JULY 2020

ISSUE BRIEF

KNOWLEDGE WEB-SERIES

SESSION IV

DIGITAL ACCELERATION, PRIVACY AND DATA PROTECTION

Jointly Organised by

HAMMURABI & SOLOMON PARTNERS

INDIA STRATEGY GROUP

SUMMARY

On 25th July 2020, Hammurabi & Solomon Partners & India Strategy Group jointly convened a knowledge web series ("KWS") to discuss the issue of what do businesses need to factor-in with regard to privacy & data protection laws in order to mitigate risk exposure on the avalanche of information pushed into the digital space post the advent of Covid 19. This report tries to capture the discussions with the distinguished speakers and to highlight the dos and don'ts in this regard.

The KWS was convened with the aim to discuss, deliberate, and analyze implications of recent legal developments – legislative, regulatory/policy as well as judicial pronouncements.

DISTINGUISHED SPEAKERS

Hon'ble Justice. B. N. Srikrishn

Former Judge,
Supreme Court of India

Dr. Manoj Kumar

Founder & Managing Partner,
Hammurabi & Solomon Partners

Ms. Smriti Subramanian

General Counsel,
Snapdeal

Mr. Maxime D'Angelo Petrucci

Dentons,
Paris TMT Group

Mr. Kumar Ankit

Head – Legal & Regulatory – Iron Ore, Steel & Ports,
Vedanta Limited

Mr. Arjun Jayakumar

Associate Fellow - Cyber, Tech & Media, Observer Research Foundation

KEY POINTS

Introduction

The discussion around the importance of Data privacy and protection has been triggered by the large scaletransition of businesses and transactions from the non-digital space to the digital space overnight due to the pandemic. The stakeholders involved are primarily consumers or people at large or businesses corporate entities at large. A huge section of the Indian businesses have suddenly been compelled to work and funcrtion predominantly in the digital space, and what has made it even more difficult and unique in our case is that the law on the subject is itself in the making and evolving. The Personal Data Protection Bill is before the parliament and in fact before the joint parliamentary committee at present. Right to privacy is recognized fundamental right and it is therefore not only necessary to safeguard and protect personal data as an essential facet of informational privacy but also to prevent misuse of personal data as such. While the laws around data protection and privacy have become effective in many jurisdictions, absence of a similar law in India has not been helping businesses operating in multiple jurisdiction in being above board on compliance with data protection laws elsewhere.

Since privacy and personal data protection is rapidly becoming a competitive advantage in the digital age, redesigning policies to make protection of personal data regime more transparent is likely to significantly benefit businesses.

Evolution of data protection in India

The establishment of the Unique Identification Authority of India (UIDAI) by the Indian Government for providing a unique ID, i.e Aadhaar brought the need for personal data protection in sharp focus.

In this regard, Hon'ble Supreme Court of India has held that the Right to Privacy is a Fundamental Right under Article 21 of the Constitution of India and directed a law to be put in place. The Central Government thereafter constituted a committee seeking recommendations for an appropriate data protection law led by Mr.(Justice) B.N.Srikrishna, former Judge, Supreme Court of India. The B.N.Srikrishna Committee took various inputs from the stakeholders of this country and abroad, academicians, lawyers, professors of law, and also from all various people who are interested in the subject pursuant to which a report and draft Bill was subsequently submitted to the Central Government. The draft Bill submitted by the B.N.Srikrishna Committee however underwent modifications by the relevant department and in 2019, a modified version of the Bill was formulated and placed before the Parliament.

However, before enacting this law, the Parliament must make sure that it is citizen centric. The primary purpose of the law must be to protect the rights of the citizens.

It is ultimately the question of how nations evolve and adapt themselves. Every nation is clear in theory but the problem area has been the understanding of 'sovereignty' and its limits from the 17th to today's 21st century. Today 'soverenity' is intended for a particular region and purpose. Therefore the challenges around divergent regimes and inconsistencies on data protection regimes could be solved on version principles of reciprocity and inclusive law making.

It is also therefore necessary to enable all affected stakeholders to plug-into the law making process. Taking the example of the banking industry, they have a body called Indian Banking Association which debates all the laws extensively, and then persuades the RBI and the government to introduce the law. Other industries must take a cue from the banking industry, and start following this practice.

In the proposed data protection Bill, since the parliament does not have the time and bandwith, the Data Protection Authorities (DPA) will have to discuss these issues. The DPA must discuss with stakeholders about all these problems and come to a solution. The first action item on the list is to appoint a data protection authority in the immediate future.

Rationale behind consumer courts addressing issues of 'right to privacy'

As discussed, privacy has been held to be a fundamental right and in this regard the Constitution of India has empowered High Courts and Supreme Court with the jurisdiction to remedy violations of fundamental rights of citizens. Lower Courts such as District Courts do not have such authority.

A Consumer court at a lower level will be headed by a Civil Judge at a Junior Division or a Magistrate of the First Class. However, the recent amendments to the Consumer protection law includes issues of data protection within the ambit of jurisdiction of a consumer Court.

The speakers expressed concern that there is a high probability of consumer court presiding officers/judges lacking sufficient familiarity and expertise on data protection laws. For example, if a person comes forward with a complaint that his data has been breached, he/she must be compensated. However, it is extremely difficult to understand on what level such compensation is to be granted as well as quanum of compensation Since data can be breached in many ways such as hacking, stealing personality etc. and one would need to navigate through the applicable jurisprudence and laws to be able to handle such claims. Therefore, it is improper to give this responsibility to the consumer court in the absence of domain expertise or understanding of the data protection laws.

Hence, it is also important to establish a data protection body and have experts at the earliest. They will come out with effective solutions which the data protection authority can ultimately debate and implement.

Decoding non-personal data

The definition of NPD is any set of data which does not contain personally identifiable information. This means that no individual or living person can be identified by looking at such data.

Non-Personal Data (NPD) has a much wider scope and the B.N.Srikrishna Committee did not want to get into the intricacies of the same and hence had not dealt with the same and primarily focused only on personal data..

However, in the proposed Personal Data Protection Bill, non-personal data was introduced.

The Hon'ble Supreme Court has never said that NPD is a fundamental right. Therefore the amount of protection for personal data is much higher than the NPD.

This is a debate between fundamental and non-fundamental rights. For example, right to vote is not a fundamental right therefore, can be modified by the government. However, the right to life is a fundamental right. Similarly, protection of personal data is a fundamental right coming from article 21 of the Constitution. Therefore, there could be a different standard for the NPD.

NPD would include IPR. However, there are various laws to protect IPR already. Financial data like the company's budget is an example of non-personal data. If someone accesses this data unauthorized, then such person can be charged by the SEBI for insider trading.

Another aspect of data protection debate is the non-personal data and the use of this data to derive economic value. The grounds under which non-personal data can be demanded by the government needs to be far more nuanced. It is not enough to say that we can access non-personal data for enabling service delivery or for policy making processes. Businesses store personal and non-personal data, and have different levels of protection depending on the purpose for storing data. If one does not have clarity on the grounds under which the non-personal and anonymous data is demanded, it can have a lot of compliance burdens for the business.

Another feedback was that anonymization is not exactly a one-way process. It is not like data, once anonymous it cannot be reversed. This has been mentioned in the first edition of the Data Protection Bill. The fact that it doesn't recognize anonymization of data is not a reversible process. The fact that it doesn't count that anonymization data can also be reidentified. If one is going to say that we can access the anonymous data then we must prescribe the standards for anonymization which sets a baseline and ensures that data is protected to an extent. Section 91 of the current bill (PDP, 2019) talks about accessing non- personal data. It defines non- personal data as data that is not personal which is a very broad definition and is not nuanced enough. This could even capture instances of proprietary knowledge like trade secrets, IPR etc. Therefore, a provision like this can encroach such rights and capture within the ambit of non-personal data and business would have no option than to let go off such data which can be harmful.

Further, additional safeguards for secondary uses of non-personal data is a challenge that has been raised throughout. Collecting data for other purposes than the original purpose, needs a system of checks and balances so that there is no encroachment of constitutional rights. Such a system is absent in the PDP bill 2019. The recent report on how to monetize non-personal data and to generate economic value, address a lot of concerns. It does define the grounds for access than what was done in the PDP bill. Also, it suggests that that anonymization standards must be prescribed so that it is not easily reversible. At the same time, we should remain aware that these are just recommendations. When the final legislation comes into force, the government should ideally take into account the recommendations of the committee and the various stakeholders.

The Challenges

The first and foremost challenge with regard to the PDP bill is the timeframe within which the bill is going to be implemented.

The second challenge is the manner in which consent is going to be obtained. This factor is presently being considered by the Joint Parliamentary Committee.

This is not a switch on and off approach, recording such consent would require a huge amount of infrastructure requirement and at the same time retaining them or right to erasure as per article 17 of the GDPR, that is not going to be present, per say in the PDP bill. This is going to be definitely one of the major concerns coming through in the bill.

The third challenge is regarding the overlap between personal data and generic data sets. This might create a situation where multiple people will look into a similar set of data. Very few people only have access to what exactly a system does.

Therefore, education is definitely going to be very important in terms of implementation of the PDP bill across all cadres.

Further, personal data as well as NPD is available to the government without the consent of the user. Hence, it is important to have a law to define the same.

If you want to infringe a fundamental right, you should have a competent legislative enactment declaring the objective and the rationale between the terms and objective to be achieved.

The primary question is what is the law under which the Aarogya Setu application is operating, the authority which issued the use of the application which is collecting personal data which is one's fundamental right and secondly, the app primarily collects personal data from user cellphones and cellphones are an immense repository of personal data of users and sometimes, of a user's contacts and acquaintances.

Compliance Challenges for E-Commerce companies

Every digital business, includes digital payments, e-commerce, social media, and other types of digital businesses that are operating at present.

One of the challenges with regard to the IT Act is that it doesn't recognize the technological advancements and variety of technological changes that has happened over the last 7-8 years, though some revisions will be included in the IT act as well.

As an industry, specifically e-commerce looking at the PDP bill, it is realized it's more based on regulation of data usage and data collection. This means that all the enterprises (specifically talking about e-commerce) will have to focus more on compliances and regulated environment with respect to collection and usage of data.

The biggest fear many of the e-commerce firms have is the possible requirement to change business models overnight, which would drastically increase costs as well as disrupt businesses.

E-commerce firms bore the brunt of overnight changes when the government changed the foreign direct investment rules.

There are huge challenges which E-commerce actually handles including millions of users, millions of transactions per day and having vast consent management which is technically possible but extremely hard to execute.

This implies that additional investment in collection and ensuring record consents. This is based on a very old principle, perhaps when there were few enterprises which had data on limited mainframe servers and it was easy to identify where the information was and on which server.

However, in the current times, one is looking at global servers, data sitting in different kinds of systems making it quite difficult to identify. Also, looking at principles like data anonymization where there is actually less or limited technology today to have an anonymization and there is no 100% guarantee on anonymization.

As an industry, to cope up with some of those requirements which are coming up in the PDP bill, it's interesting and at the same time worrisome. This is due to the fact that the bill actually sets out principles and needs a lot for Data Protection Authorities (DPA) to decide and there is no actual reasonable test to check the balance of DPA's powers. There are no set of guidelines of compliance requirements and reasonability of the same under the PDP Bill.

Apart from handling every other complexity in the business and the evolving laws, handling a compliance which we aren't aware of is extremely difficult. As our E-com companies prepare towards compliance with PDP, they are also certain that they would have to do extensive investment in data management, automation, and security measures.

The only hope is that it's going to play a more preventive and guidance role in terms of engaging with industries, stakeholders by framing specific guidelines.

E-com companies hope that industries get time to set up their compliances as we move forward. Also, the problem gets aggravated when data collection and processing are done by different agencies, in which case, each fiduciary will have to take consent at every step of the operation. Such ambiguities lead to unnecessary compliance burden on companies and hinders the ease of doing business.

One concern as an industry stakeholder is perhaps the consequence of the regulations in terms of growth of the new businesses. For example, the restrictions on the use of data. That almost cripples the AI or Big Data or the development of new businesses or sharing the data with the government.

There needs to be a lot of thought in balancing innovation with the privacy rights of individuals. Such a balance is very important in this vastly growing industry. It also has an impact on smaller businesses like AWS services for example and also mirroring of data in India.

Are we actually making it very difficult for MSMEs which have access to much cheaper servers because we have a service that is similar to AWS? Today with the kind of use restrictions that are present, there is a confusion in understanding the role of data or the difference between collection and processing.

There are huge challenges for companies providing services like SAAS for example. The professionals who help the government to come up with guidelines, need to understand the technology and understand the implication of these laws on the technology and the industry front.

Legality of location tracking applications

It is quite painful to see that a lot of applications that are used in our daily life have been collecting location data. For instance, Flashlight application collects location data for an application that merely provides simple flash. This delves into the principle of purpose limitation which states that only the data that is necessary for a specified purpose should be collected and that the customer must be informed and explicitly be aware that the data is collected for a particular purpose and such data will be available with certain people only.

It is definitely a concern that a lot more information is being collected than what is necessary from the users. The DPA, once it comes into force, will cover these principles which provide a framework against the companies which collect such information than necessary and shall be held accountable. This will be a positive step that will solve the problem to a certain extent.

Has the GDPR been implemented effectively in Europe?

Most people agree that GDPR has been the biggest legislation relating to data protection in the past 20 years. Before GDPR there was already a European legislation on data protection but it was not very well known.

Now the subject of data protection is taken extremely seriously not only because of very high sanctions of GDPR, but having put many political agendas to shed lights on data protection. In my opinion, GDPR is not really a revolution but more of an evolution of the past directive that existed in Europe.

Companies that have followed compliance before the GDPR shouldn't have had so many difficulties in compiling with the GDPR. However, all the other companies that discovered data protection with the GDPR faced an enormous amount of work to bring their practices in compliance with the GDPR. A lot of work has been done by European companies and companies outside Europe in the past 2 years with regard to compliance.

The authorities tend to consider that GDPR has been a success. Now that being said, authorities, practitioners and the companies are well aware of limits today that we see with the GDPR. The one limitation of GDPR is the Bureaucratic aspect of the GDPR.

GDPR requires a lot of paperwork, too many resources and the effect is that some companies simply abandon the same. In the next few years, one of the most important challenges would be to find the balance between actually protecting people, giving them information and forcing their rights and on the other hand being realistic on what companies can do. Emphasis should be laid on trying to prioritize on imposing things and not to make GDPR a kind of bureaucratic compliance exercise.

GDPR : Use of encryption technology v. need for transparency and access to data

GDPR encryption is one among the many possible security measures that the company has to take in order to secure data. There is no preference for encryption compared to other security measures in the GDPR. Encryption can be terribly affected to secure data as a means to show to the authorities that you are taking the security of personal data very seriously.

However, from the positions taken by protection authorities in Europe, it is clear that encryption does not necessarily mean that it is the golden- standard for security. It is not because you encrypt data that systematically considers the data anonymized. It is a mistake on the part of the companies to buy an encryption solution to deploy it across all systems. It's a good tool, but not the perfect tool.

Regulation of NPD in Europe

In the EU, people are well aware regarding the importance of Non-Personal Data. Very often, that data sets in companies and organizations, comprise of both personal and non-personal data.

In most cases, there is a mix of personal and non-personal data. In Europe, in 2018, a regulation was enacted regarding the free flow and approach to non- personal data. This data is important for companies, for business development, and therefore has to freely flow between European countries.

The principle is that EU member states cannot restrict legitimately non- personal data to flow from one to another EU country. The idea of the commission was that this regulation would complete the GDPR. Company sets have personal data and Non- Personal Data. The problem with Non- Personal Data is that companies also need to know what they are dealing with, the way to deal with copyrighted information, commercial secrecy is not the same if it's only technical.

The complexity is that one has to put things in a box and then legally check what is subject to Personal Data protection, subject to commercial secrecy etc. The current situation in the EU is that there is a free flow of personal data. Handling this data at the local level must ensure that the local laws are complied with.

EU-US privacy shield

The European Court of justice in its judgment of 16th July 2020 invalidated the EU-US privacy shield primarily because it did not accord sufficient protection to individuals whose personal data has been possessed.

Many people in the legal community felt that the life of the EU-US privacy shield would be short.

The European Court of justice simply stated in its decision that standard contractual clauses are a contract, they don't bind foreign authorities which may access personal data and so it is the role of the company sending the data and the entity receiving the data to ensure that European standards can be complied with the country where the data is being transferred.

TAKEAWAYS

Conclusion

The Personal Data Protection Bill discusses things related to electronic format and also assures to protect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for overseeing processing activities.

Currently, India has a population of approximately 1.3 Billion, and 30% use mobile phones. At the same time, people belonging to rural areas have now become familiar with use of the internet. The number of people joining is high. However, they are ignorant about the laws.

Education and advocacy regarding privacy should start from a very young age. In such a manner, an entire generation may be educated. Until now, only electronic documents or inputs are forming a part and parcel of the data protection laws in terms of IT Laws.

The existing IT laws are silent on the way manual data is being stored because even that has personal data. One important distinction between natural resources and data is after a certain point when data becomes more, it tends to become a part of the community. There is no particular individual who can be identified from this and the ownership is difficult to find out. There are few companies which are monopolistic in nature due to which they can use data at a faster pace. Indian business environment is not designed in such a way where everyone can adhere to similar kinds of privacy or in terms of architecture stands.

There's a huge difference in the way Indian MNCs and foreign MNCs work. The economic dimension of the data and the suitable taxonomy what we call are prominent in this big data which is happening in the country right now. It is difficult to segregate between personal and non-personal data which may lead to troubles in future.

The Speakers concur that it requires and will require a lot of education, as from level zero one is being catapulted to the hundred level. We do not understand the meaning of data, however at present we almost have a regulation governing the same.

Software or encryption data leakage is not necessary from a tech point of view, it can be from human actions also, security has to be plugged in at this end, from tech end and finally there would be infinite confusion on the same.

While PDP has not even come into effect, other institutions such as RBI and TRAI have already shot the gun. The RBI has notified that all financial data must be in India and TRAI has declared that all mobile transaction data must be only in India.

The biggest challenge would be subjecting data to the right jurisdiction and oversight which is partly a technological challenge and legal challenge as well.

Click below to watch the KWS session

https://www.youtube.com/watch?v=qoT6Lk0usdA

Click below to listen the KWS session podcast

https://anchor.fm/hammurabi-solomon

ABOUT US

Hammurabi & Solomon Partners was founded in the early 2001 and is ranked amongst the top #15 law firms in India. Our journey has been marked by stellar growth and recognition over the past 2 decades with over 16 partners handpicked from the top of their fields. Paving our way into the Indian legal landscape we believe in providing complete client satisfaction with a result driven approach.

We have always aimed at being the change-maker for a newer India and the world around us. With our portfolio of services - law, public policy, regulation and justice converge to enable solutions to our client needs within the legal framework to operate in India with ease and predictability.

Our main aim is to provide world-class legal services with a unique client-centric approach. We aim at providing the utmost quality and result-oriented solutions with our out of the box thinking and teamwork. We focus on being very approachable and highly reliable legal advice with a practical and relevant approach, we tailor solutions with each client's needs.

Our firm implements a holistic approach towards client satisfaction by offering higher level of services, in-time solutions and exercising greater insights to understand the clients' sectors.

Visit us at www.hammurabisolomon.in/

DELHI | GURUGRAM | MUMBAI | BENGALURU | RANCHI | PATNA