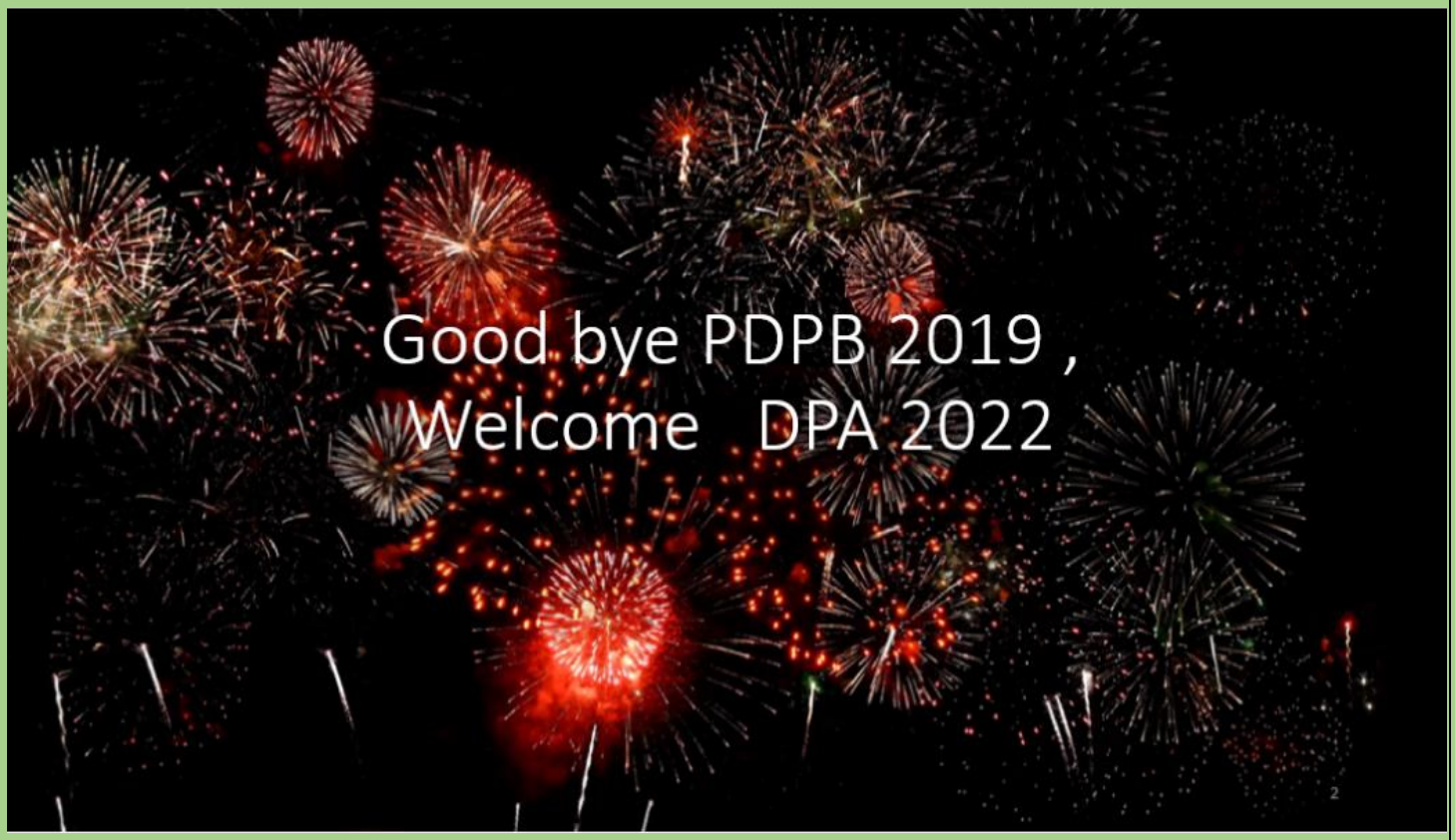
Data Protection Journal of India

Volume 2: No: 1/2022: 31st January **2022**



The New Data Protection law of India unveiled

Journal published For

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

Publisher: Na.Vijayashankar

What is Inside

Previous versions of the Journal are available at www.dpji.in

From the Chairman's Desk

On December 16th, 2021, the long-awaited report of the Joint Parliamentary Committee on Personal Data Protection Bill 2019 was placed with the Speaker of Lok Sabha.

The detailed report has provided the suggestions of the JPC for amendment of different provisions of the PDPB 2019 which had been formally tabled in December 2019 along with a version of the Bill as it would now appear after all the amendments are incorporated.

When passed, the Act is expected to be named "Data Protection Act 2022" or DPA 2022.

FDPPI has already activated action on updating of all its previous programs and in association with its training partner Cyber Law College also conducted two webinars to update the previously certified persons with the changes.

The Bill is expected to be presented during the Budget session starting from February 1, 2022, and passed during the session.

This issue of the Journal tries to present some of the discussions relevant for all of us to understand what has changed between PDPB 2019 and DPA 2022.

Additionally, this issue also records the deliberations of IDPS 2021 which was held as a virtual event on November 18, 19 and 20, 2021. We had covered the details of the program as envisaged in our earlier issue which was released on 31st October 2021. The deliberations were all in tune with the earlier program as planned.

Mr K N Narasinga Rao one of our members has prepared a summary of the events which is provided in this issue.

We thank all the members of FDPPI who assisted us in making the event successful. We specially thank all the external speakers who by their participation enriched the proceedings.

We hope in the coming years, the event will gain further strength and we would be in a position to conduct it as a physical event.

Naavi

Please Note

For the first time in this issue, we are giving a direct Video link to a discussion on the Metamorphosis of PDPB 2019 into DPA 2021/22. This is a 3-hour webinar conducted by Naavi on 9th and 16th of January 2021. This makes this issue a hybrid issue as a "Video Magazine". In future, more such short videos would be made available as part of the issue.

News Section

From the Newsroom

1. The JPC on PDPB 2019 submitted its final report to the Speaker of Lok Sabha along with the suggested amendments. 8 opposition party members submitted their dissent notes.
2. In the GDPR domain, total penalties in the year crossed $1.2 billion. This is 7 times increase over the corresponding previous year. Notifications of data breaches climbed by 8% to 356 a day on average. The fine included the record fine of 746 million euros imposed by Luxembourg authority on Amazon.
3. European Data Protection Supervisor (EDPS) has accused EU Police Body, Europol of illegally holding information equivalent to 3 million CD ROMs and ordered that Europol erases the data held for more than six months within the next one year.
4. In another order EDPS has held the European parliament guilty of allowing data transfers to Google and Stripe illegally and handed over a reprimand and an order to comply. The EDPS has been appointed jointly by the European Parliament and the Council for a term of 5 years.
5. Mr Masood a Muslim activist in Telengana has approached the Court with a plea that use of Facial Recognition is illegal and unconstitutional.
6. Aditya Birla Fashion and Retail has reported that over 5.4 million email addresses were released online by hackers. Company has said that no sensitive information has been breached.
7. A Security firm has claimed a vulnerability in CDSL exposing sensitive data. The extent and scope of the breach is not available. The data related to investors with a net worth of over Rs 1000 crores. CDSL has claimed that there was no data breach though it admits the vulnerability.

8. According to a report in BBC.COM, the AI led Amazon owned device Alexa instructed a 10 year old girl to touch a live electric plug. Though the girl did not respond, and a tragedy was averted, this highlighted the dangers of errors committed by the AI systems.
9. About 13 million records of the UK Police data was released by Russian hackers to the dark web under a ransom demand.

Knowledge Section

Report on IDPS 2021

By

Mr K N Narasinga Rao

Day 1: 18th November 2021: Bated Breath

Yes indeed, on Day 1 of the IDPS 2021, it was easy to see that there was a certain anxiety about what will be the nature and constituents of the final draft of the PDPB, and when it will see the light of day.

Stake holders committed to data protection are waiting with bated breath. But it was a kind of relief and reassurance felt when Justice Srikrishna, in his captivating delivery, mentioned that he feels that the Bill will be through this winter session of parliament, even as he expressed that he too cannot speculate about what the final provisions of the Bill will be.

Justice Srikrishna conveyed that privacy is not a new concept and its importance was heralded in the ancient scriptures of the land as part of hitopadesha. He quoted the ancient text mentioning 9 aspects that always need to be kept secret about oneself including age, wealth, domestic issues, charity etc…

Data Subject was the term used in GDPR and Justice Srikrishna elevated the individual status to that of a Data Principal in the draft bill. Speaking about data localization, he stressed that it is not practical to rely on treaties to get access to data stored in servers abroad, instead a copy of it should be stored locally. He emphasized on the importance of time as to when the bill will be made a law, and that it needs to be spelt out clearly and not left indefinite. He elaborated on why non personal data is not a fundamental right and how complex laws can be enacted section by section instead of at one go.

In general, there was a clear message that the privacy law has to be enacted as early as possible.

On the matter of identifying sensitive personal information, Justice Srikrishna said that what is sensitive is a personal matter and depends on a certain cultural imprint.

Earlier in the day, the welcome speech by Sri SP Arya and the introduction to the event by Sri Naavi set the tone for the rest of the day and the event as a whole.
Sri Arya stressed on the importance of data protection in the wake of the ever-increasing intensity of cybercybercrime incidents especially ransomware. He emphasized on how 130 nations have enacted the privacy laws and how other nations are in the process of implementing new laws.

Sri Naavi, in his introductory address, introduced the structure of FDPPI and went on to mention how the privacy rules are already in force in India through the provisions of ITA 2000/08. He spoke about the importance of PDPSI framework and how it is an Indian version of a framework that the other nations can use across the world. Sri Naavi emphasized how due to lack of valuation of data, a particular private company lost out on INR 100cr during its insolvency process.
Later in the day, as part of panel discussions, panellists emphasized on the importance of building privacy awareness starting at home and at school. There are good opportunities for data protection professionals especially the DPO roles. It was said that DPO role needs several skills including technical, legal, auditing, good communication etc . and, on a lighter note, it was mentioned that it may be difficult to find a person who can interview and select a DPO.

In another panel discussion, a specific takeaway was about how AI and data analytics technologies are used in profiling and used for social exclusion

purposes. The difficulty of identifying offline data stored in order to comply with right to be forgotten requests, was spoken about. Advertisements are believed to be the source of funds to keep the internet running free of charge for users. But if privacy laws force cookies and tracking apps to be blocked, then advertisements suffer and may result in basic internet access being made chargeable.

Panellists stressed on how data scrapping tools are blocked in order to block harmful tracking and profiling of individuals. On the issue of misuse of legitimate interest to access personal data, the panellists opined that as long as due process is followed it is necessary to trust legitimate interest requests.
The importance of fair adjudication was emphasized by the knowledgeable panellists especially in the case of percentage-based penalty determination and the conflict of Data Protection laws with the sectoral and also new central legislations like RTI.

Overall, it was a day when the data protection professionals viewing the event, were treated to a plethora of knowledge packed information.

Day 2: 19th November 2021: Zooming In

While the 1st day was all about the contours of the PDPB and the suspense around it, the 2nd day shifted focus towards zooming into more tangible area of familiarity – the corporate.

There was a natural curiosity about how the companies will cope with the rather fuzzy demands of the data protection rules across the globe. Companies with global presence or serving global customers, are exposed to the requirements of the global privacy laws prevailing, with different depths. With some exceptions, there may not be many companies that have understood the applicability of these

laws clearly, and that have gone on to conduct audits and reviews. Perhaps, the seriousness and commitment would increase manifolds once a law is in place and the threat of fines hang on the head.

Even before delving into the data protection domain, the participants were treated to an enlightening session on cyber security and data breaches from Dr Triveni Singh, IPS, SP UP Police, a renowned cybercrime and financial fraud investigator. Dr Triveni spoke about the mounting cyber fraud incidents in UP quoting 70k cases in past 2 years with 10k FIRs filed, a majority of which are of the financial kind. He revealed a rather startling information that some cyber security compliance certifications for companies are available for paltry payment of 15 to 20k rupees. He however rued the fact that many BFSI segment corporates ignore compliance requirements in-spite of IRDA insisting upon them. The awareness amongst the top management and the seriousness about incident handling is sadly absent in many companies. Dr Triveni emphasized that it is very easy for a hacker to steal employee credentials information and sell it in private or through dark web. He supported his claim with many examples in real world. He lamented that companies are concerned about reporting cyber data breach incidents due to the fear of damaged reputation and bad press. They tend to hush up the incident instead of doing internal investigations and forensic due diligence. The HR is a significant owner and custodian of sensitive personal data of employees. A captivating panel discussion revealed the challenges and what measures have been taken by corporates belonging to different verticals. The practice of sharing incoming CVs with many internal managers indiscriminately was seen as a practice to be changed. Tracing of data flow and being sure where all data resides is very important to satisfy the rights of individuals as per the law. Panellists reinforced the fact that a lot of technology intervention is necessary to comply with the rules of data privacy.

The participants were enlightened about the SCC requirements and the Schrems II invalidation of privacy shields. Additional checks are necessary in instances of cross border data transfer. On the impact of GDPR on Indian Companies, panellists opined that compliance was never a onetime activity and instead a continuous vigil of due diligence coupled with internal assessments and audits were necessary. Awareness of the impact of the GDPR regulations and the consequences of non-conformity were discussed to be very important. The supply chain issues that make visibility of data and a control on them is a big challenge and privacy by design is vital component of compliance. In the international sphere, the conflict that exists between state laws, sectoral laws and federal laws in the USA was highlighted to be a nagging issue.

An engaging panel discussion on Technology tools threw light on the importance of Zero Trust and DLP as such and the overall cyber posture of the organization. Panellists were unanimous in saying that even though there are security measures like firewalls, end point protection, email security, and provisions like sandbox testing, virtual desktop and thin clients – there is always the threat of advanced attacks exploiting unknown vulnerabilities. Collaboration tools used for online purposes have been upgraded to allow configurations for consent, and personalized settings. Panellists said that privacy policy, privacy by design, and privacy scoping in application development are crucial activities that contribute to due diligence.

The main takeaway from the 2nd day session was the knowledge about how different functions inside organizations are coping with the challenges of compliance including the HR, the IT, the supply chain and the insightful view from outside the corporate by Dr Triveni Singh.

Day 3: 20th November 2021: Winding Down

It was a hectic 3 days of a rollercoaster ride delving upon myriad details of the data protection subject. As Sri Ramesh summed up at the end of the event in his synopsis, it was a very productive 3 days.

As the curtains were drawn on the event at the fag end of the day, the takeaways were plenty and if the event has succeeded in generating a new curiosity and interest in Data Protection – then the event has achieved a lot. Thanks to technology, many were able to attend the sessions. It seemed like the virtual participation was not a dampener but an enabler.

As Sri Sanjay Sahay, IPS, ex ADGP, Karnataka, mentioned – it was a heartening response to a new coming domain of data protection addressing all the nuances and organizing such an event is not an easy job at all. He said that the event is an attempt by FDPPI to bring India up to speed in the complex area of Data protection and has deciphered many crevices in the challenging domain. Sri Sahay in his breath taking delivery, deliberated upon the importance of technology and how the challenges of data protection are at the crossroads of technology and law. He said that the complex subject of data protection needs interdisciplinary skills. Sri Sahay reiterated on the importance of data and how it is used as a money spinning means by those who manage it. Interestingly, he said that the concept of privacy by design is easier said than done as not many understand the technology aspect clearly. Policy, Law, Technology and Enforcement form the important factors and enforcement is not adequate although an IT act is in place. Sri Sahay was candid and came down hard on the IT behemoths who are ruling the roost and no amount of political or government intervention is able to control them.

At the end of Sri Sanjay Sahay's session, Sri Naavi said that the session has left the audience awestruck, while Sri Ramesh exclaimed that the session left him shellshocked.

Sri Rakshit Tandon, a renowned cyber security evangelist and trainer, said that the Healthcare, Fintech and Edtech are critical sectors as large volume of sensitive personal information is handled by them. As a part of his keynote address, on the topic of Privacy and Social media, he narrated about a ploy by con artists who steal information from vulnerable and unsuspecting users – A user calls a helpline number of a bank, but there is no response, and soon after, there is an incoming call from a con artist masquerading as a bank agent. The agent claims to represent the bank and seeks account details and information of credit card etc … from the hapless unsuspecting victim. He stressed on the importance of protecting children from cyber crimes by building awareness in them. In another panel discussion, panellists emphasized on how cyber security, data protection and privacy apply to smart cities and payment companies. The panellists particularly expressed concern about the vulnerable citizens in the rural areas where the awareness is absent about cyber security and rights over their personal data.

In his presentation on Data Valuation, Sri Naavi mentioned as to how the awareness of the value of data held by a company is important to set the budget aside for tools that are needed to protect the data. The valuation of data is needed as it will be used to justify the support for DPO roles. Just as the share price of an organization depends on assets held amongst many other factors, the data held by the company too must be viewed as a similar asset. Data value should be considered in the same manner as how the intangible assets like IP rights, Trademark rights and goodwill etc… are looked at. Sri Naavi expressed his opinion that customers should give consent for certain purposes beyond the primary, so that certain value added services can be turned on for themselves.

Later in the day, as part of a panel on the same topic, the panellist cited an example of how a food delivery company can use the customer data collected to provide advisory services to hoteliers who want to setup business in a particular area. The customer dietary preferences can be shared with the hoteliers for focused services. But this is beyond the purpose for which the data was collected initially. Earlier, as part of a panel discussion on the impact of privacy upon innovation, the panellists strongly believed that privacy must be a factor of consideration at every step of development. Innovation will bring its own solutions to privacy challenges. The risks posed by medical implants were discussed. These implants being IOT devices can share vital parameters pertaining to the patient. Adequate protection techniques including encryption and geofencing need to be implemented. The risks posed by GPS enabled devices which share location information were also discussed.

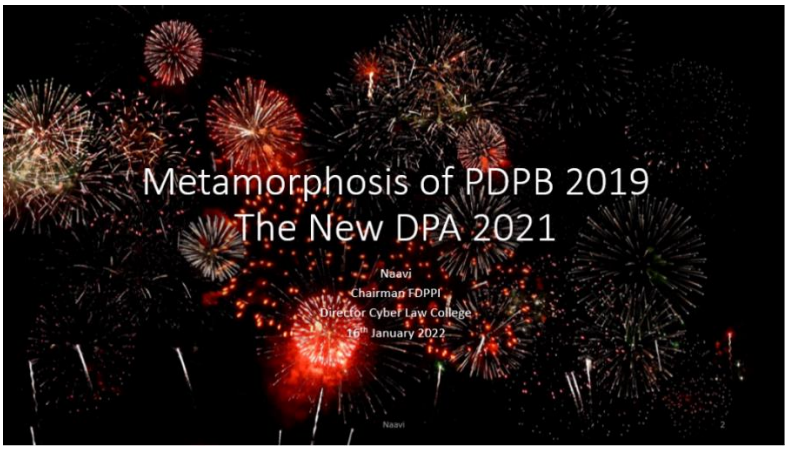
Sri Ramesh presented a very informative session on PDPSI framework. He highlighted the unifying property of the framework that addresses the requirements of different standards, regulations and frameworks like ISO, GDPR, CCPA, HIPAA, NIST etc.. He shared information about how FDPPI as an accredited certification body is geared up to enable compliance in relevant organizations.

IDPS 2021 was a unique event, on an emerging topic. Such events are difficult to organize and meet the intended objectives. It can be safely said that FDPPI has taken the lead position in thought leadership in the challenging domain of data protection.

With the PDPB on the verge of being tabled in parliament, this event was a timely one and there can be no doubt that many practitioners, enthusiasts, and other

interested parties would have benefitted from it. The ecosystem looks forward to IDPS 2022 with a renewed curiosity and lots of positive hope.

The New Modified Data Protection Act



This is a video of a webinar conducted by Naavi on 16th January 2021

In December 2019, the Government of India had presented Personal Data Protection Bill 2019 (PDPB 2019) as a revised version of what Justice Srikrishna Committee had drafted and presented along with its report. This bill had been referred to the Joint Parliamentary Committee (JPC) which after a long deliberation and wide public consultation, presented its report to the parliament on 16th December 2021 where a new draft bill with clause by clause amendment to PDPB 2019 was presented. In this bill the title of the Act was amended as Data Protection Act 2021. However since the act is now scheduled to be passed in 2022, it is likely to be renamed as Data Protection Act 2022 (DPA 2022).

This document tries to capture some of the salient amendments that have been suggested to PDPB 2019 by the JPC.

A total of 81 recommendations have been made in the Bill along with 150 drafting corrections. Out of these, around 30 major recommendations are discussed here in below.

1. **Scope of the Act widened:**

The first observation on the amendment is that the applicability of the Act has been extended to "Non Personal Data" also in certain respects and hence the name of the Act itself has been modified to drop the word "Personal" and calling it as "Data Protection Act 2021".

Further, under Section 2 of the Act, a new subsection 2(d) has been added stating that the provisions of this act shall apply to the processing of non-personal data including anonymised personal data.

However the actual changes made in different operating sections are limited to Section 25 related to the reporting of data breach of non personal data. According to the new provisions such data breaches must be reported to the Data Protection Authority of India (DPAI) created under this Act along with the breach of personal data.

Currently data breach of both personal and non personal data is being reported to the CERT-IN as per the provisions of the Information Technology Act (ITA 2000).

An enabling provision has been created under Section 25(6) that the DPAI shall after receiving the data breach report of non personal data take such necessary steps as may be prescribed. We therefore need to wait for the further regulations to come out in this regard.

To avoid overlapping of the DPAI and the CERT-In activities regarding the follow up action that may be required in respect of any data breach, it is expected that the data breach may have to be reported to both CERT IN

and DPAI but directions for follow up action in respect of non personal data would be given by the CERT-In and in respect of personal data by the DPAI.

By notionally expanding the scope of the Act to Non Personal Data, the section 92 (earlier numbered as 91) in which the Government had empowered itself for "directing any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed" has come within the scope of this Act. The possibility of the section being questioned for its validity on the ground that this section was ultra vires the Act has therefore been removed/reduced.

2. **Implementation Time:**

While no changes have been made in the Bill on the implementation schedule, the Committee has recommended that different provisions of the act may be implemented over a period of 24 months.

The first step would be the appointment of the Chairman and Members of the Data Protection Authority of India (DPAI) within 3 months. Following this, DPAI must commence its operations in the next 3 months and start registration of organizations within the next 3 months. Adjudicators and tribunals are recommended to be set up within 12 months. All other provisions are recommended to be completed within 2 years.

3. Inclusion of "Psychological Manipulation" as "Harm"

Under section 3(23)(xi), the list of "Harm" now includes "Psychological manipulation which impairs the autonomy of the individual".

Whenever law tries to enter the domain of "Psychology", it would be treading an area of "Uncertainty". The very aspect why "Privacy Protection" by the industry is complex is that "Privacy" is a "State of Mind" of an individual and for others to understand and do things which are not an infringement of the state of mind is almost impossible. We can only try a reasonable approximation to "Privacy Protection" by recording the choice of the individual and then try to strictly follow the choice.

As a "Fiduciary" however, the Data Fiduciary is expected to go beyond the "Expressed Choice" and "Anticipate" what is good for the data principal and try to provide that "Anticipated Choice". At the same time "Profiling" which is nothing but "Anticipation" and "Forecasting" is itself a processing activity that requires the consent.

The current concept of "Privacy" which is "Privacy1.0" does not even omit the "Observation by non human technical devices such as the hardware and software" for the purpose of "Consent" makes it difficult to remain compliant to the depth to which "Privacy" as a right can be interpreted.

The definition of "Psychological Manipulation" in the law also uses the condition "Impair the autonomy of the individual". Hence harm can be imputed if an individual is made to change his state of decision in a particular manner to another because of an information input. Whether it is "Impairment" or "Knowledge" is now for Courts to interpret.

When we conduct “Harm Risk” assessment as part of the Privacy Risk assessment and DTS calculation it will now be necessary to make “Psychological Impact analysis” as well.

4. **Definition of “In Writing”**

In the Previous version, definition 3(23) stated, that "in writing" includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;

In the current Version the definition has been modified as, “in writing” includes any communication or information in electronic form generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

This may be considered as “de-linking” the definition of “Writing” from the ITA 2000. While by itself this looks inconsequential, it may leave a shadow of impact on the interpretation of “Authentication” of an electronic document under ITA 2000 which is dependent on an electronic signature.

5. **Lawfulness defined with specific reference to this Act only:**

Under Section 4, it is now stated that processing of personal data by any person shall be subject to the provisions of this Act and the rules and regulations made thereunder. In the earlier version, it stated that “No personal data shall be processed by any person, except for any specific, clear and lawful purpose” This definition left the scope for bring in “Lawfulness” with respect to a law outside this act. Now it appears that the lawfulness would be considered only with reference to this act.

6. **Manner of Sharing data with a Processor to be specified**

Under Section 8(4) it has now been stated that a data fiduciary may share, transfer or transmit the personal data to any person as part of any business transaction in such manner as may be prescribed. The addition of the words "As may be prescribed" suggests that some elements of a contract between the Data Fiduciary and the Data Processor that needs to be included in the Data Processing contracts may be specified by the DPAI like the "Standard Contractual Clauses".

7. **Period of Retention beyond processing**

By a minor amendment to Section 9(1) requirement of deletion of data at the end of "processing" has been extended to the end of "period necessary to satisfy the purpose for which it is being processed". This change can be interpreted as providing some flexibility for extended retention based on the legitimate interest of storage of data for a period beyond the primary processing activity.

8. **Reasonable Expectation of the Employee**

As regards the processing of non-sensitive information in employment scenario, the amended section 13(1) states that if the data principal, namely the employee may reasonably expect that his personal data will be processed in a certain manner, the absence of consent may not be considered a deficiency.

9. **Exception to Consent requirement**

Under Section 14(2)(c) consent exemption has been recognized in the context of "Mergers" and additionally "any other similar combinations or

corporate restructuring transactions in accordance with the provisions of applicable laws".

This addition may avoid the controversies on what is a "Merger" and what is "Acquisition" or any other form of corporate restructuring.

10. Handling of Children data when they attain majority

A recommendation has been added (without suggested amendment) that three months before a minor attains majority, the data fiduciary should inform the child and seek fresh consent on the date of attaining majority. But the recommendation also suggests that the services will continue unless and until the person opts out to avoid discontinuity. There is a contradiction in this suggestion which needs to be resolved by the DPAI when drafting the regulation.

11. Nomination for Data Asset

One other interesting propositions which could be a legal nightmare is that under Section 17 on the Rights of the Data Principal the following right is added.

"The data principal shall have the following options, namely:-

(a) to nominate a legal heir or a legal representative as his nominee;

(b) to exercise the right to be forgotten; and

(c) to append the terms of agreement,

with regard to processing of personal data in the event of the death of such data principal."

While this provision does address one of the issues of dealing with the disposal of the data assets of a deceased person, it must be understood that "Nomination" in the general legal parlance is not "Inheritance" and does not settle the title to the property of the deceased. The Nominee becomes the trustee and executor on behalf of the legal heirs and the asset controller is discharged of his responsibilities by handing it over to the nominee.

The Nominee becomes the "Substituted Data Fiduciary".

The legal nightmare comes from the fact that the rights of the nominee originates from a "Consent" document that is signed by the data principal while he was alive and operative when he is deceased. Since the "Consent" undersection 11 has to comply with the standard specified under Section 14 of Indian Contract Act and is also bound (In electronic documentation of consent) by the prohibition for recognition of digitally executed Will under Section 1(4) of ITA 2000, the "Nomination" has to be executed only through a paper document until ITA 2000 is amended suitably.

12. Right to Portability and Trade Secret

In Section 19 of PDPB 2019 the right to portability was held as not applicable when it would reveal the trade secret of any data fiduciary. In PDPA 2021, the section has been modified with the removal of the specific mention of the "trade secrets" and it has been left to the DPAI to issue appropriate guidelines. While this does not mean that "Trade Secret" would not be a factor to be considered, the data fiduciary may have to consider it as part of his "legitimate interest" and raise the dispute with the adjudicator if necessary.

13. Right to Forget clarified

In PDPB 2019, Section 18 addressed the Right to correction and erasure and Section 20 addressed the Right to forget. The distinction between the two were not clear. While Section 18 reiterated that data collected for the purpose should be considered for deletion once the purpose is over and it would be part of the principles of processing and determine the lawful basis, Section 20 spoke of the "Disclosure" to prevented. The Right to forget was therefore linked to the "Disclosure" of the information after the purpose of collection is over. Right of deletion after the purpose was considered part of the Section 18 itself.

In the amended PDPB 2021, the right to forget has been clarified as to extend to "Processing" also.

Similarly the right of the data fiduciary to retain data for its own "legitimate interests" was also available in PDPB 2019 as part of the extended definition of the "Purpose". In PDPB 2021, a clarification has been added under Section 20 that such a right is to be recognized by the adjudicator while making any order on the right to forget request.

14. Transparency-Algorithmic Processing

Under Section 23 (h) on "Transparency", the information that should be made available to the data principal now includes "fairness of algorithm or method used for processing of personal data; " .

There is no mention here about the protection of trade secret or existence of patent rights which could be a point of legal exploration in the coming days.

15. Reporting of Data Breach

Section 25 of the act deals with the reporting of data breach to the Data Protection Authority. A clarification has been added to suggest a reporting time of "within 72 hours" which was earlier expected to be part of the regulations but has now been added in the section itself.

A second change in the same section is the addition of 25(6) stating as under:

(6) The Authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed.

This only suggests that the data breach of non personal data also has to be reported within 72 hours and later DPA may take such steps as may be required. However, it must be remembered that reporting of data breaches for both personal and non personal data still is required under ITA 2000 also to the CERT-IN. The DPA may not be the custodian of prevention of "Cyber Crimes" and hence the responsibility of the CERT IN to respond to a Non Personal Data Breach would be more than that of the DPA. On the other hand, when there is a personal data breach, while the DPA will look at it from the point of view of compliance or failure there of by the Data Fiduciary, the CERT-IN and the Police would be still required to carry out their own investigations from Cyber Security perspective and Cyber Crime perspective.

By adding the Non Personal Data breach within this law, while the Government has solved the problem of having two different regulators one for Personal Data and another for Non Personal Data, some additional overlapping might have been created now between the CERT IN and DPA.

While the role of sectoral regulators have been acknowledged under Section 26, the role of CERT-IN has not been given any recognition. ITA 2000 provides a "Quasi Judicial" status to the Director of CERT-IN but PDPA 2021 seems to have not given due recognition to the office of the Director of CERT IN who is designated as the "Nodal Officer" responsible for Critical infrastructure security as well as Cyber Security in general.

16. Social Media Intermediary

ITA 2000 has been grappling with the regulation of social media as "Intermediaries" under Section 79 and the Intermediary guidelines of February 25, 2021 addresses the regulatory mechanism which covers, the need for "Self Regulation", Regulation at the community level" besides declaring social media intermediaries above 50 lakh registered subscribers as "Significant Social Media Intermediaries". Such Significant Social media intermediaries are required to ensure that the identity of the members to be verifiable and a mark to be placed for the view of others.

The issue of providing an opportunity for users of the Social Media intermediaries came up because there was a need to control "Fake Accounts" through which false news was being propagated. This was addressed in PDPB 2019 with the provision that users should be given an opportunity to identify themselves and the social media make necessary arrangements to display the identity.

Now PDPA 2021 has used a terminology of "Social Media Platform" and under Section 28(3) and (4) prescribe as follows:

(3) Every social media platform which is notified as a significant data fiduciary under sub-section (1) of section 26 shall enable the persons who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.

(4) Any person who voluntarily verifies his account on a social media platform referred to in sub-section (3) shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.

When the above is read along with Section 26(4) which states

(4) Subject to the provisions contained in section 56, the significant data fiduciary shall be regulated by such regulations as may be made by the respective sectoral regulators.,

there appears to be a possibility that the ministry of information and broadcasting which under the Intermediary guidelines of February 25 is required to designate a ministry level authority for regulation could be considered as a "Sectoral Regulator" for Significant Social Media Intermediary.

17. Guardian Data Fiduciary

PDPB 2019 had recognized a category of data fiduciaries as "Guardian Data Fiduciaries" where significant data of children are likely to be processed. This category has now been merged with the "Significant Data Fiduciary".

18. Concurrent Audits

Under Section 29 where the requirement of annual data audit is prescribed, it has been mentioned that the authority shall encourage the practice of

concurrent audits. No clarification is provided if the concurrent audit must be conducted by an internal audit team or an external auditor.

19. Data Protection Officer

The PDPA 2021tries to elaborate on the credentials of the Data Protection Officer (DPO) to be appointed by a Significant Data Fiduciary.

Firstly it refers to the DPO to be a "Senior Level officer" in case of the Government and a "Key Managerial personnel" in a company possessing such qualifications as may be prescribed for the functions to be discharged. The explanation to Section 30 goes on to add that "Key Managerial personnel" means the CEO or Company secretary, the whole-time director, the CFO or such other personnel as may be prescribed.

It is not clear why the Government felt it necessary to spell out the designations such as Company Secretary and CFO while omitting the CCPO, CRO, CTO or CISO.

20. Cross Border Transfer

Contrary to expectations the section 34 on cross border transfer has not been changed and there are no restrictions on cross border transfer of data.

There is no mention under Section 34 about non-sensitive personal data and therefore it is freely transferable even without keeping a copy in India.

As regards the Sensitive personal information, transfer is permitted when an explicit consent is give and it is supported by a contract with the transferee protecting the interest of the rights of the data principal.

In the case of Intra-group scheme the DPA is expected to approve the scheme in consultation with the Central Government. The need for

Government intervention in every intra-group schemes even after the authority is required to approve may introduce unwanted procedural hurdles in the operations of a company without a corresponding benefit.

Also it is stated that sensitive personal information shall not be "shared with a foreign Government or agency". Once the information is allowed to be transferred out of India, it is difficult to envisage how the data exporter can exercise control in preventing the sharing of the information by the Data importer with a foreign Government.

There is also a provision that the transfer of sensitive personal data may not be permitted if the transfer "Promotes any breach of law" or is opposed to the "public policy" or could harm the interest of the state or its citizens.

21. Exemptions to the Government

Section 35 has been one of the most hotly criticised sections of PDPB 2019. It provides the Government or any of its agencies may be exempted from the provisions of law under certain circumstances such as in the interest of national security etc. Though the exemptions were limited to what was permitted under Article 21 of the Constitution as "Reasonable Exceptions" for fundamental rights, there have been criticisms that this could be misused by the Government.

To reduce the perceived objections and explanation has been added stating that the powers under this section shall be used only under an appropriate procedure and

"the expression "such procedure" refers to just, fair, reasonable and proportionate procedure. "

22. Constitution of the committee for selecting the Chairman and Members of the Data Protection Authority

The PDPB 2019 had stated that the Chairman and the members of the DPA would be selected by a three man committee of the Cabinet Secretary, Secretary of Law and Justice. and Secretary of the Meity. The composition of this selection committee was criticized since it could lead to a biased selection.

Under PDPA 2021, the committee has been substantially expanded with the inclusion of the Attorney General of India, an independent expert to be nominated by the Central Government, one Director of IIT and one Director of IIM.

23. Hardware and Software Certification

Under the powers of the DPA under Section 49 a provision has been added to enable the Government to appoint an appropriate agency for monitoring, testing and certification of hardware and software on computing devices to ensure integrity and trustworthiness and to prevent any malicious insertion that may cause data breach.

24. Codes of Practice

Section 50 has been expanded to include that the authority may approve any code of practice submitted by the associations representing technical services organizations apart from the industry or trade, interest of data principals etc.

Complaint by Data Principal

To remove the uncertainty, under Section 62, it has been provided that an aggrieved data principal may seek compensation by filing an application to the authority.

25. Adjudicating Officer and Penalty determination

A provision has been introduced under Section 64 that the authority shall specify guidelines to the Adjudicators on the determination of the amount of penalty.

26. Appellate Tribunal

Under Section 68 the number of members of the Appellate Tribunal has been expanded to Six and a provision has been made that the eligibility for appointment of the Chair person includes a person who is "qualified to be a judge of the Supreme Court".

As regards the "Member" of the Appellate Tribunal it has been prescribed that he shall be a person who is an expert and has ability, integrity, standing and specialized knowledge with an experience of not less than twenty years.

27. Experts to represent complaints in Appellate Tribunal

Under Section 77, a provision has been inserted to permit "Experts" to represent the appellant apart from the legal practitioners.

28. Liability of Independent and non executive directors

Under section 85, it has been clarified that an independent director or a non executive director may also be held liable for an offence under the Act

(Section 83) unless he proves that the offence was committed without his knowledge and he had exercised all due diligence.

29. Liability of Officer of a Government data fiduciary

In the case of a Government data fiduciary, it has been prescribed under Section 86 that an in house enquiry will be conducted and the person responsible would be proceeded against.

Summary

The New DPA 2021 has tried to address the criticisms that has been made against the earlier draft by some sections of the society. The report has been dissented by a few of the members on specific counts and probably the criticisms will continue. However, the community has waited for a long time for the law to take shape and it would be good if the act is passed at the earliest. Further changes can always be accommodated in the future based on the experience.

We should therefore welcome the new Bill and hope it would usher in a new area of Data Protection and Data Governance in India.

Personal Information Protection - Some Thoughts

M. G. KODANDARAM,

Democracy is primarily oriented towards providing basic human rights in the form of guaranteed fundamental rights to the citizens, a pre-requisite for a happier social living. Freedom to speak and express views with reasonable restrictions is one of the cherished human needs which includes 'Right to information' an inalienable right, recognized by our Constitution and duly asserted by the judiciary. Every individual's desire to keep certain personal information unto oneself and not make it public, deserves to be honoured. The 'Right to Privacy' of an individual is the basic requirement, for preservation of reputation and protecting oneself from the harm caused by others.

In the days of yore, the flow of information, including that of personal matters, was by word of mouth, which had limited reach, and therefore caused lesser harm to individual's reputation, privacy and personal life. As innovations picked up, the use of electronic devices for faster and wider communication, impacted the protection of personal information more than ever. As all the information/data, including the personal data, could reach huge numbers simultaneously, within seconds, that too at a small cost, endangering the Individual's right to life. The protection of the personal information of an individual became more challenging, as all the activities by every entity, including Public Authorities, in every sphere of life are based on digital technology. The commercial exploitation of information/ digital data disrupted the management and regulation of the personal data, which could be abused by fraudsters through illegitimate means. The increase in density of smart phone users around the globe further accelerated and aggravated the criminal activities in the cyber world. The present-day data devices and services have turned out to be disastrous tools as there is no concern for protection of personal information/data of users and are not equipped or positioned to contain the harm caused to personal data.

The rampant deployment of digital technology tools to collect such personal data, without the consent or knowledge of the individual, (rightly termed as '*Principal'* by Honourable Justice Srikrishna in the Personal Data Protection report) has formed a scary situation for the privacy of an individual. When such personal data reaches the dark nets dominated by the outlawed criminals, the damage it could cause to personal life and liberty cannot be guesstimated. Mark my words, that unless stringent laws are in place to regulate the creation and flow of personal data/information, the fraudsters continue to cause irreparable harm to the unprotected and exposed individuals. Measures to be taken for protection of the Personal Data must prevail over commercial exploitation of the data. Privacy protection shall prevail over pecuniary gains. What matters is (wo)man and not the money.

As on date, the Information Technology Act 2000 (IT Act), the primary legislation that regulates the ICT products and the usage of the data in electronic format has limited scope for protection of personal information of individuals by the entities engaged in the data related activities. The need for a personal data protection law in India attained urgency and significance, when the Government started the 'Aadhaar project' aimed at building a database of personal identity and biometric information covering every Indian citizen. If such critical personal data goes unprotected, it will certainly cause huge harm to the individual, the society and the country. In view of the changing circumstances, the Supreme Court of India, in the case of *Justice K.S. Puttaswamy v/s Union of India* [(2015) 8 S.C.C. 735 (India)], passed the historic judgment on 24th August 2017, affirming the constitutional right of a citizen to protect her / his personal data. Further developments include, based on Hon Justice (Retired) B N Srikrishna report, the Authorities are in the process of making suitable Persona Data Protection(PDP) law to address the privacy concerns of the residents.

It is interesting to observe that Right to information Act 2005, mandated with an objective to empower citizen, the right to seek information available with Public Authorities (PA) to promote transparency and accountability in the administration, provides the right to information to any citizen, whereas the former allows an individual to guard her/his personal information from reaching the public domain. Both are guaranteed fundamental rights that deserve equal merit. However, both the rights are not absolute rights as reasonable restrictions could be carved out through proper legislations. The RTI Act predominantly covers and concerns the PAs whereas the PDP Bill encompasses all fiduciaries and processors, including the PAs. The types of data collected by PAs include the personal data, collected in fiduciary capacity or otherwise, as well as non-personal data. Both the legislations have provisions for formation of authorities to oversee the compliance and implementation of the law and procedures in the making.

The Honourable Supreme Court of India in *'Central Public Information officer, Supreme Court of India v/s Subhash Chandra Agarwal',* in Civil Appeal No. 10044 OF 2010 dated 13th November 2019 determined the balance between the right to information guaranteed to all individuals with the principle of confidentiality and privacy. The decision provides much required equilibrium between the 'right to privacy', along with the disclosure of information by PAs, to move towards transparency in governmental services. The bench of the Supreme Court deliberated the among others, the questions of law as to Whether the Section 8(1)(j) exempts the information sought for the public disclosure?

During the deliberation, the Hon'ble judges have clarified the interplay of rights between RTI act and privacy rights. '*The right to privacy though not expressly guaranteed in the Constitution of India is now recognized as a basic fundamental right vide decision of the Constitutional Bench in K.S. Puttaswamy and Another v. Union of India and Others holding that it is an intrinsic part of*

the right to life and liberty guaranteed under Article 21 of the Constitution and recognized under several international treaties, chief among them being Article 12 of the Universal Declaration of Human Rights, 1948, which states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. The judgment recognizes that everyone has a right to the protection of laws against such interference or attack." (Refer para 40.). Observing the interplay with RTI act, the Hone Supreme court states as follows: *" While clause (j) exempts disclosure of two kinds of information that is "personal information" with no relation to public activity or interest and "information" that is exempt from disclosure to prevent unwarranted invasion of privacy, this Court has not underscored, as will be seen below, such distinctiveness and treated personal information to be exempt from disclosure if such disclosure invades on balance the privacy rights, thereby linking the former kind of information with the latter kind."(Refer para 53).* The above observation provides the much-required background of the privacy protection needs in the present-day society. The RTI Act has sufficient safeguards in place to protect the breach of personal information by virtue of section 8(1) (J) exemptions read with Section 11 procedures in respect of third-party information.

It is to be noted that in respect to each activity the Right to Information is not vested absolutely. As per Section 8(1)(j) of RTI Act, information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the individuals' privacy unless the Central Public Information Officer or the State Public Information Officer or the appellate authority as the case may be, is completely satisfied that the larger public interest justifies the disclosure of such information is involved in the matter. The Section 8(1)(j) protects the personal information of an individual against disclosure under RTI Act. The applicants seek many information such as personal detail, income, PAN, source of funds,

partnership detail plan to learn dealership, affidavit etc, which are personal documents and contain a lot of confidential information submitted by third parties that are not to be given as per the stated provision.

Even earlier to Puttaswamy judgement the Hon Supreme Court has been consistent in holding that Courts shall not allow application for disclosure of personal information of employee, if information sought for was not for larger public interest. In Girish Ramchandra Deshpande Vs. Cen. Information Commissioner and Ors, the Supreme Court (order 2012) held that "*Details given by a person in his income-tax returns Details of his service career are his "personal information" and are exempt from disclosure unless larger public interest justifies disclosure of such information*."

In the case of UPSC Vs. R.K. Jain, WP (C)1243/2011 and C.M.No. 2618/2011, the Hon Supreme court on right to privacy had held, "*The right to privacy is implicit in the right to life and liberty guaranteed to the citizen under Article 21. It is a "Right to be let alone". A citizen's right to safeguard the privacy of his own, his family, marriage, his procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent. Whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages*".

As per section 11 of the RTI Act, Where the CPIO or SPIO intends to disclose any information or record on request made under this Act, which relates to and was supplied by a third party, it shall be within five days of the receipt of such request, given a written notice to such third party inviting her/him to make submission in writing or orally regarding whether such information should be disclosed, and such submission shall be kept in view while taking decision regarding the disclosure of such information. In such cases disclosure is allowed only if public interest outweighs the non-disclosure in importance any possible

harm or injury to the third party. If the information seeker requests an information, document or records which are in relation to the third party and it has been treated confidential by that party, then the CPIO or SPIO can serve a notice to a third party as an opportunity given to make representation against the proposed disclosure and after hearing the third party, proceed later for making fair decision as per law.

Further as per the proposed PDP law, all PAs, including the Data Protection Authority (DPA) to be established for overseeing the initiation and implementation of the proposed PDP act, are treated as data fiduciary. (Section 49(*3*) of PDP Bill). In view of the above legal position all PAs are mandated to adhere to the obligations of a fiduciary under the act. From the above legal position, it can be concluded that there is no threat to protection of personal data in the combined PDP-RTI regime, as protection to privacy gets further strengthened. However as there are no definition provisions of certain common terms like ‘personal information’ *"**sensitive personal data**” and* ‘Fiduciary’ in the RTI Act, some ambiguities may set in. To avoid any such lapses, it is pertinent to borrow the stated definitions in the proposed PDP Bill to the RTI act through an amendment. There is an immediate need to enact the much-awaited PDP Bill by the parliament, so that the privacy of the citizen receives the legal protection from abuse.

Moving Towards Personal Data Protection Regime-

Milestones in Information Technology Laws: A Bird's Eye-View

M.G.Kodandaram

The advent of computers and rampant usage of Internet, created volumes of users, popularly called as Netizens, has revolutionised the human existence and their conduct in the present Cyber Society. The traditional paper documents have given way to their electronic equivalents in majority of business and commercial activities as well as in social communications. The individual functioning, commercial transactions and Governance by administration are primarily driven by the digital technology. In today's Cyber-savvy virtual environment, the world has become digitally sophisticated and so also the crimes in cyber space. The Internet in the initial stages, developed primarily as a research and information sharing tool, did not require many regulations as it was used by selective section of persons. As time passed, the usage of cyber gadgets in social communications, e-business, e-commerce, e-governance and IoT etc. has brought huge scores of users into the fold and this in turn has paved way for increase in internet crime also. The changing situation warranted Laws to regulate the usages in cyber space and Cyber laws became essential part of this revolution.

In the preface to 'Digital Economy Report 2021' Mr. António Guterres, Secretary-General United Nations, observes that, "*Data have become a key strategic asset for the creation of both private and social value. How these data are handled will greatly affect our ability to achieve the Sustainable Development Goals. Determining what is the best way forward will be difficult but necessary. Data are multidimensional, and their use has implications not just for trade and economic development but also for human rights, peace and security. Responses are also needed to mitigate the risk of abuse and misuse of data by States, non-State actors or the private sector*". As the number of internet users is ever on the rise, the need for cyber laws and their application have also gathered greater

momentum. The growth of Information Communication Technology (ICT) has propelled the need for vibrant and effective regulatory mechanisms to strengthen the legal infrastructure, crucial to the regulating all aspects of usage. This is no different to India which is one of fast-growing societies adopting digital technology for day to day use in all walks of life. In the following part an attempt is made to deliberate some of the important historical developments and changes in the Indian cyber law scenario.

Cyber space includes computers, networks, software, data storage devices, the internet, websites, emails and even ATM machines and electronic handheld devices such as cell phones, etc. The Cyber law encompasses laws relating to electronic and digital signatures, e-commerce, Cyber security, Cybercrimes, Data protection and privacy in which products of ICT are being used/Involved. The important laws covering the above aspects in India are: *The Information Technology Act, 2000, The Information Technology Amendment Act, 2008, PDP Bill 2019 and non-personal data governance law.* Under the stated heads important milestones in development of law and impact on society are deliberated.

The Information Technology Act, 2000

The United Nations Commission on International Trade Law (UNCITRAL) plays the key role in development of framework in pursuit of its mandate to further the progressive harmonization and modernization of the law in the international trade. UNCITRAL does this by preparing and promoting the use and adoption of legislative and non-legislative instruments in several key areas of commercial law. The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model

Law on Electronic Commerce on International Trade Law. The resolution among others, recommended that all states may consider the said Model Law while revising/enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations.

The Information Technology Act, 2000, (also known as IT Act 2000), was notified on 17th October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. Laws apply to the whole of India. The legislative history of ITA 2000 starts with the draft of E-Commerce Act 1998 based on the UNCITRAL Model law on E-Commerce. The Act of 2000 provided a legal framework for electronic governance by giving recognition to electronic records and digital signatures. ITA 2000 had provisions of "Data Protection" under Section 43 which provided for compensation to a victim of "Data Loss" due to unauthorized access. This provision could be extended to the victim who had lost personal data, and therefore acted as a legal remedy against personal data theft also.

The Government had also introduced a "Privacy" bill in 2005. The Indian citizens missed the opportunity of having a Privacy Act much before the Supreme Court could sit in judgement of Privacy issues in the use of Aadhaar. This bill of 2005 was allowed to be lapsed, but fortunately the Honourable the Supreme Court in the famous "Justice (Retd) Puttaswamy Judgement" held that the Privacy of an individual is a fundamental Right enshrined in the Indian constitution" opened the doors to the introduction of personal data protection bill,2019 in the Indian parliament.

The Information Technology Amendment Act, 2008

A major amendment, ITA Amendment Bill 2008 was made in 2008. It was signed into an Act by the President on 5th February 2009 and was notified for implementation with effect from October 27, 2009. With the passage of the

Amendment Act 2008, the legislation reached a significant stage in the development of Cyber Laws in India. The amended act defined cybercrimes and prescribed penalties for them along with technological neutral definition for e-signatures. Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism. The offences and the corresponding punishment have been a major part of the enactment.

The Act also amended various sections of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies. The Rules notified included, under Sections 43A, on the Sensitive Personal information, Under Section 79 on the intermediaries, Cyber Cafe Regulations (also under Sec 79) and Section 6A (Electronic Service Delivery).

The amended Act gave a concrete shape to the “Data Protection law” in India with the introduction of Section 43A as a measure of fixing accountability to body corporates for protection of sensitive personal information and Section 72 A for personal information. Sections like 67C, 70B, 69,69A,69B all supplemented the either supplemented the personal data protection or added exemptions through powers to different authorities. The GOI provided some clarifications on Sec 43A rules issued on 11th April 2011 essentially indicating that the responsibility for obtaining "Consent" would be on the body corporate that deals with the persons whose information is being collected. Similarly, it was clarified that under Section 79, the interpretation of objectionable content would be left to the Courts. During the intervening period, the technology related challenges were confronted by the Judiciary at many a time and one of the important is related to Constitutional validity of Section 66A regarding penalization of offensive

messages sent through a communication device being violative of fundamental right to freedom of speech.

Constitutional validity of Section 66A

After several arrests made by Police for posting of objectionable contents on social media, the Supreme Court considered the constitutional validity of Section 66A regarding whether the said provision violated the principles of Freedom of Speech guaranteed by the Indian Constitution. The inappropriate application of law due to deficient understanding of technology arose when Section 66A was scrapped by the honorable Supreme Court by holding that "Punishing the act of sending an offensive message through e-mail or SMS message" violated the Fundamental Right to Freedom of Expression" guaranteed under the constitution. The Supreme Court concluded that Section 66A was violative of the Constitution under Article 19(1). The technology challenge in this issue which the Court failed to resolve was to determine whether a socially accessible Publication available to general public in applications like face book, twitter etc., and searchable in a search engine is the same as E-mail messages / SMS messages which are used for communication between known person, and not accessible to general public. Court interpreted that there is no difference between a Publicly available information and a Confidential private message which lead to treating the said provisions as ultra vires.

Related developments

The current usage of internet is no longer limited to the realm of computer specialists alone. It is everywhere, 24X7 and for every individual has been using them world over without any barrier of physical boundary or political sovereignty. The Indian legislature has from time to time, made several

amendments to the IPC, to specifically cover cyber-crimes. Some of the important amendments are as follows:

a. in sections 118 and 119 of the IPC (that deal with the concealment of a design to commit an offence punishable with death or imprisonment for life and a public servant concealing a design to commit an offence which it is his duty to prevent, respectively), the words "*voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design*" were inserted before the words "*to commit such offence or makes any representation which he knows to be false respecting such design*";

b. In section 464 of the IPC (which penalises the making of a false document), the phrase "digital signature" was replaced with the phrase "electronic signature" in all places. The section was also amended to include the making of false electronic records and affixing electronic signatures under its ambit and the phrase "affixing electronic signature" was given the same meaning as it has under the IT Act;

c. "Electronic record" was included within the ambit of sections 164, 172, 173, 175, 192, 204, 463, 466, 468, 469, 470, 471, 474 and 476 of the IPC that earlier only provided for "documents", "books", "paper", "writing" or "records", as the case may be;

d. in section 466 of the IPC (which deals with forgery of court records or of public registers), the term "register" was defined to include any list, data or record of any entries maintained in an "electronic form", as defined in section 2(1) (r) of the IT Act[10]; and

e. a new section 354D was inserted in the IPC that introduces the offence of cyber stalking.

National Policy on Information Technology 2012

In additional to the developments in cyber laws, the Union Cabinet in September 2012 approved and announced the National Policy on Information Technology 2012. The Policy aimed at leveraging Information & Communication Technology (ICT) to address the country's economic and developmental challenges. The vision of the Policy was "to strengthen and enhance India's position as the Global IT hub and to use IT and cyber space as an engine for rapid, inclusive and substantial growth in the national economy". The Policy envisaged, among other objectives like, to increase revenues of IT and ITES Industry; to expand exports; to create a pool of 10 million additional skilled manpower; to gain significant global market-share in emerging technologies and Services; to encourage adoption of ICTs in key economic and strategic sectors to improve their competitiveness and productivity; to enhance transparency, accountability, efficiency, reliability and decentralization in Government and in particular, in delivery of public services; to leverage ICT for key Social Sector initiatives like Education, Health, Rural Development and Financial Services to promote equity and quality; to strengthen the Regulatory and Security Framework for ensuring a Secure and legally compliant Cyberspace ecosystem. There was no precise mention of protection of personal data as a factor in the development of digital realm.

Personal data and privacy protection in India

To protect oneself from unwarranted interference in life, Privacy of certain personal information is essential as it gives one the required space to be comfortable within self and people around in the society. The 'Right to Privacy' of an individual is the basic requirement for preservation of reputation and for protection of oneself from the harm caused by others. The privacy of an individual as a right has become a matter of concern as more and more entities are using

data pertaining to individual's life and activities, for illegitimate purposes and money-making. The rampant deployment of digital technology tools to collect such data of a person on some pretext and commercially exploit the same for profit, without the consent or knowledge of the subject, has created a scary situation to the individual. Privacy is the foundation upon which many other human rights are built. As on date India does not have a dedicated law for personal data protection and enforcement of privacy rights. The ITA 2000, enacted with an objective to promote e-commerce, included elementary provisions relating to Cyber Crime. The ITA 2000 was amended in 2008, in which more aspects relating to personal data protection were added.

The Section 43A contained issues pertaining to matters like Data Protection, definition of sensitive personal information, reasonable security practice and related issues. The said provision provides for compensation to the individual/victim in the event of any entity/person is negligent in using 'Reasonable Security Practices and Procedures' (RSPP) in protecting 'Sensitive Personal Data and Information' (SPDI) and this results in a wrongful gain or wrongful loss to that individual. The Section 79 had rules defining the responsibilities of an intermediary to protect privacy of individuals whose personal information is collected by the organization and Section 72A renders the personal data breach a punishable offence. The Section 67A related to data retention and sections 69/69A/69B/70B contained provisions relating to powers of agencies for surveillance etc. Therefore, we can conclude that the amended law had most of the features of a data protection in theory, but with no exclusive Data Protection Authority in place for implementation of the stated provisions.

However, the IT Act 2000/8 provides for appointment of an Adjudication Authority to decide whether a person has contravened the IT Act, or its rules made thereof. In instances where the claim of injury or damage to the individual does

not exceed 50 million rupees, the Secretary to the Ministry of Information Technology (Meity) in each State has been appointed as the Adjudicating officer. The adjudication process mandated for obtaining fair relief to the victims failed miserably due to negligence and poor performance of the adjudicators. The plight of the victims has gone unattended for long as little attention is given by the Ministry concerned towards refining the system. In fact, the victims have stopped using this route, as it never gave them any timely relief. From the existing poor practices, we can certainly conclude that the legal remedy provided for protection of personal data in India has totally failed.

Poor performance of cyber tribunal

In pursuance to section 48 of IT Act, the Cyber Appellate Tribunal (CyAT) was established as an important judicial authority, is guided by the principles of natural justice, with the same powers as are vested in a civil court under the Code of Civil Procedure, 1908. The CyAT was the appeal Court for all Adjudicators (One in each State and Union Territory) and the Controller of Certifying Authorities, started operating from 2006. But from the beginning until merging with TDSAT, it remained either a poor performer or non-performer, the reasons for which are not worth the deliberations. The CyAT has been merged with Telecom Disputes Settlement and Appellate Tribunal (TDSAT) by making necessary legal amendments to ITA 2000/8 during 2018. As on day the TDSAT becomes the appellate authority after the Adjudication of a Cyber dispute under ITA 2000/8, but the activities of this tribunal also have remained poor. "In the absence of an effective body, which can provide recourse in cyber fraud cases, most victims head either for their local cyber-crime police cell or decide to go to a consumer forum or their local district or High Court. Most of these options are either time-consuming or logistical nightmares," Na Vijayashankar, the cyber

expert opines[i1]. So the plight of victims of personal data breaches remain unattended even to this day.

Proposed Privacy and personal data realm

The historic judgment of a Nine Member bench of Supreme Court on Privacy (Puttaswamy Judgement) declared that the "Privacy to be a fundamental right" under the Indian Constitution. Since this judgment on 24th August 2017, there was a clamour for "Privacy Laws in India" with specific reference to laws related to Information Privacy. In 2012, Justice K.S. Puttaswamy (Retired) filed a petition in the Supreme Court of India challenging the constitutionality of 'Aadhaar project' on the ground that it violates the right to privacy of an individual. The Aadhar data, among others, involved privacy information of all Indian citizens, which could be misused by any person who has access to such crucial information. As it was a question of law having impact and importance on life and liberty of a person, the same was referred to a five-judge bench, which thereafter, got referred to an even larger bench of nine judges, to pronounce commandingly on the status of the right to privacy.

The Supreme Court in the above case viz., Justice K.S. Puttaswamy v/s Union of India [(2015) 8 S.C.C. 735 (India)], affirmed the constitutional right of a citizen to protect her/his privacy. The Apex Court held that the privacy of a person is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual's liberty. Further the individual's dignity is cited as the basis for extending it the status for it as a fundamental right. The Article 21 mandates that, *"No person shall be deprived of his life or personal liberty except in according to procedure established by law".* Further, the

[1] https://www.sundayguardianlive.com/news/12014-body-meant-resolve-cases-cyber-fraud-near-defunct

Supreme Court clarified that the right to privacy is not an "absolute right" but may be subjected to reasonable restrictions in certain situations. For using such restrictions (i) there must be existence of a genuine state interest ;(ii) such restriction should be proportionate to the interest;(iii) and it shall be through valid legislations.

During the proceedings of the said case, the Indian government set up an expert committee, headed by Justice (Rtd) B N Srikrishna, to devise a data protection legal framework. After public consultations, the committee submitted its report along with a draft Personal Data Protection Bill 2018. The Union Government, after certain modifications, introduced the 'Personal Data Protection (PDP) Bill, 2019' in the Lok Sabha on December 11, 2019. The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority of India for the same. The Bill aims to: to provide for protection of the privacy of individuals relating to their personal data; specify the flow and usage of personal data; create a relationship of trust between persons and entities processing the personal data; protect the fundamental rights of individuals whose personal data are processed; to create a framework for organizational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data; remedies for unauthorized and harmful processing and to establish a Data Protection Authority of India for the said purposes and for matters connected there with or incidental thereto. As of now the Bill is being analyzed by a new Joint Parliamentary Committee (JPC) in consultation with experts and stakeholders and is process of finalization of the report.

Non-personal data (NPD) governance

In the meanwhile, the The Ministry of Electronics & Information Technology (MeitY) in 2019 formed a committee to make recommendations on the regulation of non-personal data (NPD) for the Government's consideration. The Stated goals

for the committee were, (i) To study various issues relating to Non-Personal Data. (ii) To make specific suggestions for consideration of the Central Government on regulation of Non-Personal Data. The expert committee headed by Mr. Kris Gopalakrishnan[2] released its report on non-personal data governance on 12 July 2020. The report on Non-Personal Data Governance (NPDG) contained recommendations for identifying "Data Business", setting up a marketplace for "Data Trading", recognizing Non-Personal Data ownership as "Anonymized PD"," Community NPD" "Private NPD" and "Public NPD" etc. The goals of the Non-Personal Data Governance Framework (NPDF) include creating a framework to unlock the economic, social and public value from using data; creating incentives for innovation and new products, services and startups in India; and addressing privacy concerns, including from re-identification of anonymized data. After receiving the feedbacks from concerned, the Committee of Experts issued a revised report[3] on the Non-Personal Data Governance Framework for India on December 16, 2020. The Committee observed that non-personal data should be regulated to: (i) enable a data-sharing framework to tap the economic, social, and public value of such data, and (ii) address concerns of harm arising from the use of such data. The NPD Governance Act which Kris Gopalakrishnan proposed therefore can focus entirely on the monetization of the NPD. The new governance framework is stated to be creating delay in passing of the PDP legislation.

Commercial interest stalling the privacy bill?

There are moves to merge the Non-Personal Data governance measures with privacy laws as tabled through PDP Bill 2019 to create common authority which

[2] https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf
[3] https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

is a move in wrong direction. By resorting to such a move, the privacy rights of individual go unheard again as the authority will be filled up with corporate commercial interests as is happening in the IT Act 2000/8 regime. Added to this, as the objective of both proposed laws are entirely different, merging them under one roof will result in downplaying with the fundamental rights of the citizen as held by the Apex court.

As per the bill placed before parliament the Section 43A of ITA 2000/8, will be deleted and accordingly the responsibilities presently exercised by the Adjudicator gets shifted to the proposed Data Protection Authority. In view of the exclusive Authority is going to be formed to resolve the privacy issues, the victims who normally are individuals, may hope to receive a faster and fair treatment in obtaining damages for the caused harms.

The objective of PDP is primarily to protect the Privacy rights of the individuals whereas the NPDG intends at providing a governance mechanism suitable for monetization to the commercial entities in respect of non-commercial data. Any Breach of Personal data by a fiduciary affects the interest of the Individuals, who should be placed in a comfortable environment to seek the remedy for violations of the of the right to privacy. As against this, any breach in non-personal data impacts the Companies who are better placed than the individuals to seek redressal. Further the personal data breach has consequences like subjective issues like loss of reputation in addition to monetary loss to an individual. It should be noted here that the individual is seeking relief as it is an unalienable right assured by the Constitution. The complaints will be normally against corporate entities who have breached privacy norms. As against this, the non-personal data breach, which are not treated as violations of the fundamental rights, has only commercial interests and consequences. Therefore, the laws intended for different purposes shall not be stringed together to create an

uninvited eco-system, where justice to individuals will be a mirage again. If done the privacy aspect of individual will certainly takes heavier beating as well as it results in diluting the fundamental rights guaranteed under the constitution. '*If the JPC takes the bait, it could be falling into a trap and it will find it difficult to get the PDPB 2019 passed or avoiding operational conflicts after it is passed which could delay its the notification of operating rules*' opines Naavi[4], the veteran Cyber Law specialist. There will be no one to listen to the individual's cry of privacy as the corporates' heavy bugles always steal the show as usual.

It is a pertinent to mention here that the same corporates are adhering to stricter privacy regimes in their working places in the developed and privacy law protected nations, without any remorse. At the same time, they do not want the Indian exclusive privacy law to take suitable shape enabling the rights of the individuals served as desired by the Apex court which is surprising.

Conclusion

In view of the above facts, it is expected that the proposed privacy law and administration shall be in the exclusive domain where every Indian citizen can access, with simple procedures in place and obtain timely reliefs for the violations/breach of her/his fundamental rights as guaranteed in the Constitution of India. Therefore, the appropriate and the fair approach to be followed in making of the laws for protection of personal data and privacy rights of the citizen must be **e**xclusive *sui -generis* measures to protect personal data protection as inalienable rights as recommended by the Srikrishna commission and as being followed by many countries around the world.

[4] https://www.naavi.org/wp/a-challenge-accepted-if-pdpb-is-converted-into-dpb/

Jnaana Vardhini

FDPPI conducts periodical webinars under the Jnaana Vardhini series as its effort to continue spreading of relevant knowledge to its members. These sessions are counted for the CPE points mandatory for the certified persons.
Some of the sessions are available as video links here.

https://youtu.be/Jf4waWpem8c : Role of AI in Cyber Security
https://youtu.be/Dgxa3wTuKL4 : Crowd Funding
https://youtu.be/ZUJZeEkXv5w: Data Valuation
All sessions of IDPS 2021 are available through the link:
https://fdppi.in/wp/idps2021-videos/

Q & A

Here are a few questions that FDPPI has come across recently and some viewpoints from FDPPI team:

Q 1: Some countries consider the age of minority as 16 years or even less while India considers it as 18. Should India also reduce the age of minority?

A: The objective of DPA 2021 or similar laws is to "Protect the data principal/subject from harm". Reducing the age of minority is a "Convenience Feature" as services would be made available without parental consent. This could be the objective of a law to promote use of Internet services and not the objective of a Privacy or Data Protection law. Hence reduction of the age of minority for mandatory parental consent is counter to the objective of the law.

Q2: Recently the EDPS passed an order to delete accumulated surveillance data from Europol records. Does it improve the Privacy administration?

A: Deleting the information as proposed may erase some information vital to the security of the state. This could adversely affect the right to privacy of the individuals whose information is involved. However, instead of deletion, efforts to de-identify and introduce an element of human intervention for its use through an escalation process could have been ordered instead of the order to delete.

Q3: What are the responsibilities of the Cloud service providers during a data breach?

A: A Cloud service provider is often the "Data Storage Agent" and therefore a "Data Processor". He is responsible for the security. Ideally the data owner should store only encrypted data so that any data leak from the cloud should not immediately cause harm to the data principals. But having a proper security system to manage the access of authorised persons is part of the minimal security

to be provided. Hence measures to identify abuse of access through multiple factor authentication and adaptive authentication measures need to be adopted. Failure may be considered as “Negligence” and drag them into the liability chain.