Data Protection Journal of India

No: 1/2021: **28th January 2021**

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

Content

From the Chairman's Desk

Dawn of the New Era

The year 2021 in India is expected to see the dawn of a new era of Personal Data Protection Act (PDPA) in India. The new era is not only because the Parliament is expected to pass the Data protection law but also because an organization like, FDPPI is already in place as an organization to ensure that the law be quickly adopted and the benefits start flowing into the society.

Seeing the Sun and the Moon in the same sky may be a rare event and so is the industry being ready even before the law comes into existence.

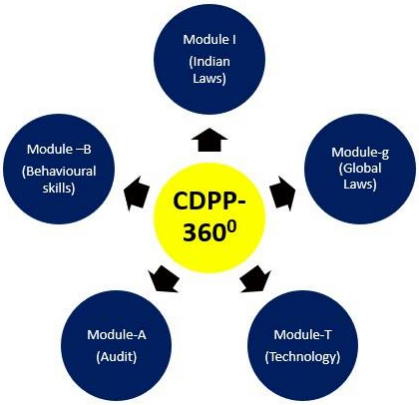
FDPPI has kept the PDPA implementation engine revved up to ensure that the PDPA-India will be able to take off without any further delay.

While PDPA would be the Sun raising on the Indian Skies this year, FDPPI will also raise in all its reflected glory. The harshness of the Sun light will be tempered with the softness of the moon light. Together we should build a Nation which recognizes Privacy as a valuable human right without forgetting that it co-exists with other fundamental rights of existence for individuals.

PDPSI
...Key to Data Protection

FDPPI in its quest to develop a self-reliant (Aatma Nirbhar) **Certification and Audit** system for the Data Protection industry in India has introduced since last one year, "Certified Data Protection Professional" to create the necessary "Knowledge Empowered Professionals" and extended it to "Data Audit Skill Development" through the recent training program on Data Audits. Additionally it has also introduced a tool for Compliance in the form of **the Personal Data Protection Standard of India (PDPSI).**

The 5 Certification programs of that has already developed a group of Data protection professionals who are ready to effectively guide the industry for adoption of PDPA Compliance Programs. Nearly 100 such professionals are now ready to take on the responsibilities of trained "Data Protection Officers" with varying degrees of expertise required by different sections of the industry.



Since 17th September 2018 when FDPPI was incorporated, FDPPI has been undertaking different initiatives to develop professionals who can carry the mantle of Data Protection once the Act comes into existence.

In November 2020, FDPPI conducted the first Indian Data Protection Summit as a virtual event

This journal is a part of this FDPPI movement to reach out to the Professionals, the Regulators, the General public and the Data Processing industry. We shall ensure that the entire industry is empowered with knowledge of Data Protection in all its dimensions.

We are launching this journal on the Privacy Day of 2021. We have also taken this occasion to publish a white paper on Surveillance laws in India which is required for Data Exporters from EU region to India.

We still have projects like DDMAC (Data Disputes Mediation and Arbitration Center) to implement during this year.

I look forward to all the members to pool their professional resources and make this Journal a **Jnaana Bhandara**. (Treasure of Knowledge). This inaugural issue is only the beginning of our journey. We look forward to a continuous improvement of the presentation and content of this Journal as we go forward with the contributions of all those who are committed to Data Protection.

To add a personal touch, we have a "Creative Corner" where we have invited our members to express themselves through Cartoons, poems or other forms of personal expression

relevant to Privacy. We hope this will attract more participation from our members to this publication in the coming days. We are aware that this journal needs improvement and will endeavour to continuously improve. We will have a Q&A section in the coming issues.

Naavi

28th January 2021

A Pride of the Nation

We have a goal…

We shall build a new Cyber Nation,

Where every one is a Responsible Netizen

A Nation where compliance is implicit and Voluntary

Where awareness is widespread and Mandatory

A Nation where Privacy Protection is an accepted Culture

Where Fairness in processing of data is the Future

We are aware…

Data Business is also a part of building a prosperous Nation

Ensuring security is also the duty of the Government of the Nation

The Right to Privacy needs to yield to a reasonable Exception

We therefore need to build a harmonious Union and not a Rebellion

We shall endeavour…

To Come together and Build FDPPI as an Institution

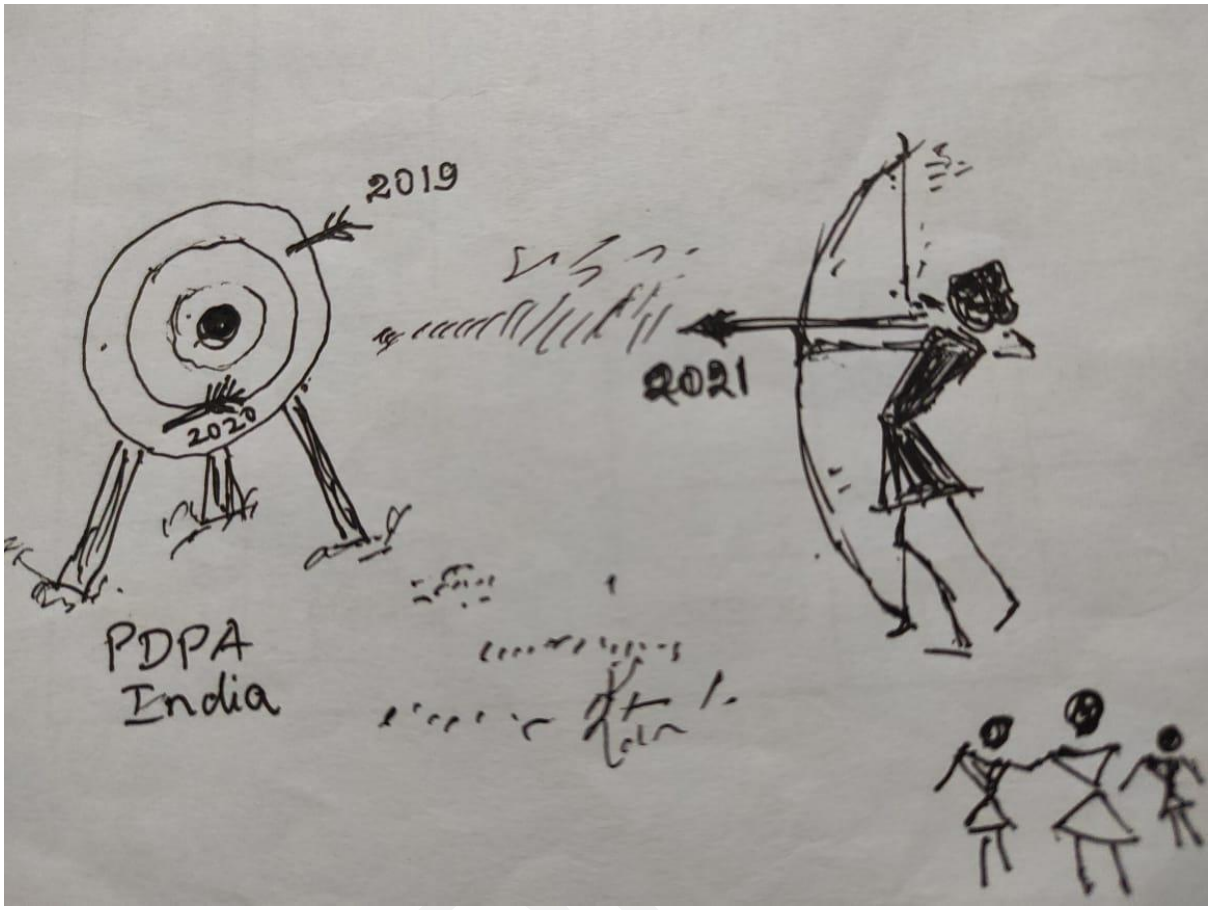
Which shall be a Beacon of Privacy for the Nation

That shall empower the Nation for Global Recognition

And make FDPPI, the Pride of the Indian Nation

Naavi

Cartoon of the Month



Contributed by Durai Kannaiyan

The first draft of PDPB 2018 prepared by the Justice Srikrishna Committee was presented in December 2018 in the Indian Parliament. It could not be passed since the Parliament completed its term and fresh elections were held. In December 2019 the next draft PDPB 2019 was placed before the Parliament. It was expected to be a law in 2020. But again the pandemic situation prevented the law being passed. We all hope it may be passed in 2021.

News Section

From the News Room

1. WhatsApp announced revision of its Privacy policies and Terms of service with effect from 8th February 2021 with a take it or leave it option. The change indicated that WhatsApp will share the information available with FaceBook for advertising without clarifying that it was only the meta data that they perhaps intended to share. This triggered a big debate on Privacy issues and for the first time made many ordinary persons ask what is this Privacy all about.

   Many users are shifting to Telegram and Signal. Search for similar Indian messaging apps are also on. A PIL has also been filed against WhatsApp in Delhi High Court and the Government has also asked for more details from Whats App.

   The public outrage has forced WhatsApp to defer the decision to implement the change of policies till May 2021.

2. From the first of January 2021, UK formally exited the EU. As a result, GDPR ceased to apply in UK and the Data Protection Act 2018 of UK will be coming into operation. These provisions are similar to GDPR. But, until GDPR grants the "Adequacy" status, UK will remain out of GDPR zone and data transfers between UK and EU countries get impacted. There will be need for Standard contract clauses, Binding Corporate Rules or other forms of consent for transfer of data between the UK and other EU countries. Companies which had opened London Offices to manage their EU business may need to shift their offices or open additional offices in the EU region. Many are migrating their data storage systems from London to EU region.
   As an interim measure, UK and EDPB has agreed that for the next 6 months, transfer of data between them would not be treated as a third country transfer.

3. In India, Kris Gopalakrishnan Committee on Non Personal Data Governance filed a revised report making some modifications in the earlier recommendations. Amongst other things, the committee has also recommended that "Consent must be obtained

for Anonymization of Personal Data" by the Data Fiduciary under the Personal Data Protection Act.

4. The JPC on Personal Data protection Bill 2019 has announced that after several rounds of discussions, the committee has suggested about 89 amendments to the Bill and one new clause to the earlier draft. The revised Bill would be submitted to the Parliament during the budget session of the Parliament.

5. The German regulatory authority imposed a fine of EUR 10.4 million on a midsized online retailer who allegedly monitored its employees on CCTV. The Retailer used CCTV in its premises to prevent and investigate criminal offences and to track the flow of goods in the warehouses over a period of at least two years. The State Commissioner did not consider these purposes sufficiently legitimised the use of CCTV in working areas and areas accessible to visitors. The decision has been challenged in a Court.

6. A Cyber attack on **Juspay,** a company in Bengaluru which handles credit/debit card processing for a number of clients like Make My Trip, Amazon etc, has reportedly resulted in compromise of 3 crore data subjects. Juspay claimed that the data breach did not contain much sensitive and transaction data, and mostly contained masked card data which is displayed on merchant websites.

7. The National Digital Health Mission (NDHM) announced its health data management policy incorporating several provisions which are part of the Personal Data Protection Bill 2019.

8. Vodafone was fined Euro 12.25 million in Italy for making hundreds of unwanted telephone calls for promoting its services. Vodafone claimed that the calls were a result of a human error, which was rejected by the regulator.

9. A Gauhati based Start up has launched a new e-mail service named “Letter” claiming high level of Privacy. The service offers e-mail hosting which is encrypted using the user’s password as the passphrase for the encryption keys making it impossible for the email service operator to access the conversations.

10. FDPPI reached the milestone of issuing 100 Certifications for Data Protection Professionals who passed out of its two modules on Data Protection laws , one on Indian laws and another on Global laws. It has now certified 58 professionals for Indian data protection law, 34 professionals for Global Data Protection Laws. It will shortly commence a unique Data Audit Module to impart skills of Data Audit to create Data Protection Consultants as well as Auditors under the PDPSI certification system who also will evaluate the Data Trust Score as part of their audits. These are global firsts achieved by FDPPI.
11. Mr Sridhar Vembu, the celebrated entrepreneur from Tamil Nadu and the founder of ZOHO, was awarded Padmashree by the Government of India. It may be recalled that ZOHO is launching a messaging app called “Arattai” which may be an alternative to WhatsApp
12. Close on the heels of WhatsApp’s attempt to monetize its services through advertising, Twitter has taken certain steps to monetize its platform by acquiring “Revue” , a newsletter subscription service and integrating it as a paid service on the Twitter platform.

13.

Creative Corner

(Where our members express their creativity)

Eager to learn

(On the occasion of launching of Module A program)

We as practising professionals come together
To learn, enrich, contribute and add a feather
- today, is the time for edification as we all gather..

What will we gain?, Is Audit a significant pain? …..I ponder
It is all about Verification, Communication and Reporting, I gather
It may depend on how we Observe, Track, Record, I wonder…

I know, the sessions involve interaction with experts
I Know, I will share my doubts and concerns
I know I will be enriched by the discussions
And
I will be better in my group of professionals

Reena Bengeri

Be Aware

App of Appstore, Playstore, Samsung store

Waiting to capture our personal data

In App world, be aware, nothing is free

At every corner something is scary

Each free app reveals few things

Carry-out many things under the cover

Data trade is the norm of the day

Otherwise why is the App free

Data traders are roaming the cyber streets

To monetize you and me in the trade

Be aware of the hidden dangers

Prevent the attacks of cyber predators

Bondaiah Adepu

Knowledge Section

How does Personal Data Protection System differ from ISMS?

By convention, when we discuss the term "Data Protection", we are referring to *"Personal Data Protection for the purpose of protecting the Privacy of the individual to whom the Personal data belongs."*

At the same time, we recognize that the term "Data" may apply to both "Personal Data" as well as "Non Personal Data". "Information Security" is the term which is more appropriate to be used when we refer to the protection of data that consists of both personal and Non Personal.

"Non Personal Data" may consist of data that has no relation to an individual such as say weather data or data about an industry. Data about an entity which is not a "Natural Person", viz., data about a Company is considered as "Non Personal Data".

The law related to Personal Data Protection often defines what is "Personal Data" and therefore whatever is not coming within the definition of such "Personal Data" would be considered as "Non Personal Data". Such data may include "Anonymized Personal Data", which is data which was once identifiable to a natural person but from which all identity parameters have been removed through a process which may be called the "Anonymisation Process".

There are other kinds of data which are often in the grey area between Personal and Non Personal data.

For example, if the data is about a deceased person, even though the data relates to a natural person, it is unclear if there exists any "Right to Privacy" which needs to be addressed by protecting the subject data.

Also, when we discuss "Personal Data" in the perspective of a law that applies to Citizens of one country, "Personal Data" of persons other than the Citizens of that country may not be within the definition of personal data unless specified.

There are also instances when personal data relates to a Proprietary business entity and whether the data about the concern is considered "Personal Data" or not is often unclear.

Similarly, whether an e-mail address which is say proprietor@vijaytraders.com is to be considered as the personal e-mail of a person called Vijay is unclear.

We shall discuss these types of grey area issues in detail in a future issue. For the time being, let us use the convention that whenever we speak of "Data Protection" we refer to "Personal data protection" unless otherwise specified.

Since the objective of protecting the Personal Data is "Protecting the Privacy Right" of an individual, the scope of Data Protection cannot be limited to preservation of Confidentiality, Integrity and Availability of information, which is the classic definition of "Information Security". Data Protection includes these aspects but extends further to several other Privacy Aspects.

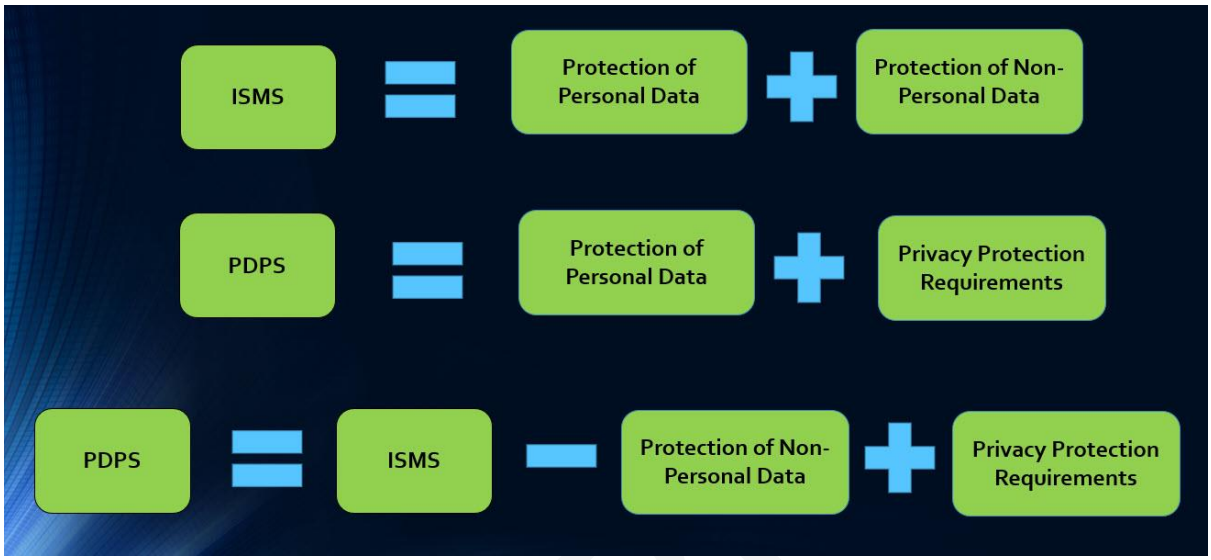
It is for this reason that an Information Security Management system is insufficient as a Personal Data Protection Management System. For the same reason, frameworks for compliance or audit meant for Information Security are not suitable for Personal Data Protection.

The essence of Privacy Protection is that the data collector/processor needs to capture the preference of the Data Subject/Data Principal on how he intends the personal data to be used or disclosed by the data collector/processor. This intention should be available for reference and incorporated into the processing of the personal data through out the life cycle of personal data. Additionally most data protection laws prescribe certain specific rights to the data subject/principal which needs to be ensured during the processing. Also since personal data protection laws designate a separate regulatory mechanism that may include the designation of the DPO, reporting to the regulatory authority, conduct of audits, notification of data breach etc, the Information Security Management System (ISMS) used by organizations for protecting the data under he principle of "Preservation of Confidentiality, Integrity and Availability" (CIA Principle) is inadequate for Data Protection.

The Personal Data Protection System (which is often referred to as PIMS) addresses the need to incorporate the Privacy protection principles to the CIA principle. Again by convention, it is

better to refer to this as Personal Data Protection System (PDPS) instead of PIMS since "Management" is a word which is broader and does not focus on "Protection".

To understand the relationship between PDPS and ISMS, we can express the relationship with the help of the following equations:



Naavi

IMPACT OF PROPOSED INDIAN PRIVACY LAW ON GST DIGITAL GOVERNANCE

The unified indirect tax reform, the Goods and Services Tax [hereinafter for brevity GST], is a comprehensive, tax law, and is gradually progressing towards the self-regulated and transparent tax regime.

GST Network

For effective execution, implementation, and administration of the comprehensive GST law, from the sheer volumes of transactions, it is imperative that an efficient interface of the taxpayer with the tax authorities, largely technology driven is the primary requisite. To achieve this digital special purpose vehicle as the interface of the Registered Taxable Persons (RTPs) a GST common portal (www.gst.gov) was established .The common electronic portal facilitates all front end business processes & settlement of integrated tax, electronic way bill, e-invoice, return and refund mechanisms etc., to the RTPs and other authorized agencies. Any breach in security of data of any sort associated with this portal will cause irreparable damage to the whole of Indian economy as it will hamper all the national and international business of India.

All the GST digital systems and facilities are as on date governed by the privacy norms stipulated under Information Technology Act 2000 (IT Act) act , which have been disclosed in their respective web facilities. The data exchanges with other e-governance digital facilities create further challenges in protection of personal data of an individual.

Personal data in GST digital eco-system

The proposed PDP Bill, being a citizen's rights oriented bill, is bound to make huge impact in the privacy policies being adhered to by all entities in the **in GST digital Governance system**. The collections of information about individuals have become a lucrative source of unjust enrichments for the entities engaged in data collection and processing activities. The main purpose of the Bill is to prevent the breach of privacy of an individual. Therefore the Bill governs the collection and processing of personal data by all such agencies, may be (i)

government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India. The Bill is designed to regulate all agencies involved directly or indirectly in the activities relating to collection and processing and preserving of personal information, and therefore has huge ramifications in management of data by almost all the entities under the umbrella of GST digital governance regime.

Data protection in India

India has been a major outsourcing destination for digital data processing for various entities of the developed nations like United States and Europe. Its popularity has increased day by day as it is one of the largest markets in the world. A varied number of business houses and organizations evince keen interest to do trade with India. In tune with the development in trade and commerce, the activities relating to collection, exchange, processing and analysis of data, including personal data, are taking place at a rapid pace across many entities situated in different countries of the world. The data related activities are carried out in virtual mode by employing various Information Communication Technology (ICT) tools and gadgets. The use of mobile technology as well as increase in density of smart phone users in India has further intensified the stated activities in the cyber world. The quantum leap in use of social media applications, real time deliberations etc., have added more volume to generation of digital data. The adoption of work from home culture so as to safeguard against the pandemic has intensified the activities in the virtual forms by leaps and bounds.

The digital technology has no respect for geographical or political barriers, as it is one of the 'global commons' accessible to the entire population, with little restriction in place. The citizens, one may call them as netizens, communicate each other or amongst groups through high speed networks in real time and huge data of all sorts are produced in inestimable volumes every second. The data storage due to availability of storage option in the form of cloud technology does not indicate the location of such storage. Further related processes may take place in such undisclosed locations. The popular statement that 'the Data is the new oil, attempt to create economic colonies using data mining is a reality' is true in all respects.

This sort of technological explosion has given way for data related activities between netizens of different locations and Nations with no barriers and control. These activities have resulted in a situation where the personal data of an individual could be gathered remotely and exploited for meeting the ulterior motives by the cyber criminal or the enemy Nation. By virtue of dynamic development of computer technology and internet over the years, the problems of cyber crimes have assumed gigantic proportions. It has created an entirely new set of challenges to law enforcement agencies all over the world. It has equally become a cause of serious concern to every user, to find effective ways and means to prevent and combat the unregulated illegal flow of data worldwide. Therefore there is urgent need of suitable privacy protection laws to enforce discipline and accountability for generation and exploit of digital data in India as well as in other countries, so that such cyber crimes could be identified and contained which further helps in deterrence.

Many countries around the globe including India have enacted their own criminal laws and computer laws, information technology laws, privacy laws (among other laws) to respond to the problem of cyber criminality. But considering the sheer international dimension of these crimes and concerns of evil designs, particularly where the crime relates to individual citizens of foreign countries, the laws in place in India are found to be inadequate. The internet as a global media may be accessed throughout the world and can be viewed in any part of the globe and therefore the applicability of particular country's law for the disputed transaction remain unresolved, as its reach marches ahead to a different sovereignty and differences in cyber legislations. In certain instances it is reported, that some states actively encourage and engage remotely in criminal activities and cyber-espionage, which further aggravates the problems. Such lapses provide the criminal undesirable advantage to cover-up the crime, directly at odds with interests of any civilised society.

The legal frame work under IT act 2000

In India the Information Technology Act, 2000 (hereinafter referred to as IT Act) is the primary legislation that regulates the use of computers, computer systems and computer networks as also the data and information in electronic format. This statute provides the necessary legal framework in regulation of the electronic applications, storage, processing, authentication as

well as electronic contracts, e commerce, cyber offences and liability of network service providers. This legislation also provides protection in respect of digital data or information concerning the privacy of an individual. The Sections 43, 43A, 72 and 72A of the IT Act provide the required legal framework for protection of all data in digital form, which includes the privacy and security breaches. "The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) (SPDI) Rules 2011 is the specific provision as on date that covers the matters relating to sensitive personal data and its protection. Therefore one can conclude that the IT Act does not exclusively deal with the right to privacy, but the SPDI Rules lay out a framework to govern the collection, management, use, and sharing of personal data or sensitive personal data or information. The said Rules do not recognise that a right to privacy applies to every individual. In other words the subject provisions do not treat the personal and sensitive data as a separate set entitled for privacy as a fundamental right.

The IT Act provides civil remedies in case of unauthorised access, theft of passwords, login credentials,, trespass, unauthorised copying, downloading and extraction of data, introduction of any contaminant or virus, unauthorised transmission, deletions or alterations of any information residing in a computer resource, resulting in violation. The Section 43A and the SPDI Rules apply to 'body corporates', requiring them to maintain reasonable security practices and procedures while possessing, dealing or handling data in a computer resource. The common yard stick of measure in respect of intermediaries engaged in such data related activity is limited to following due diligence principles. Further the ‘body corporate' as defined under IT Act excludes any government agencies or non-profits entities. The Breach of confidentiality and privacy and disclosure of information in a lawful contract are liable for criminal action under IT act. The above findings categorically indicate that in the ever growing digital society, there is no specific law that protects the privacy of an individual from the business entities who are involved either as perpetrators of crime or abettors of crimes, by way of unauthorised collection and processing of personal data and selling them like a commodity.

Privacy as a fundamental right

The extensive use of digital technology tools to collect privacy data of a person on some pretext or other, for commercial exploitation, without the knowledge of the subject, has

created an environment of fear for the individual. The need for such a law attained a larger proportion, when the government initiated the 'Aadhaar Project' without a proper legislation in place.

In the year 2012 , Justice K.S. Puttaswamy (Retd.) 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 Supreme Court in the said case viz., Justice K.S. Puttaswamy v/s Union of India, passed the historic judgment on 24th August 2017 wherein it affirmed the constitutional right of a citizen to protect her/his privacy. *"The Right to Privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution",* the Apex court held. Treating the privacy rights as fundamental right, the Apex court protected the citizen from the clutches of an entity engaged in the business of data collection and process, without a valid consent of such person. Further, the 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 that (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.

Origin of Personal Data Protection Bill

During the proceedings of the said case, the Indian government set up an expert committee, headed by Justice (Retd) B N Srikrishna, to devise a data protection legal framework. Based on the committee's report, the Union Government introduced the 'Personal Data Protection (PDP) Bill, 2019' in the Lok Sabha on December 11, 2019. This Bill proposes to provide a legitimate structure for protection of personal data of individuals and regulatory framework for collection and processing of such data by various agencies through establishment of a Data Protection Authority.

In the Preamble, the stated objectives of the Bill are: "*…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 rights of individuals whose personal data are processed, to create a*

framework for organisational 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 unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes..." It further asserts that, "*the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy. The growth of the digital economy has expanded the use of data as a critical means of communication between persons and therefore it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals ….*" At present, the Bill is referred to a joint parliamentary select committee for scrutiny and report, after suitable consultation with all stake holders. It is pertinent mention here that the flow and usage of personal data create a relationship of trust between persons and entities processing, which shall be protected by such entities, in a unique trustee relationship, which is different than the one advocated in IT act.

Data and personal data under PDPB

In the PDP Bill, **data** has been defined to include representation of information, facts, concepts, opinions or instructions suitable for communication, interpretation or processing by digital (automated) or non-digital (paper-pen) ways. Even the information, facts, concepts etc., capable of being communicated in traditional form, by way of writing on paper or in any similar manner are treated as 'data'. The IT act defined the data to consist of information, facts etc., that are stored or processed in digital way only which is much narrower as compared to data as per PDP Bill.

If such data is "personal data" about or relating to a natural person who is **directly or indirectly identifiable**, having regard to any characteristic, trait, attribute or any other feature of the **identity of such natural person** are protected under PDP Bill. The natural person to whom the personal data relates is named as the Data Principal, treating each such person as the owner of her / his personal data. Under PDP provisions mere data itself will not create any right to the principal unless there is an element (unique to such a Data Principal) that connects such data to the principal. If such relationship is not forthcoming, then no breach of personal data could be alleged to have taken place under PDP Bill. Further such personal data should be pertaining to the group of 'sensitive personal data' viz., financial data, health data,

official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation etc., of the principal, to seek protection under the proposed Act. For example, in a hypothetical situation, in places like a reception hall or office premises, certain personal data may be collected manually with identifiers like telephone number, mobile number, email address etc. of individual(s) through the use of visitors' books and such information of a natural person (principal) is said to be in a non-digital format. In such instances, caution must be exercised to guard such personal information, as breach of such information without the consent or knowledge of the Principal may result in violation of provisions under PDP Bill.

Any person, including the State, a company, any juristic entity, a firm, a HUF or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data are termed as the Data Fiduciary. Therefore the Government, in the role of a fiduciary is also treated as a person who should adhere to the legal framework under PDP Bill. The fiduciary may permit the processing of such personal data on his behalf by any person, including the State, a company, any juristic entity or any individual etc., who processes data on behalf of a fiduciary are called a Data Processors. Such activities will also be present in GST digital regime as all stake holders are involved in collection and process of the personal data and therefore all such entities should be mandated to follow the PDP norms as a fiduciary and / or a processor.

It is important to note that the provisions of PDP Bill will not be applicable to the data other than personal data of an individual. The data that have an identity of a Company or such entities or general business data, which does not include personal information with identity of such person, remain outside the purview of the PDP Bill. Further any personal data, when converted to form an Anonymized data, are not covered under the ambit of PDP Bill. Only the personal data with an element of identification of an individual are treated as Non-Anonymized Data and are covered under the ambit of PDP Bill.

The Anonymization in relation to personal data, means *'such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority'.* Hence the

Data anonymisation refers to the removal of identifiers, either direct or indirect, by some form of an irreversible process, which must be a standardised process approved by the authorities. This means that the data still exists, but the link between the data and the data principal is converted or transformed in such a way that the data principal cannot be identified from such data and such anonymised data cannot be attributed back to the person by any means by any one. Such data which has undergone the process of anonymisation are called as "anonymised data".

For faceless assessment or any such processes, the personal information identifiers may be removed from the available data using certain digital tools and after completion of the assigned task, such data will be converted back into their original form. The whole process is called as "de-identification" meaning, 'the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal". These processes do not amount to anonymisation of data and therefore are very much covered in the ambit of PDP Bill.

Sensitive Personal data during GST registration

For Registration of a taxable entity, the GST laws provide for furnishing of, among other data, the following information which may fall under the sensitive personal data of individuals, who may be a proprietor, or partner or Karta or director or trustee or member of such entity viz.,

(i) declaration of Permanent Account Number, mobile number, e-mail address under Rule 8(1) of CGST Rules 2017;
(ii) declare Aadhaar number under Rule 8(4A) of CGST Rules 2017;
(iii) information with respect to details of bank account under Rule 10A of CGST Rules 2017;
(iv) passport details and identification number or unique number or Permanent Account Number, of a non-resident taxable person under Rule 13 (1) of CGST Rules 2017, or his Authorised Signatory under Rule 13 (4) of CGST Rules 2017;
(v) addresses of premises and telephone number of such entities.

The list can be further extended in respect other functions of the GST laws and procedures. Whenever the manual process are resorted to in any function activity, especially with regard

to refunds, necessary care should be taken to follow the provisions of PDP Bill religiously.. The IT Act through the *IT (SPDI) Rules, 2011* deals with protection of "Sensitive personal data or information of a person", which includes such personal information consisting of information such as passwords, financial information like bank account or credit card or debit card or other payment instrument details, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information. The definition of the term Sensitive Personal Data under PDP bill is more expansive than the sensitive personal data information mandated under IT act. Therefore due care should be taken to safeguard all such additional sensitive personal data. However it is surprising that Password is not treated as a sensitive personal data in PDP bill. However the protection under IT act continues in respect of passwords.

Data Principal and personal data processing

The PDP Bill states that, 'no personal data shall be processed by any person, except for any specific, clear and lawful purpose'. One more important factor to be noted is that the protection under this proposed legislation is limited to the personal data. The definition of personal data covers any inference drawn from personal data for the purpose of profiling since such inference typically leads to indirect identification of a natural person, called **"Data Principal**

The entities that collect and / or process a data relating to a principal are called as **"Data Fiduciary** and any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary called as data processor are covered under the PDP Bill. The "P**rocessing** in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

The "Data Principal and Data Fiduciary" relationship is a kind of a mixed and unique one, a blend of essentials features of a contract as well as of a Trust. The Data Fiduciary can be termed as a Special trustee as the relationship with Data Principal is not a simple "Principal and Agent" contract.

PDP Bill defines two kinds of Data Fiduciaries namely (i) the Significant Data Fiduciary, to be notified by Data Protection authority [DPA] based on the volume and sensitivity of data processed as well as the risk of harm; and (ii) the Guardian Data Fiduciary, who operates any commercial website or online services. The definition of "Data Processor" includes any person including a State which processes personal data on behalf of a data fiduciary and the definition of processing includes all operations including storage and retrieval of information.

Obligations of data fiduciary

The Bill allows the processing of data by Fiduciaries only after the **due consent is obtained from** the individual / Principal. For obtaining the consent of a Principal for collection or processing of personal data there is need of issue of a notice by the fiduciary to such person, stating the reasons in clear, concise and easily comprehensible terms. The procedure for issue of notice to the principal, at the time of collection of data, for obtaining the consent is elaborate and due care to be taken to devise digital tools for meeting the requirements. In the notice the Principal should be informed about the purpose, nature and categories data being collected. The identity and contact details of the data Fiduciary and the contact details of the data protection officer are also to be informed to the Principal. Such Principal should be informed of the procedure to withdraw his consent in the mandated way. Therefore the facilities in GST Digital Regime may have to gear up for implementing this provision for each of such individual with whom personal information are gathered. Such consent should be obtained in respect of existing personal data of the principal existing in the GST digital regime once the PDP law comes into effect.

A personal data can be processed only for specific, clear and lawful purposes. The Data Fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it was processed and shall delete the personal data at the end of processing. The personal data may be retained for a longer period only after the data fiduciary gets necessary consent from the Data Principal.

In certain circumstances for performance of any function of the State as authorised by law the personal data may be processed without the consent of the Principal. Thus, explicit

consent by data principal may not be taken in circumstances where data is processed (i) for providing any service or benefit to the Data Principal; (ii) for the issuance of any certification, licence or permit; (iii) for any action or activity, under any law for the time being in force made by the Parliament or any State Legislature; (iv) for compliance with any order or judgment of any Court or Tribunal. Some of the above reasons could be applied to the activities in GST digital regime, which needs to be further explored.

Under clause 14(1) of the PDP Bill, the personal data may be processed without obtaining the consent of the principal, like in public interest for reasonable purposes, which could be surveyed for applicability of certain activities of the GST digital regime.

The Bill mandates that a data fiduciary is required to formulate a 'privacy by design' policy that ensures (a) Managerial, organizational, business practices and technical systems designed in a manner to anticipate, identify, and avoid harm to the data principal, (b) above listed obligations towards protection of personal data, (c) technology used is in accordance with commercially accepted or certified standards, (d) legitimate interests of businesses including any innovation is achieved without compromising privacy,(e) protection of privacy throughout the processing, from the point of collection to deletion of personal data, (f) processing of data in a transparent manner and (g) interest of the data principal at every stage of processing of personal data. The data fiduciary should submit its Privacy by Design Policy to the Authority for certification by DPA and display such certified document in their websites.

Each company classified as significant data fiduciaries will have appoint a Data Protection Officer (DPO) who will liaison with the DPA for auditing, grievance redressal, recording, maintenance and more. In addition to the above stipulations, all fiduciaries should periodically undertake certain transparency and accountability measures. Therefore, they are required to: (i) implement data security safeguards, such as data encryption and preventing misuse of data; (ii) Set up grievance redressal mechanisms to address complaints of individuals.

The primary objective of the Bill is to safeguard the right to privacy of the citizen /principal. The principal, in respect of the personal data pertaining to him/her, has rights namely, (i) right to confirmation and access to the personal data with the fiduciary;(ii)right to seek correction

of inaccurate, incomplete, or out-of-date personal data;(iii) right to have personal data transferred to any other data fiduciary in certain circumstances. [Data portability];(iv) right to restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn;(v) right to receive the data from the fiduciary in a machine-readable format. These rights of data principal need to be noted carefully by the fiduciary. Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any Data Principal.

The data fiduciary shall not engage, appoint, use or involve a data processor[1] to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor. Further such appointed data processor shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorization of the data fiduciary and unless permitted. The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.

Other important contents of the Bill

The Bill proposes for setting up of a Data Protection Authority (DPA) who may, (a) take steps to protect interests of individuals; (b) prevent misuse of personal data; and (c) ensure compliance of concerned with the Bill.

The central government may exempt any agency from the applications of the provisions of the Act for meeting certain specified needs that are (i) in the interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to commission of any cognisable offence relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain specific purposes such as: (i) prevention, investigation, or prosecution of any offence; (ii) personal, domestic; or (iii) journalistic purposes. However, such processing must be for a specific, clear and lawful purpose, with proper safeguards. For use of personal data found

necessary for activities like such as research, archiving, or statistical purposes, the DPA subject to certain conditions may notify such class of activities for a particular fiduciary as an exempted category.

It is important to note that any data principal who has suffered harm as a result of any violation of any provision by a data fiduciary or a data processor shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be. The Data Principal may seek compensation under this section by making a complaint to the Adjudicating Officer in the prescribed manner to be notified.

Whenever there is personal data breach, it creates the scope for an offence under the proposed bill. The personal data breach is defined as any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal. Stated offences under the Bill include, (i) processing or transferring personal data in violation of the stated law and (ii) failure to conduct a data audit. The processing or transferring personal data in violation of the Bill is punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher. The failure to conduct a data audit is punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher. The Officers in the DPA are vested with the power to call persons concerned for inquiry into fiduciaries, assess compliance, and determine penalties on the fiduciary or compensation to the principal.

The way forward

Data Protection refers to the set of privacy laws, policies and procedures that aim to minimise intrusion into one's privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency.

The provisions relating to obtaining consent of the principal to collect personal data may have to be followed in a scrupulous manner so that the stringent compliance of the stated law is adhered to. The entities classified as data fiduciaries should determine the purpose and means of processing personal data in a fair manner as stipulated in the law. Organisations will have to undertake a great deal of **technical changes in engineering the existing architecture** to modify business processes to meet the requirement of the proposed law. They need to place limits on data collection, processing and storage and similar responsibility they owe to the principal. There is need of proper encryption of personal data along with **technical security safeguards, including de-identification, preventing an individual's identity to be inadvertently revealed so as to prevent** instances of data breach.

Under IT Act, a body corporate is considered to have complied with reasonable security practices and procedures, if they have implemented security practices and standards along with having a comprehensive documented information security program and information security policies such as ISO 27001:2013, duly approved by the central government. In view of the wider and distinctive scope of provisions of PDP Bill it is opined that global standards of data protection contained in stated standards are inadequate to meet the privacy requirements of the said Bill. Therefore such standards are to be reviewed and revised by the concerned authorities to meet the requirements and endorsement under the PDP Bill. Though PDPA 2019 has adopted several principles of Privacy Protection from global documents including the GDPR (General Data Protection Regulation of the European Union), the compliance requirements in India regarding Information Privacy Protection is distinct and therefore the revisions of the standards are essential. It is important to mention here that while calling for quotations for outsourcing any activity involving sharing or exchanging of personal data for any purpose, there must be a condition inserted to the effect that such vendors should be compliant to provisions of PDP laws. Only then they should be considered for working with the GST Digital Regime. This action and care should be initiated in respect of existing stake holders also as soon as the PDP law comes into force.

As countries around the globe start to enact and implement personal data governance regimes, this Bill will have an immensely vital role in shaping the regulation governing today's increasingly data-driven geopolitical landscape. It tries to address some of the major issues

faced in privacy protection landscape by heralding fundamental changes in the way data is gathered, processed, stored and deleted by different parties with access to such invaluable data. The Bill contains some elements of the protectionist data policies that are similar to other statutes made or in pipe-line around the world, so as to curtail the global and open internet, which has become a cesspool of exploiters of such data waiting to prey on their next victim of cybercrime.

M. G Kodandaram, IRS

Assistant Director (Retd),

ADVOCATE and CONSULTANT

mgkodandaram@gmail.com

Q&A Section

This Section is meant to answer the questions of the readers. Since this is the inaugural issue, we donot have any questions to answer.

We look forward to receiving questions from our readers and publish our views from the next issue.

We have now picked up a sample question to start the section

Question:

In IT Act, there was some reference to ISO 27001 as one of the evidences of having reasonable security practices. In PDPB?A, there is no such reference… Is it something to be viewed as good (being framework agnostic:?

T.Subbarayudu

Our View

Yes. Act should not specify a framework . Even when referred to in a regulation, it should be as an example and not be treated as "Deemed Compliance". This was done in the notification of Section 43A rules in April 2011.

PDPB/A envisages "Codes and Practices". We need to wait and see if these Codes and Practices will remain agnostic of the framework.

Special Section

(White Paper on Surveillance Laws in India)

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

WHITE PAPER

LAWS OF SURVEILLANCE IN INDIA

Date: 26th January 2021

Published by

Foundation of Data Protection Professionals in India

37, "Ujvala", 20th Main, BSK First Stage, Bangalore 560050

From the Chairman's Desk

After the EDPB published its recommendations on the European Essential Guarantees for surveillance measures on 10th November 2020, it has become necessary for Data Exporters from EU region who export Data for processing in India to conduct an assessment of the surveillance laws in India before finalizing the Standard Contractual Clauses of the Data Processing agreement.

It may be expected that most of the Data Exporters would request their Indian Counterparts to advise them of the surveillance laws in India. In order to assist the Indian companies to prepare such a report, FDPPI wanted to generate a background paper to present the different laws which are required to be examined in this context.

An internal task force lead by Ms Meena Lall consisted of Dr Amitkumar Khatu, , Ms Meenal Maheshwari, and Ms Vasanthika Srinath put together a report which is enclosed.

We hope this report would be useful to Indian companies and may be shared by them if they so desire.

I thank the members of the task force for their painstaking work and a detailed presentation.

Na.Vijayashankar

(Chairman)

Preface

In today's age of ubiquitous dataveillance, the state has become an Informational State and together with the evolving and ever-advancing technologies of data mining and data aggregation, the concerns that privacy faces today has been realistically portrayed in the judgment of nine Hon'ble Judges in the famous case of *K.S. Puttaswamy v Union of India*[2], commonly known as the Privacy case.

What does the expression **"surveillance"** mean? The Hon'ble Apex Court of India asked itself this question in as far back as in the year 1963[3], while interpreting the constitutional validity of U.P. Police Regulations. A Bench comprised of six Hon'ble Judges answered the question as:

"Surveillance conveys the idea of supervision and close observation"

In recent times, the suit filed by WhatsApp and its promoter company Facebook against the Israeli cyberintelligence firm NSO in the court at California accused the latter of despatch to 1400 mobile phones and devices across the globe of Pegasus for surveillance. Whether or not the allegations are devoid of merit, in the context of India, the question that arises is: *Is this kind of surveillance illegal in India?*

It is further a belief that Governments mandating data localisation are motivated by surveillance also as a reason, besides many other reasons such as data security, protection of business, check on privacy or freedom of speech, etc. The data localization requirements as contained in the 2018 Personal Data Protection Bill garnered censure heavily. It may have been that the underlying objective was to achieve better privacy safeguards for the personal data of a principal, stakeholders viewed the restrictions as an attempt to increased state surveillance, data sovereignty, and greater costs for doing business in India.

Additionally, it is clear that adequacy decisions are mostly bilateral cooperation exercises between countries. In such decisions, relevant laws, justice system, access to the system, the prevailing rule of law, access to justice, human rights enforcement regime, etc are the factors which play considerable role. However, the evolution of stability on adequacy decisions through judicial scrutiny is bound to take time. Not only that, developing standard contract clauses or binding the industry across the globe to common clauses itself is expected to take considerable time.

---

[2] Reported in (2017) 10 SCC 1

[3] *Kharak Singh v State of U.P. and Other* – AIR 1963 SC 1295

This paper is being presented to given an outline of surveillance framework as it presently exists in India. The topic has its relevance in all spheres of business touching the core of 'Atma Nirbhar Bharat' i.e. ease of doing business, the economics of business, cross-border data transfer, the justice system in India, the contractual aspects coupled with laws supporting implementation of the agreed obligations and finally the risks associated with actions and omissions, along with the governance expectations.

We sincerely hope and trust that the readers will find this paper useful and rich in content. We shall be happy to receive your valuable feedback which may be sent to the Chairman, FDPPI through e-mail at fdppi@fdppi.in.

*****

TABLE OF CONTENTS

*****

CHAPTER: I

SCOPE AND PURPOSE OF WHITE PAPER

1.1 Introduction:

Digital technologies have drastically changed our world. They have made our lives easier and have given us a feeling that everything in the virtual world is available at our fingertips. At the same time, the digital revolution has created a menace of leaving behind minutely detailed records of the activities that we indulge in our daily lives. Contemporary governments are showing a keen activism to acquire this data and use it for various purposes.

Though there exist several laws that protect citizens against the interference of government authorities in the form of surveillance, secret programs of any government cannot be challenged until they are declared or discovered. On the other hand, very often, citizens have little understanding of the impact of surveillance on their lives. Surveillance can curtail or put the exercise of civil liberties at halt. Surveillance may also make people not to experiment ideas which are new, controversial or which deviate from the ideology of the government. This is the real danger of surveillance. One of the fundamental principles of the concept of 'state' is to protect the intellectual freedom of its citizens to think without the oversight or interference of state, which is called "intellectual privacy"[4] of its citizens.

It is an undisputed fact that the degree of surveillance varies from nation to nation and jurisdiction to jurisdiction, but all nations indulge in surveillance activities. The degree of surveillance exercised by the nations can be measured based on several factors like constitutional protection, statutory protection, privacy enforcement mechanisms, visual surveillance, communication interception, workplace monitoring, government access to data, retention of communication data, surveillance of medical and financial records, etc.

With the advent of various laws governing protection of personal data, there has been increase in awareness across the world about surveillance. This awareness has made the surveilling parties more accountable and answerable to the measures provided under enabling provisions of laws governing privacy and data protection. Recent

[4] Neil M. Richards, *Intellectual Privacy*, Texas Law Review , Vol. 87, p.387, 2008, Washington U. School of Law Working Paper No. 08-08-03, available at Intellectual Privacy by Neil M. Richards :: SSRN, last seen 15.12.2020.

judgements of the European Court of Justice ("EUCJ") in Schrems-I and Schrems-II cases raised several questions about the adequacy of data protection measures in a country to which EU data is proposed to be transferred under a data processing contract.

Pursuant to the decision of EUCJ, the European Data Protection Board ("EUDPB") has issued recommendations on 10th November 2020 to supplement the transfer tools available to Data Controllers, who are covered under the GDPR. One of the requirements under the recommendations of EUDPB is that the data exporter needs to assess the law or practice in the destination country that may impinge on the effectiveness of the appropriate safeguards being relied upon.

1.2 Our endeavour:

Since FDPPI is an organization that has set an objective to empower the data protection ecosystem in India, it has compiled this white paper on existing surveillance laws and practices in India that may have an impact on the data processing industry in India. This white paper intends to assess the surveillance laws and practices prevailing in India. This assessment may be helpful not only to the data industry players in India but also to the data controllers intending to do business with Indian data processors. They may form their independent opinion whether the surveillance measures in India are acceptable as per the recommendations of the EUDPB.

An endeavour is made in this white paper to cover the public as well as private surveillance, which in our view are simply related parts of the same problem, rather than being wholly discrete from each other. Though the cross-border contracting parties may be more concerned with government surveillance, we have tried to cover the legal position applicable to the government as well as corporate surveilling entities.

We have tried to encompass the fundamentals of cross-border data transfer by giving a world view of the general principles of surveillance and what has changed for cross-border data transfer after the recent recommendations of EUDPB. While trying to give a detailed account of the Indian laws related to surveillance, we have enunciated the view of the Supreme Court of India on surveillance through few landmark cases. This white paper also illustrates the principles of privacy and the concept of due process to be followed by governmental authorities while making policies governing surveillance.

The representations and warranties as well as indemnities, guarantees and dispute resolution clauses contained in material covenants of a commercial contract have also added a great value to this white paper. We have also included some model clauses to

protect the data principal from impact of surveillance. The paper also covers corporate governance by emphasizing on the requirements of legitimate documentation and factors for mitigation of risk, while underlining the need for third party independent audits.

Finally, this paper makes comments on the adequacy of the existing legal framework of India governing surveillance and whether there is a need for a separate sectoral or general law for surveillance. This white paper also highlights the need for balance between privacy and surveillance.

*****

CHAPTER: II

FUNDAMENTALS OF CROSS-BORDER DATA TRANSFER & RECENT CHANGES

2.1 A World View:

On July 16th 2020, the Court of Justice of European Union issued its land mark decision in "Schrems II". This judgment has the following effect:

(i) The certainty of conditions for lawful transfer of data has been obliterated.
(ii) The ruling invalidates the EU-U.S. Privacy Shield arrangement.
(iii) Until July 16, Privacy Shield had served as an approved “adequacy” mechanism to protect cross-border transfers of personal data from the European Union to the United States under the EU GDPR.

Reportedly, over 5,000 organizations participate in Privacy Shield. Many thousands more EU companies rely on Privacy Shield when transferring data to these organizations.

The protection of personal data is considered to be a human right and any compromise on the privacy of Personal Data has been viewed very seriously by EU member countries. The European Union Data Protection Directive of 1995 was issued by EU to ensure this protection and each member country has made corresponding national laws. This Directive lays down the key criteria for making data processing lawful and the principles of data quality in order to protect the rights and freedoms of persons with respect to processing of personal data. Broadly, the European Union Directive of 1995 (Directive 95/46/EC) lays down the following prescriptions:

(i) Data processing would be lawful, only if the data subject has provided unambiguous consent OR processing is imperative for any one of the following:

- performance of a contract to which the data subject is party;
- compliance with a legal obligation
- protection of vital interests of the data subject
- performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller or a third party
- pursuing legitimate interests by the Controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection

(ii) Mandatory principles of data quality:

- If the data is personal data, it must be processed *fairly and lawfully*, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant, accurate and not excessive, and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected;
- It is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. The only exception to this is a situation where processing is necessary for preventive medical diagnosis and treatment or vital to the interest of data subject.

(iii) Rights of a data subject: A data subject is entitled to exercise the following rights:

- Right to information: The Controller must provide the data subject from whom data is collected with certain information relating to himself/herself (the identity of the controller, the purposes of the collection and processing, recipients of the data, etc.)
- Right of access to data: Every data subject should have the right to obtain from the controller all data collected pertaining to the data subject
- Right to object to processing of data: The data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her.
- Disclosure of data to third parties: The data subject should be informed before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures.

(iv) Other relevant aspects:

- *Exemptions and restrictions from data subject's rights*: the scope of principles relating to quality of the data, information to be given to the data subject, right of access and publicising of processing may be restricted in order to safeguard national security, defence, public security, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union or the protection of the data subject.
- *The confidentiality and security of processing*: any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the Controller. Additionally, the Controller must implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

- The *notification* of processing to a supervisory authority: the Controller must notify the national supervisory authority before carrying out any processing operation. Prior checks to determine specific risks to the rights and freedoms of data subjects are to be carried out by the supervisory authority following receipt of the notification from the controller. Measures are to be taken to ensure that processing operations are publicised and the supervisory authorities must keep a register of the processing operations notified.

(v) Judicial Remedy & Compensation: Every person shall have the right to judicial remedy for any breach of the rights guaranteed by national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.

(vi) Cross-Border Data Transfer: Transfer of personal data from a Member State to a third country with an adequate level of protection are authorised. Although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive e.g. the data subject him/her self agrees to the transfer; in the event of the conclusion of a contract; it is necessary for public interest; and also if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.

There is a significant difference in how the US and EU view protection of personal data. Data transfer between European companies and its counterparts in the United States was a concern. After a series of negotiations between the two sides, a middle ground called the Safe Harbour framework was arrived at whereby the EU member countries secured certain commitments from US with respect to privacy of personal data. The Safe Harbour framework was executed between the United States Department of Commerce and the EU Commission in 2000 (EU Decision 2000/520).

The revelations of Edward Snowden brought to light several global surveillance programs, many of which were run by US Government with the cooperation of telecommunication companies. It is in this context that Mr Schrems, an Austrian national residing in Austria, who is a user of Facebook, filed a complaint in 2013 before the Irish Data Protection Commissioner, requesting the latter to use his statutory powers and prohibit Facebook Ireland from transferring his private data to the United States. Maximillian Schrems had been

a Facebook user since 2008. As is the case with users residing in the European Union, some of the data belonging to Mr. Schrems had been transferred by Facebook Ireland to its servers belonging to Facebook Inc., located in the United States.

The contention was that the law and practice in force in the US did not ensure adequate protection of the personal data held in its territory against the surveillance activities that the US public authorities engaged in. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency (the NSA).

2.2 Development in Schrems-I:

(i) The Commissioner refused to entertain this request, based on Decision 2000/520/EC, stating that the United States does provide adequate levels of protection to the personal data of an individual.

(ii) Against this order of the Commissioner, Mr Schrems brought an action before the High Court of Ireland. The High Court opined that:

- the citizens of European Union have the effective right to be heard when agencies in the United States, on the pretext of intelligence services, are accessing their personal data.
- the transfer of data outside national territory should be made only when the recipient ensures an adequate level of protection.
- privacy being a fundamental right, is inviolable.
- Analysing the decision 2000/520/EC, the High Court verified the legality of Safe harbour regime. After a detailed hearing, the High Court of Ireland effectively noted that EU citizens have no effective right to be heard.
- mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution.
- for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards.

- the matter needed to be assessed in the light of EU law and not Irish law alone, as the case concerned the implementation of EU law as referred to in Article 51 of the Charter.

  Thus, according to the Irish High Court, if the matter were to be looked at only on the basis of Irish law, the Commissioner should have investigated Mr Schrems' complaint and should not have rejected the complaint.

(iii) The High Court of Ireland referred the case to the Court of Justice of the European Union referring the following questions to the ECJ for a preliminary ruling:

- Whether in determining a complaint that a third country's laws and practices do not contain adequate protection for data being transferred to it, a national supervisory authority (such as the DPC) is bound by Decision 2000/520, having regard to Articles 7, 8 and 47 of the Charter and to Article 25(6) of the Data Protection Directive.
- Alternatively, may and/or must the DPC conduct its own investigation of the matter in light of factual developments since Decision 2000/520 was made.

On 6-10-2015, in Case C-362/14, the Court of Justice of the European Union invalidated the Safe Harbor and stated that, in order to be "adequate", the level of data protection offered by the third country should be "essentially equivalent" to that being offered in the EU. As a result, the High Court annulled the decision rejecting Mr. Schrems' complaint and referred the case back to the DPC. Invalidation of Safe Harbour framework for data transfers between the EU and USA, obviously triggered an uncertainty among business enterprises and members of the global privacy community. Businesses worried about continuance of their operations as most multinational companies work as a single entity allowing seamless movement of data among group entities.

This judgment became the genesis of EU-US Privacy Shield.

2.3 Privacy Shield and Schrems-II:

(i) To ensure continued business between the two continents and to overcome the judgment, US and EU Data Protection agencies negotiated a better framework. The outcome was the new arrangement announced on 2-2-2016, named *the EU-US Privacy Shield*. This new framework promises to protect the fundamental rights of Europeans when their personal data is transferred to the United States

and ensure legal certainty for businesses. However, the legality of this arrangement is also expected to be challenged in EU courts. The US too will not give up its surveillance rights easily. We will cover the new US-EU Privacy Shield in a future article.

(ii) In the remittal judgment before the DPC, Facebook Ireland explained that the invalidated adequacy decision was not relevant as a large part of personal data was transferred to Facebook Inc. pursuant to European Commission's Implementing Decision (EU) 2016/1250 of 12 July, 2016 (the Privacy Shield Decision) and Standard Contractual Clauses (SCCs).

(iii) On this basis, the DPC asked Mr. Schrems to reformulate his complaint. In his reformulated complaint lodged on 1st December 2015, Mr. Schrems alleged that US law required Facebook Inc. to disclose his personal data to certain United States authorities in the context of various monitoring programs (in particular, the FISA 702 and the Executive Order 12.333). In Mr Schrems' view, these programs contravened different data protection principles as well as Articles 7, 8, and 47 of the Charter.

(iv) After investigating the allegations made by Mr. Schrems, the DPC argued that it could not adjudicate on them until the ECJ had examined the validity of the SCCs, and so it brought proceedings before the High Court. On May 4th, 2018, the High Court made the reference for a preliminary ruling to the ECJ.

(v) In its reference to ECJ, the High Court specified that Section 702 of the FISA permitted the Attorney General and the Director of National Intelligence to authorize jointly, following FISC approval, the surveillance of individuals who are not US citizens and who are located outside of the US in order to obtain foreign intelligence information. It was also affirmed that Section 702 of FISA provided the basis for the PRISM and UPSTREAM surveillance programs. PRISM in particular, requires Internet Service Providers (ISPs) to supply the NSA with all communications to and from a 'selector'. UPSTREAM on the other hand, permitted the NSA to copy and filter Internet traffic flows from the 'backbone' of the internet, granting it access to both the content of communications and their metadata.

(vi) High Court had found that Executive Order 12.333 (E.O. 12333) allowed the NSA to access data in transit by accessing underwater cables on the floor of the Atlantic. The High Court stated that the only limit on US surveillance activities

was found in the Presidential Policy Directive (PPD-28), and even this only stated that intelligence activities should be 'tailored as feasible'.

(vii) On the basis of these findings, the High Court considered that the US carried out mass processing of personal data without ensuring a level of protection that was essentially equivalent to that which was guaranteed by Articles 7 and 8 of the Charter. The High Court highlighted that EU citizens did not have the same remedies available to them as US citizens with regards to the processing of their personal data, since the Fourth Amendment to the Constitution of the United States did not apply to non-US citizens. This meant that it was particularly difficult for EU citizens to establish standing before a US court. Moreover, activities based on E.O. 12333 were not subject to judicial oversight and were not justiciable.

(viii) Given the considerable effects of US surveillance law on the rights of European citizens, the High Court raised the question of whether the SCCs are valid, given that they may not be binding on the State authority of the third country. If they did not bind the third country State authority, then they are not capable of remedying a possible lack of an adequate level of protection of personal data.

(ix) The High Court referred the following questions to the ECJ for a preliminary ruling:

- the applicability of EU law to data transfers made for commercial purposes, but further processed for national security and law enforcement purposes
- the relevant legislation for determining whether there has been a violation of individual rights
- how to assess the level of protection in a third country
- whether data transfers to the US violate the Charter
- whether the level of protection offered in the US respects or limits an individual's right to a judicial remedy
- what level of protection is required to be afforded to personal data that is transferred under SCCs
- whether the SCCs can even be adequate as safeguards given they do not bind national authorities
- whether there is an obligation to suspend data flows if a data importer is subject to surveillance law
- what is the relevance of the Privacy Shield decision is with regards to assessing safeguards

- whether the presence of an ombudsperson can ensure that the US provides an effective remedy to data subjects
- whether the SCCs violate the Charter

2.4 Highlights of Schrems-II Judgment:

The European Court of Justice in its composition of 13 Judges, rendered the judgment on 16th July 2020. This judgment has a significant impact on cross-border data transfer. The highlights of the ruling are:

(i) The Court began by clarifying that GDPR applies to transfer of personal data for commercial purposes by an economic operator established in a Member State, to another economic operator established in a third country, even if in that country the data would be processed by the national authorities for public security, defense, and state security purposes. In particular, the Court emphasised that a transfer of data is not excluded from the scope of the GDPR for the reason that it may be processed by the national authorities of a third country.

(ii) Regarding the level of protection required in such an instance, the Court held that the requirements presented by GDPR regarding safeguards, enforceable rights, and legal remedies must continue to be applied. In other words, when their data is transferred abroad, a data subject must be afforded a level of protection essentially equivalent to that which they would receive in EU. In such circumstances, in order to assess the level of protection, both existing contractual clauses between the data importer and exporter, and the potential access by public authorities in a third country must be taken into account, along with the relevant aspects of the legal system in the third country.

(iii) The Court then analyzed Decision 2016/1250 (the "Privacy Shield"), which was self-certification scheme in place for controllers based in the US. Examining the decision in light of the provisions of the Charter, the Court held that the requirements of US national security, public interest, and law enforcement do in fact interfere with the fundamental rights of persons whose data is transferred. These limitations on the protection of personal data were not circumscribed in a way that satisfied requirements that are essentially equivalent to those required under EU law. The principle of proportionality was also not satisfied, in so far as US surveillance programs are not limited to what is 'strictly necessary'. It was

noted that the provisions in the US surveillance programs neither limited the power they conferred onto national authorities, nor granted data subjects actionable rights before the courts against the US authorities.

(iv) The Court proceeded to scrutinize the Ombudsperson mechanism that had been in place under the Privacy Shield, stating that it too did not provide data subjects with a cause of action before a body which was fully independent, and that this body was limited in so far as it could not impose rules that were binding on US intelligence services.

Taking all of this into account, the Court declared the Privacy Shield Decision to therefore, be invalid.

(v) The Court also clarified that in the absence of an adequacy decision, the competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they consider that the standard data protection clauses are not or cannot be complied with in the third country, and that the protection of the data transferred cannot be ensured by other means.

(vi) **Re: SCCs:** Following such verdict on Privacy Shield, the Court then examined the validity of the SCCs (Decision 2010/87). In this regard:

- The Court held that validity of the Decision of SCCs was not called into question by the mere fact that the SCCs do not bind national authorities in a third country.
- The Court emphasized that the validity of the SCCs, however, did depend on whether there were effective mechanisms in place that make it possible to ensure compliance with the level of protection required by EU law.
- SCCs in themselves did provide for such mechanisms. However, it went on to stress that where these mechanisms cannot be complied with, the transfers of personal data pursuant to these clauses is to be suspended or prohibited.
- Furthermore, there is an obligation on the data exporter and the recipient of the data to verify prior to a transfer, what the level of protection in a third country is, and whether it will be possible to comply with the requirements of the SCCs.

Conclusively: By Schrems-II judgment, the Privacy Shield was invalidated and ECJ made some observations on SCCs. It is but obvious that the judgment created turbulence, once again causing EDPB to ponder over the subject.

2.5 Latest Recommendations by EDPB:

European Essential Guarantees For Surveillance Measures: On 10th November 2020, the European Data Protection Board adopted and issued Recommendations 02 of 2020.

EDPB noted that according to the CJEU, the protection of the right to privacy requires that derogations from and restrictions to the right to data protection *"must apply in so far as is strictly necessary"*. Furthermore, an objective of general interest must be reconciled with the fundamental rights affected by the measure, *"by properly balancing"* such objective against the rights at issue.[5]

Consequently, stipulated that access, retention and further use of personal data by public authorities within the remit of surveillance measures must not exceed the limits of what is strictly necessary, assessed in the light of the Charter, otherwise it "cannot be considered to be justified, within a democratic society".

With this background the in the said Recommendations, the EDPB prescribed the following **European Essential Guarantees,** intended to specify how to assess the level of interference with the fundamental rights to privacy and to data protection in the context of surveillance measures by public authorities in a third country, when transferring personal data. Also, it stipulated as to what legal requirements must consequently apply to evaluate whether such interferences would be acceptable under the Charter. Against each of the Guarantees, the highlights of respective Explanation as contained in Recommendations 02/2020 adopted by EDPB on 10th November 2020 is as follows:

(i) Guarantee A: Processing should be based on clear, precise and accessible rules:

Referring to Articles 8(2) and 52 (1) of the Charter:

- a justifiable interference needs to be in accordance with the law
- the legal basis should lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards
- the interference must be foreseeable as to its effect for the individual in order to give him/her adequate and effective protection against arbitrary

[5] CJEU, Privacy International, §68 and jurisprudence referred therein

interference and the risk of abuse. As a result, the processing must be based on a precise, clear but also accessible (i.e. public) legal basis

- it is essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure.

(ii) Guarantee B: Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated:

Referring to Article 52(1) of the Charter:

- As per the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must respect the essence of those rights and freedoms.
- Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
- Regarding the **principle of proportionality**, the question as to whether a limitation on the rights to privacy and to data protection may be justified must be assessed, on the one hand, by measuring the **seriousness of the interference** entailed by such a limitation and by verifying that the **importance of the public interest objective** pursued by that limitation in proportion to that seriousness, on the other hand.
- In Schrems II, CJEU has stressed that legislation of a third country which does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter.
- Regarding the **principle of necessity**, the CJEU has made clear that legislations "authorising, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public

authorities to the data and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to the data and its use entail", do not comply with that principle. In particular, laws permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.

- The CJEU held in La Quadrature du Net[6] and others, that "legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data retained and the objective pursued". In the same context, in Privacy International, it also held that the legislator "must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue[7]

(iii) Guarantee C: An independent oversight mechanism should exist:

- Interference takes place at the time of collection of the data, but also at the time the data is accessed by a public authority for further processing. The ECtHR has specified multiple times that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[8] (e.g. an administrative authority or a parliamentary body).
- The ECtHR specifies that while prior (judicial) authorization of surveillance measures is an important safeguard against arbitrariness, regard must also be given to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of actual abuse[9].
- As to the independence of oversight mechanisms in relation to surveillance, the findings of the CJEU concerning the independence of a body in the context of redress could be taken into account. The Court has expressed its preference for a judge to be responsible to maintain oversight. However, it is not excluded that another body may be responsible, "as long as it is

[6] La Quadrature du Net and others, § 133
[7] Privacy International, § 78
[8] ECtHR, Klass, §§17, 51
[9] ECtHR, Big Brother Watch under appeal §§319-320

sufficiently independent from the executive"[10] and "of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control"[11]

(iv) Guarantee D: Effective remedies need to be available to the individual:

Referring to Article 47 of the Charter:

- An individual must have an effective remedy to satisfy his/her rights when (s)he considers that they are not or have not been respected.
- Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article."[12]
- The question of an effective remedy is inextricably linked to the notification of a surveillance measure to the individual once the surveillance is over.
- In particular, the Court found that "there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications"[13].
- The parameters for independent redressal mechanism are: an independent and impartial body, which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers and that there is no evidential burden to be overcome in order to lodge an application with it[14].In undertaking its examination of

[10] 5ECtHR, Zakharov, §258, Iordachi and Others v. Moldova, §§ 40 and §§ 51 and Dumitru Popescu v. Romania, §§ 70-73.
[11] ECtHR, Klass §56 and Big Brother Watch under appeal §318
[12] CJEU, Schrems I, §95.
[13] ECtHR, Zakharov, §234
[14] ECtHR, Kennedy, § 190

complaints by individuals, the court should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance.

2.6 Conclusion:

The four EEGs are to be seen as the core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection. They should not be assessed independently, as they are closely interlinked with the relevant legislation in relation to surveillance measures, the minimum level of safeguards for the protection of the rights of the data subjects and the remedies provided under the national law of the third country.

These guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework. The assessment of the third country surveillance measures against the EEG may lead to two conclusions:

First: The third country legislation at issue does not ensure the EEG requirements: in this case, the third country legislation would not offer a level of protection essentially equivalent to that guaranteed within the EU.

Second: The third country legislation at issue satisfies the EEG.

When assessing the adequacy of the level of protection, pursuant to Article 45 GDPR, the Commission will have to evaluate whether the EEG are satisfied as part of the elements to be considered to guarantee that the third country legislation as a whole offers a level of protection essentially equivalent to that guaranteed within the EU.

When data exporters rely, along with the data importers, on appropriate safeguards under Article 46 of the GDPR, given the requirements of the third country legislation specifically applicable to the data transferred, they would need to ensure that an essentially equivalent level of protection is effectively achieved. In particular, where the law of the third country does not comply with the EEG requirements, this would imply to ensure that the law at stake will not impinge on the guarantees and safeguards surrounding the transfer, in order for a level of protection essentially equivalent to that guaranteed within the EU to be still provided.

The EDPB has issued further guidelines and recommendations to be taken into account to proceed with the assessment, depending on the transfer tool to be used and on the necessity to provide appropriate safeguards, including as the case may be, supplementary measures.

The EEGs have been said to be of referential standard when assessing the interference, entailed by third country surveillance measures, in the context of international data transfers. These standards stem from EU law and the jurisprudence of the CJEU and the ECtHR, which is binding on Member States.

*****

CHAPTER: III

CROSS-BORDER DATA TRANSFER & SURVEILLANCE: INDIAN LEGAL SPECTRUM

3.1 Indian Laws relating to Surveillance of Data:

Major provisions relating surveillance in India stem from substantive laws like (i) Indian Telegraph Act, 1885[15], (ii) Indian Telegraph Rules, 1951 (as amended from time to time), (iii) the Information Technology Act, 2000[16], (iv) Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009[17] (v) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[18] and (vi) Model Unified License Agreements between Government of India and Internet Service Providers (ISPs) and Telecom Service Providers (TSPs)**.**[19]

It is also pertinent to note here that there exist provisions in these legislations and instruments, whereby an officer of the Government (Central of State) can be authorized to intercept or monitor the computer system and data by issuance of an order from the competent authority.

3.1.1 Substantive Law Governing Surveillance in India

The definition[20] of word "telegraph" under Section 3(1AA) of the Indian Telegraph Act virtually covers any communication device, including telephones, within its purview. The definition is thus very wide and future-proof.

Section 5 of the Indian Telegraph Act, 1885 confers power on the Government of India to take possession of licensed telegraphs and to order interception of messages. Such interception can be ordered on the occurrence of any public emergency, or in the interest of the public safety. The Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public

[15] Text of the Indian Telegraph Act, 1885 can be found at: Indian Telegraph Act 1885 | Department of Telecommunications | Ministry of Communication | Government of India (dot.gov.in).
[16] Text of the Information Technology Act, 2000 can be found at: A2000-21.pdf (indiacode.nic.in)
[17] Text of these IT Rules, 2009 can be found at: Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.pdf (meity.gov.in)
[18] Text of these IT Rules, 2011 16 THE GAZETTE OF INDIA : EXTRAORDINARY [PART II-SEC (meity.gov.in)
[19] Copies of various model license agreements between Government of India and TSPs and ISPs can be found at: ISP License | Department of Telecommunications | Ministry of Communication | Government of India (dot.gov.in).
[20] 'telegraph' means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions,

safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under the said Act.

Further, on the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India or the security of the State or friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.

Said Section exempts press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall from interception or detention, unless their transmission has been prohibited under the said provision.

Thus, in exercise of the powers conferred under Section 5(2), surveillance on telephone networks may be exercised only in case of occurrence of a public emergency or in the interest of public safety. The terms 'public emergency' and 'public safety' are not defined under the Telegraph Act, but they were interpreted by the Supreme Court of India in the matter of *People's Union for Civil Liberties v. Union of India*[21] to mean '*the prevalence of a sudden condition or state of affairs affecting the people at large calling for immediate action' and* '*the state or condition of freedom from danger or risk for the people at large*' respectively. It is pertinent to note that the expressions 'sovereignty or integrity of India', 'security of the state', 'friendly relations with foreign states', 'public order' or 'prevention of incitement to the commission of any offense' are not defined under the Telegraph Act.

Section 69 of the IT Act, which is drafted in line with Section 5(2) of the Telegraph Act, allows the Government to engage in surveillance of Internet data, i. e., the actual data relating to content of the communication done through internet. Section 69 provides as under:

[21] Decided on 18.12.1996, reported in AIR 1997 SC 568.

69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource - *(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.*

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to–

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

It may be noted that Section 69 dispenses with the grounds found under Section 5(2), *viz.* the occurrence of a public emergency or interest of public safety. Interception, monitoring, and decryption of Internet data under Section 69 is not dependent on the prevalence of either conditions. This has widened avenues of the Government's surveillance on Internet data. It is also important to see that the grounds under Section 69, in the interest of which interception etc. of Internet data may be undertaken, are larger in number and are significantly greater in scope. This can be explained better by the comparative table given below: [22]

[22] Available at: India's surveillance state: Substantive legal framework | SFLC.in, Last seen 20.12.2020.

Section 5, Indian Telegraph Act	Section 69, Information Technology Act
Sovereignty/integrity of India	Sovereignty/integrity of India
Not provided	Defence of India
Security of the State	Security of the State
Friendly relations with foreign States	Friendly relations with foreign States
Public order	Public order
Prevention of incitement to the commission of any offence	Prevention of commission of any cognizable offence relating to the above
Not provided	Investigation of any offence

One of the most significant difference between these two sections is that unlike Section 5(2), Section 69 imposes an obligation on those from whom Internet data is demanded (Internet Service Providers, for instance) to provide all assistance to the intercepting agency. It also stipulates that failure to comply with this provision may result in imprisonment for up to *7 years* and fine.

Section 69B in turn deals with surveillance of Internet meta-data, i.e., the internet data *apart from its core-contents.* This includes information like date and time of transmission, duration for which data was transmitted and location from/to which data was transmitted. This section provides as under:

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security - *(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.*
(2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which any extend to three years and shall also be liable to fine.
Explanation - For the purposes of this section,
(i) computer contaminant|| shall have the meaning assigned to it in section 43;
(ii) traffic data means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.

Thus, Section 69B confers power upon Government to collect and monitor meta-data, which is termed as "traffic data". This data can be collected for the purposes of enhancing cyber security and tackling computer contaminants. The term "cyber security' is defined under Section 2(1)(nb) of the IT Act as "the protection of information or devices from unauthorized access, use, disclosure, disruption, modification or destruction." The term "computer contaminants" is defined in Section 43 of the IT Act. It means "malicious software such as computer viruses."

Thus, both these grounds for surveillance of meta-data under Section 69B are broad in ambit. The wording of Section 69B permits the Government to carry out surveillance of meta-data at any time.

3.1.2 Procedural Law Governing Surveillance in India

The *procedural* law regarding surveillance is found in **Rule 419A** of the **Indian Telegraph Rules, 1951.** Rule 419A was originally not part of the Telegraph Rules at the time of their notification in. It was incorporated by amendment in 2007. This amendment was a consequence of Supreme Court's decision in the case of *People's Union for Civil Liberties v. Union of India* (referred above). It this case, the Supreme Court had expressed its dissatisfaction about lack of procedure governing telephone tapping. In this case, the Supreme Court came up with guidelines to be followed while intercepting communications under Section 5(2). These guidelines played a role of procedure for interception since 1996 until 2007. Rule 419A was officially introduced to the Telegraph Rules, 1951, replacing the guidelines issued by the Supreme Court. [23]

As the procedure laid down by Rule 419A can be divided in two parts: (1) process for procurement and review of lawful order, and (2) process for interception.

[23] Available at: India's surveillance state: Procedural legal framework | SFLC.in, last seen 20.12.2020.

(a) Process for Procurement and Review of Lawful Order

A direction, i.e., a lawful order, for interception under Section 5(2) may be issued only by the Union Home Secretary at the Centre, or a State Home Secretary at the States. However, in *unavoidable circumstances,* a lawful order may be issued by an officer not below the rank of a Joint Secretary to the Government of India, who has been authorized by the Union/State Home Secretary to this effect.

The term 'unavoidable circumstances' is not defined under the Telegraph Rules, Telegraph Act, any other legislation, or any judgments by courts of law.

Rule 419A further states that in '*emergent cases',* where procuring a lawful order is not feasible, either due to remoteness of location, or for operational reasons, interception may be carried out with the prior approval (not a lawful order) of the head or the second senior most officer of the authorized law enforcement agency in case of Central Government, or officers authorized in this behalf - not below the rank of Inspector General of Police, in case of State Government.

Thus, under this exception, if it is not feasible to procure a lawful order for either of the listed reasons, the interception process may be commenced without a lawful order, which needs to be approved by a senior official of the intercepting agency. Rule 419A further provides that when interception is carried out in this fashion, the relevant sanctioning authority, i.e., the Union/State Home Secretary or a Joint Secretary, must be informed within 3 working days, and the lawful order must be procured within 7 working days.

It is also provided in Rule 419A that a lawful order may be issued only when all other reasonable means for acquiring the information have been considered and ruled out. Such order remains in force for a period of 60 days from the date of issuance, unless revoked earlier and it shall remain in force for a maximum period of 180 days.

It is required that a lawful order must contain, (i) reasons behind the order, (ii) name and designation of the authority to whom the intercepted information is to be disclosed, and (iii) a statement to the effect that the use of intercepted information will be subject to Section 5(2) of the Indian Telegraph Act, 1885.

It is also stipulated in Rule 419A that when a lawful order is issued, its copy must be forwarded within 7 working days to the respective Central/State Review Committee, which has been constituted by the Central/State Government under Rule 419A for the sole purpose of reviewing lawful orders. Such Review Committee, in case of Central Government, consists of the Cabinet Secretary as Chairman, and the Secretary (In-

charge, Legal Affairs) and the Secretary (Department of Telecommunications) as Members. A State Review Committee consists of the Chief Secretary as Chairman, and the Secretary (In-charge, Legal Affairs) and a Secretary (other than the Home Secretary) as Members. In cases where the Review Committee is of the opinion that a lawful order is violative of Section 5(2), it may set aside the order and ask that all copies of information intercepted under that particular order to be destroyed.

(b) Process for Interception

It is to be noted that ground-level interception of communications over telephones in India is carried out by various Law Enforcement Agencies, which are specifically authorized to this effect by the Government, but the identities of such agencies are not disclosed to the public for security reasons.

All intercepting agencies are required to designate one or more nodal officers to authenticate and process requisitions for interception between the law enforcement agencies and Telecommunications Service Providers ("TSPs"). A nodal officer is required to be not below the rank of Additional Superintendent of Police or equivalent. The TSPs are also required to designate two senior officials as nodal officers to receive and handle requisitions. Requisitions, including requisitions of lawful orders authorizing interception, are required to be delivered to nodal officers of the respective TSPs by officers not below the rank of Sub-Inspector of Police. Nodal officers of TSPs are bound to issue acknowledgement to the relevant intercepting agencies within 2 hours from receipt of requisition.

The Central Government periodically specifies the standard operating procedures for internal protocol to be followed by both intercepting agencies and TSPs in handling requisitions for interception. Such standard operating procedures are not open for the public for security reasons, thereby ensuring that none other than those directly involved in the interception process have a comprehensive idea of the end-to-end procedure. Applications filed under the Right to Information Act, 2005 for obtaining copies of such standard operating procedure may be denied, due to reasons that it prejudicially affects national security.

However, some procedural safeguards are laid down in Rule 419A for preventing misuse of intercepted information. Some the safeguards are that the officers authorized to intercept are required at all times to maintain (i) records that contain the intercepted information, (ii) particulars of persons or entities whose communication was intercepted, (iii) particulars of those to whom intercepted information has been disclosed, (iv) number of copies of intercepted information

created, (v) mode of creating said copies, (vi) date of destruction of said copies and (vii) duration for which the lawful order remained in force.

In view of the procedural safeguards under Rule 419A, TSPs are required to ensure (i) adequate and effective internal checks in order to ensure that unauthorized interception does not take place, (ii) that extreme secrecy is maintained, and (iii) that utmost care and precaution taken in the interception process. TSPs are responsible for the actions of their employees, and established violations of relevant license clauses may result in action being taken against TSPs under the Telegraph Act, which may extend to revocation of their licenses.

It is also important to note that all records pertaining to intercepted information are required to be destroyed by sanctioning authorities and intercepting agencies every 6 months unless they (likely) need to be retained for "functional requirements". Similarly, TSPs are required to destroy all such records within 2 months form cessation of interception and are required to maintain extreme secrecy in doing so.

As far as the procedure to be followed while invoking Sections 69 and 69B is concerned, it is laid down under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, and the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009. The procedure outlined by these Rules is an identical replication of the procedure under Rule 419A of the Telegraph Rules, 1885. Internet surveillance under these Rules framed under the IT Act is governed by the same broad procedural framework as under Rule 419A of the Telegraph Rules, 1951, as amended from time to time.

The discussion regarding procedural aspects of access to stored data cannot be complete without discussing Section 91 of the Code of Criminal Procedure, 1973 (“Cr.P.C.”), which states that a Court in India or any officer in charge of a police station may summon a person to produce any document or any other thing that is necessary for the purposes of any investigation, inquiry, trial or other proceeding under the Cr.P.C. This necessarily implies that law enforcement agencies in India can access stored data under Section 91 of the Cr.P.C. Section 92 of the Cr.P.C. confers powers on District Magistrates and Courts to issue directions requiring document, parcel or things within the custody of any postal or telegraph authority to be produced before it if needed for the purpose of any investigation, inquiry, trial or other proceeding under the Code. The expression ‘things’ mentioned in Section 92 covers data stored in computers.

3.1.3 Surveillance Measures under the Unified Licence Agreements:

The Department of Telecommunications (DoT) of the Ministry of Communications of the Government of India has issued license agreements with which Internet Service Providers (ISPs) and Telecom Service Providers (TSPs) operating in India need to comply. Such license agreements mandate the terms and conditions under which ISPs and TSPs in India can operate and in certain circumstances, ISPs and TSPs are required to carry out mass surveillance in order to be in compliance with these license agreements.

The Unified Access Service License (UASL), Internet Service License (ISL), and the Unified License (UL) which incorporates the former two licenses between the DoT and TSPs enable the Government to receive assistance from TSPs in conducting surveillance. It is mandatory on the TSPs to provide suitable monitoring equipment as per the requirement of the DoT or law enforcement agencies.

DoT has released a model unified license agreement and has thereby permitted telecom companies in India to offer services (mobile, fixed line, Internet, long-distance calls and other telecom services) through a single license. The model UASL Agreement has also been amended from time to time. There exist several provisions in UASL which provide strong safeguards for protection of subscriber data, prohibition of unlawful and mass surveillance and imposition of robust penalties. However, many other provisions of the UASL compel TSPs and ISPs to facilitate surveillance, either directly or indirectly.

Under the ISP License, the licensee is required to install the equipment that may be prescribed by the Government for monitoring purposes. The UASL requires the licensee to install the necessary hardware/software to enable the Government to monitor simultaneous calls. As per the ISP License, and the UASL, in case of remote access of information, the licensee is required to install suitable technical devices enabling the creation of a mirror image of the remote access information for monitoring purposes.

The UASL also requires service providers to disclose Call Data Records (‘CDR’) to law enforcement agencies.

3.1.4 Law Enforcement Agencies Authorized for Lawful Interception in India:

Following is the list of authorised law enforcement agencies for lawful interception:

(a) Central Agencies

1. Intelligence Bureau
2. Narcotics Control Bureau
3. Directorate of Enforcement
4. Central Board of Direct Taxes
5. Directorate of Revenue Intelligence
6. Central Bureau of Investigation
7. National Investigation Agency
8. Research & Analysis Wing (R&AW)
9. Directorate of Signal Intelligence, Ministry of Defence- for Jammu & Kashmir, North East & Assam Service Areas only

(b) State Agencies

1. Director General of Police, of concerned state
2. Commissioner of Police, Delhi for Delhi Metro City Service Area only.

3.2 View of the Supreme Court on Surveillance: Few Landmark cases:

The interpretations and judicial precedents work as an aid to find out how to effectively implement any legislation. The right balance between security and the privacy right in the context with the surveillance of electronic communications has always been struck by the Indian judiciary and the legislations.[24]

By interpreting Articles 19 and 21, Indian Judiciary has brought the right to privacy within the realm of fundamental rights. The judiciary has recognized right to privacy as a necessary ingredient of the right to life and personal liberty as envisaged under Article 21. Right to life has been interpreted by the Supreme Court to mean right to dignified life. It has also asserted right to privacy as a fundamental right, subject to some restrictions based on compelling public interest. As interpreted by the apex Court in its various judgments, privacy means different things to different people. Privacy can be called as a desire to be left alone and the ability to act freely.

The Indian Constitution provides a right to freedom of speech and expression,[25] which implies that a person is free to express his will about certain things. Freedom of life and personal liberty of a person can be taken away only by procedure established by

[24] Sourabh Vasant Ubale, Sthiti Dasgupta, *The Surveillance Of Electronic Communications vis-à-vis Right To Privacy,* the world journal of juristic polity, 2016 ISSN No. 2394-5044 Available at www.jurip.org, (Last seen on 12/12/2020).

[25] Constitution of India, Article 19 (1)(a).

law.[26] The privacy of a person is further secured from unreasonable arrests[27] and the person is entitled to profess and propagate any religion.[28] The privacy of property is also secured unless the law so authorises that a person cannot be deprived of his property unlawfully.[29] Article 21 ensures the protection of the right to privacy and it also promotes the dignity of the individual. Privacy relates to the ability to control dissemination and use of one's personal information.

In *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors.,* it has been recently held by the Supreme Court that the dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. The Supreme Court categorically held that informational privacy is a facet of the right to privacy. Thus, privacy and protection of one's data is an important facet of right to privacy, as guaranteed under Article 21 of the Constitution.

3.3 Evolution of Right to Privacy in India

Justice A.P. Shah, former Chief Justice of the Delhi High Court, in his report on privacy,[30] submitted to the Government of India on 16th October 2012, has enunciated a detailed account of evolution of judicial precedents in the arena of right to privacy in India. It would not be out of place, rather it is extremely pertinent to quote the same account of evolution of judicial interpretation and precedents as enunciated in Justice A.P. Shah's report.

"Right to privacy was first discussed by the Supreme Court in *Kharak Singh* v. *State of Uttar Pradesh*,[31] where a Supreme Court bench of six judges decided the constitutionality of regulations which granted the police the right to conduct domiciliary visits and surveillance of persons with a criminal record. The constitutionality of these regulations was challenged by the Petitioner on the grounds that the regulations violated his fundamental right to privacy as envisaged under the 'personal liberty' clause of Article 21. However, majority of the judges refused to interpret Article 21 to include right to privacy. It was stated by the majority that:

"The right of privacy is not a guaranteed right under our Constitution, and therefore the attempt to ascertain the movements of an individual is merely a manner in which

[26] Constitution of India, Article 21.

[27] Constitution of India, Article 22.

[28] Constitution of India, Article 25.

[29] Constitution of India, Article 300A.

[30] *Report of the Group of Experts on Privacy* (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court), Available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf, (Last seen on 12/12/2020).

[31] (1964) SCR (1) 332.

privacy is invaded and is not an infringement of a fundamental right guaranteed in Part III."

Nonetheless, the common law right of citizens to enjoy the liberty of their houses was recognized by the majority and it approved the age old saying that 'a man's home was his castle'. The Court held domiciliary visits to be unconstitutional. Minority of two judges held the right to privacy to be part of Article 21, which was perhaps its first recognition as a fundamental right. Justice Subba Rao held:

"It is true, our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."

Right to privacy was once again discussed in the case of *Gobind v. State of Madhya Pradesh.*[32] Certain police regulations were challenged by the Petitioner as being unconstitutional, on the grounds that they violated his fundamental right to privacy. 3 Judges hearing this case were inclined to hold right to privacy as a fundamental right. Justice Mathew stated:

"Rights and freedoms of citizens are set forth in the Constitution in order to guarantee that the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists. 'Liberty against government' a phrase coined by Professor Corwin expresses this idea forcefully. In this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy."

It was further caveated by the observation of the Court that right to privacy is not an absolute right and can be curtailed by the State if it succeeds to establish a "*compelling public interest*".

In *R. Rajagopal* v. *State of Tamil Nadu,*[33] the Supreme Court was required to view right to privacy in the context of freedom of speech. A Tamil newsmagazine, being the Petitioner, had sought relief to restrain the respondent State of Tamil Nadu to not interfere in the publication of the autobiography of a death row convict 'Auto Shankar'. The autobiography contained details about the nexus between criminals and police officers. The questions to be decided by the Supreme Court were:

"(a) Whether a citizen of this country can prevent another person from writing his life story or biography? (b) Does such unauthorized writing infringe the citizen's right to privacy? (c) Whether the freedom of press guaranteed by Article 19(1)(a) entitles the

[32] AIR 1975 SC 1378.

[33] 1994 SCC (6) 632.

press to publish such unauthorized account of a citizen's life and activities and if so, to what extent and under which circumstances?"

It was for the first time that in this case the Supreme Court directly linked the right to privacy to Article 21. However, the Court excluded the matters of public record from 'Right to Privacy'. It was held by the Court that:

"(1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, 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. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.

(2) The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. It is for this reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others."

The scope of a blood donor's right to privacy of his medical records was considered by the Supreme Court in the case of *Mr. 'X' v. Hospital 'Z'*.[34] In this case, the respondent hospital had disclosed without the permission of the blood donor that the donor was a HIV patient. This lead to the cancellation of the proposed marriage of the donor and he became a subject of social rejection. The Supreme Court held that while medical records are private, but doctors and hospitals may make exceptions in cases where the non-disclosure thereof is likely to endanger the lives of other citizens, e.g. the proposed wife of the blood donor.

The actions of the state intercepting telephone calls were in question the case of *People's Union for Civil Liberties* v. *Union of India*.[35] In this case, the Court set out procedural safeguards which are required to be followed. Though the Court did not strike down the provision relating to interception in the Telegraph Act, 1885, it observed as under:

[34] AIR 1999 SC 495.

[35] (1997) 1 SCC 30.

"Telephone-tapping is a serious invasion of an individual's privacy. It is no doubt correct that every government, howsoever democratic, exercises some degree of supervisory operation as a part of its intelligence outfit, but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."

The Supreme Court, while ordering the creation of a 'review committee' for reviewing the surveillance measures authorized under the Act, imposed restrictions on the officers of State who could authorize such surveillance.

One of the most significant judgment on right to privacy came to be passed by the Supreme Court in the case of *District Registrar v. Canara Bank*.[36] The constitutionality of a provision of the A.P. Stamps Act was tested in this case. The impugned provision conferred rights on certain officers of the State to enter any premises to conduct an inspection of any records, registers, books, documents in the custody of any public officer, in cases of fraud or omission of any duty payable to the Government. Privacy of a customer's records stored by a financial institution such as a bank was a critical issue in this case.

The Supreme Court held the impugned provision unconstitutional on the ground that it failed the tests of reasonableness as contained in Articles 14, 19 and 21 of the Constitution. The Court observed that any legislation intruding on the personal liberty of a citizen, e.g., the privacy of a citizen's financial records, must satisfy the triple test laid down by the Supreme Court in the case of *Maneka Gandhi* v. *Union of India.*[37] The triple test laid down in *Maneka Gandhi* makes it necessary for the law intruding on 'personal liberty' under Art. 21, to meet three standards: (i) it must prescribe a procedure; (ii) the procedure must withstand the test of one or more of the fundamental rights conferred under Article 19, which may be applicable in a given situation; and (iii) it must also be liable to be tested with reference to Article 14. It was held that the impugned provision failed this triple test. The Court also held that the concept of privacy related to the citizen and not the place. It is not important that the financial records were stored in a citizen's home or in a bank. It was further held that as long as the financial records in question belonged to a citizen, those records must be protected under the citizen's right to privacy.

[36] (2005) 1 SCC 496.

[37] AIR 1978 SC 597.

The question of de-criminalizing a class of sexual relations between consenting adults was considered by the Delhi High Court in the case of *Naz Foundation v. Union of India.*[38] The Court 'read down' Section 377 of the Indian Penal Code, 1860 for this purpose. The Court accepted the argument that the right to privacy of a citizen's sexual relations, under Article 21, can be intruded by the State only if the State succeeds to establish a compelling interest for such intrusion. Since the State was unable to prove such compelling interest, the provision was read down to decriminalize all consensual sexual relations.

This decision of Delhi High court was overruled by a two judges bench of the Supreme Court comprising of Justice G.S. Singhvi, and Justice S. J. Mukhopadhaya on 11th December 2013 in the case of *Suresh Kumar Koushal v. Naz Foundation,*[39] stating that "Section 377 of the IPC does not suffer from the vice of unconstitutionality and the declaration made by the Division Bench of the High court is legally unsustainable." However this decision of the apex Court was overturned by the a five judges bench of the Supreme Court in *Navtej Singh Johar v. Union of India* on 6th September 2018. The Court held that:

"Insofar as Section 377 criminalises 51 consensual sexual acts of adults (i.e. persons above the age of 18 years who are competent to consent) in private, is violative of Articles 14, 15, 19, and 21 of the Constitution. It is, however, clarified that such consent must be free consent, which is completely voluntary in nature, and devoid of any duress or coercion"

It was held by the Supreme Court in *Selvi* v. *State of Karnataka*[40] that narcoanalysis, lie-detection and BEAP tests in an involuntary manner violate prescribed boundaries of privacy. Dilution of constitutional rights cannot be justified by medical examination. The Court may exercise the dissector of medical examination of a person in cases where DNA test is eminently needed to reach the truth.

In *Sarda v. Dharmpal,*[41] the Supreme Court held that right to personal liberty cannot be treated as an absolute right, though it has been read into Article 21. To enable the Court to arrive at a just conclusion, a person could be subjected to a medical test even though it would invade his right to privacy. The Court concluded that a balance is required to be maintained between the rights of a citizen and the right to privacy. A

[38] WP No. 7555 of 2011, Delhi High Court.

[39] (2014) 1 SCC 1.

[40] (2010) 8 SCC 633.

[41] AIR 2003 SC 3450.

healthy and congenial relationship between the social good and the individual liberty needs to be achieved."

Shreya Singhal v. Union of India[42] is a landmark case which plays a very important role in the process of evolution of information technology law of India. In this case, the apex Court discussed the fundamental right of freedom of speech and expression under Article 19(1)(a) of the Constitution of India. The constitutional validity of section 66A[43] of the Information Technology Act 2000, which provided for punishment for sending offensive messages through communication services, etc was challenged in this case. The verdict in this case is immensely important in the Supreme Court's history for many reasons. The Supreme Court adopted the extreme step of declaring a censorship law passed by Parliament as altogether illegitimate. The Judgment increased the scope of the right of Indian citizens to express freely, and restricted the space given to the State in restraining this freedom only in the most exceptional circumstances. Justice Nariman while delivering this landmark judgement, wrote that:

"The liberty of thought and expression is not merely an aspirational ideal. It is also a cardinal value that is of paramount significance under our constitutional scheme. None of the grounds contained in Section 19(2) were capable of being invoked as legitimate defences to the validity of Section 66A of the IT Act. Any law seeking to impose a restriction on the freedom of speech can only pass muster, if it is proximately related to any of the eight subject matters set out in Article 19(2) and must pass two tests (a) clear and present danger and (b) the probability of inciting hatred."

After dealing with the evolution of right to privacy through judicial decisions in India, it is necessary to see how right to Informational privacy, i.e., data protection has been perceived by the judiciary.

---

[42] Writ Petition (Criminal) No.167 of 2012 Supreme Court of India, reported in AIR 2015 SC 1523.

[43] Section *66A. Punishment for sending offensive messages through communication service, etc:*

Any person who sends, by means of a computer resource or a communication device,

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation - For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

3.4 Data Protection - a Reflection of Privacy

On 24 August 2017, the Supreme Court passed a landmark judgment on the constitutional validity of privacy. In *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.*, the apex Court upheld the validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.[44] The Aadhaar Act was held to be constitutional to the extent it allowed for Aadhaar number-based authentication for establishing the identity of an individual for receipt of a subsidy, benefit or service given by the Central or State Government funded from the Consolidated Fund of India. However, the Supreme Court disallowed the use of individual Aadhaar numbers by any private entities for establishing the identity of the individual concerned for any purpose pursuant to a contract, on the basis that it was contrary to the fundamental right to privacy. The Supreme Court also ruled on a number of laws, circulars and directions, which required the mandatory linking of Aadhaar for receiving relevant services. In January 2017, the five-judge Constitutional bench of the Supreme Court of India reserved its judgement on the interim relief sought by petitions to extend the deadline making Aadhaar mandatory for everything from bank accounts to mobile services.

On 26th September 2018, the Supreme Court declared Aadhaar scheme of Government of India as constitutionally valid and said that Aadhaar is meant to help benefits reach the marginalized sections of the society and takes into account the dignity of people from personal and community point of view. It was opined by the Supreme Court that the Aadhaar is serving much bigger public interest and it means unique, and it is better to be unique than being best. The nine-judge bench unanimously held that:

"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

Hon'ble Mr. Justice D.Y. Chandrachud[45] clearly held:

"Para 459 (A) Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the

[44] Act No. 18 of 2016.

[45] Hon'ble Mr. Justice D.Y. Chandrachud wrote the judgment on his own behalf and on behalf of Hon'ble Mr. Justices J.S. Khehar, R.K. Agrawal and S. Abdul Nazeer.

Indian Constitution; … (C) Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III; …(F) Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being; …(H) Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them; and (I) Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual."

The Hon'ble Supreme Court rejected the arguments of the Union of India, and while analysing the nature of right of privacy as regards its origin, the Hon'ble Supreme Court held that the right to privacy is intrinsic to and inseparable from human element in human being and core of human dignity. Thus, it was held that privacy has both positive and negative content. The negative content acts as an embargo on the State from committing an intrusion upon the life and personal liberty of a citizen and its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual. Therefore, the Constitutional protection of privacy may give rise to two inter-related protections i.e. (i) against world at large, to

be respected by all including State: right to choose that what personal information is to be released into the public space (ii) against the State: as necessary concomitant of democratic values, limited government and limitation on power of State.

As a result of this judgment the right to privacy has become 'more than mere common law right' and 'more robust and sacrosanct' than just any statutory right. Thus, now in the context of Article 21 of the Constitution of India, an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable.

Indian judiciary has adopted vertical as well as horizontal approach to the fundamental rights embodied in the Constitution of India. Horizontal approach tends to generalise the perspective towards fundamental rights by assuming that all fundamental rights have a similar purpose and design. As against this "all or nothing" approach, vertical approach tends to establish that it is only in situations where there is "State action" that fundamental rights can conceivably apply. They borrow the underlying theme of classical liberalism in emphasising the preservation of the private sphere against coercive State intrusion. According to the vertical approach, the society's ultimate goal is to maximise private space in which individuals will be free to pursue their own conceptions of good.[46]

3.5 Conclusion:

Thus, the privacy of personal data and information of individuals was discussed at length in the judgment, thereby considering all facets of this right. It is for the first time in this case, that informational privacy was included within the ambit of right to privacy as enshrined under Article 21 of the Constitution. The concept of data protection was also recognized to be an inseparable part of right to informational privacy by the Supreme Court. The Court, demonstrating its innovative approach, emphasized the need for a separate and robust legislation governing protection of data in India.

Hence, the Indian surveillance law spectrum is covered under the views of the Supreme Court and the State, i.e., Central or State Government are required to follow the procedure established by law and they are required to ensure that they do not encroach upon the right to privacy of an individual, while carrying out surveillance activities.

[46] Murray Hunt, *"The Horizontal Effect of the HRA"*, (1998) PL 423 at 424.

CHAPTER: IV

BUSINESS CONTRACTS AIMED AT DATA IMPORT TO INDIA

4.1 Introduction:

When data is imported into India from any country, more often than not, the data importer based in India acts as a data processor. The data exporter in such a scenario shall be the data fiduciary or data controller. The reason is that the data importer based in India when processing and using the data has to generally process the imported data in accordance with the data exporter`s instructions. Cloud computing or software and service model (SaaS) providers are typically data processors. Section 37 of the current draft of the Indian Personal Data Protection Bill, 2019 ("**PDPB**") provides that an exemption may be granted, by the Central Government of India, from the application of the PDPB in case the data, that is being imported to India for processing is that of non-residents. This of course is to address the issue of applicability of multiple national data protection laws to the same set of data.

On the other hand, if the data importer is empowered to determine the purposes for which the data is to be used or to decide on the main means of data processing (for example B storage time or third-party access rights), the data importer is considered responsible for the data and then wears the hat of a data fiduciary or data controller.

Applicable stamp duty will have to be paid as per Indian stamp laws on the agreement.

When data exporters are negotiating contracts aimed at importing data in India, there are a few clauses that need to be thought of carefully about.

4.2 Material covenants and representations & warranties:

4.2.1 Obligations of the importer: Here we will have to expand on clauses that cover exhaustively the obligations of the importer such as:

- The processing of personal data will be carried out in accordance with the relevant provisions of all the applicable data protection laws and in accordance with the instructions of the data importer.
- Sufficient guarantees covering the security obligation of the data exporter and sufficiency of the security processes and tools.

- Clauses around any special category of data depending on which country residents' data is going to be transferred.
- No further transfer of data without consent whether in India or outside. Covenants on sub-processing.
- All obligations like producing information to data principals etc. will be undertaken by the data importer in accordance with all the applicable data protection laws
- Laws of India or any other applicable legislations are not such that defeat the implementation of the data protection laws applicable to the data being imported or this contract. In case of any change in law in such a manner that the aforesaid ceases to be true, will promptly notify the data exporter.
- Cooperation with the relevant data protection authorities which regulate the exported data.
- Any unauthorized access or data breach will be quickly notified to the data exporter and will comply with the data breach laws applicable to the exported data.
- Will respond to all enquiries of the data exporter and will comply with all procedural requirements including data audit etc. as required under the laws applicable to the exported data.
- Cost of the above (depends on whether parties decide for it to be on actuals or is factored in the cost of the contract).

4.2.2 **Obligations of the exporter:** Here we will have to expand on clauses that cover exhaustively the obligations of the exporter such as:

- The processing (including the transfer) by the data exporter is in accordance with the applicable data protection laws.
- The instructions of processing to the data importer shall always comply with the applicable data protection laws.
- Sufficiency of security process and tools during transfer.

4.3 Liability and Indemnity:

Liability:

Any data principal who has suffered loss due to a breach by the data exporter or data importer shall have recourse to both the data exporter or data importer respectively. However, a back to back indemnity may be entered into by the data exporter from the data importer, in case the breach takes place due to a default in the data importers system.

Indemnity:

The parties should agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. The parties should also specifically agree upon the party who will bear the financial consequences if the government or the regulatory body or a party to the contract acts in a manner that is contradictory to the contractual clauses in the agreement between the data importer and exporter. Further it should also be agreed as to who will bear the risk in case the government, any regulatory body or a party acts in breach of the Indian surveillance laws.

Of course, caps in terms of the indemnity amounts and time period could be considered by the parties and built into the documentation. A de-minimus should also be agreed so that the nuisance of seeking indemnity can be avoided in case of small claim amounts.

4.4 Dispute Resolution:

The following methods of dispute resolution are available for any resolution of disputes between the data exporter and data importer:

A. Conciliation
B. Mediation
C. Arbitration
D. Court led dispute resolution

A dispute arising out of an agreement between a data exporter and Indian data importer may be governed by the laws and jurisdiction of the country whose resident's data is mostly the subject-matter of transfer. However, as is the case with almost every country around the globe, enforcing a foreign judgements or awards is a contentious issue in India as well.

<u>Conciliation and Mediation:</u>

The only mediation and conciliation agreements that are directly enforceable in India as arbitral awards are those that are entered into after the arbitration has been initiated. There is no law in India, for enforceability of mediation and conciliation agreements arising out of private mediation or conciliation proceedings and therefore the recourse available is to sue for breach of contract should a dispute arise from them. This should be kept in mind when drafting these clauses in the agreement.

Arbitration Award:

India is a signatory to the New York Convention as well as the Geneva Convention relating to foreign arbitral award. Therefore, if a party receives a binding award from a country which is a signatory to either of these conventions and the award is made by a country which is notified as a convention country in India (which is a sizeable number), the award can be enforced by filing a ln execution petition. The court will determine if the award meets the requirement of the Civil Procedure Code, 1908 (CPC) and if so, will enforce it in a manner a decree by an Indian court is enforced.

Judgements/ Decrees by Courts:

As per the CPC, a foreign judgement is directly enforceable only if the judgement comes from a reciprocating country. Currently India recognises 10 countries as reciprocating countries. These are UAE, UK, Fiji, Singapore, Malaysia, Trinidad & Tobago, New Zealand, Hong Kong, Papua and New Guinea and Bangladesh. Therefore, in case a judgement passed by the courts of the aforesaid nations is in issue, directly execution proceedings have to be filed in India alongwith a certified copy of the decree. After verification that the decree is not hit by any grounds set out in Section 13 of the CPC (such as it is passed by a court of competent jurisdiction, is not obtained by fraud etc), an execution decree is passed.

The issue of enforceability of a foreign judgement from a non-reciprocating country against the Indian data importer in India is a challenge. A foreign judgement from a non-reciprocating country can only be enforced by filing a suit upon the judgement. The judgement holder is left with the option to either sue on the basis of the foreign judgement or on the original cause if action in the domestic court or both. It is the resultant decree by the domestic court which will finally be executed in India. This makes the process very cumbersome. Therefore, if possible, the jurisdiction of the contract between a data exporter and an Indian data importer should be if possible should be a reciprocating country to India or India.

*****

.

CHAPTER: V

EMPLOYMENT MATTERS & CORPORATE GOVERNANCE

5.1 Employee Surveillance:

Employers resort to surveillance of premises for security reasons. In some places, depending on the requirements, employers tend to place CCTV cameras on the work floor too.

With the advent of technology, the physical workplace has moved to an online environment and employers have to mitigate a new set of threats, to prevent attacks by viruses, trojans, malwares, ransomwares, scammers and so on. Installation of cookies, anti virus software, tracking software and such other software is a protective mechanism, but also effectively results in surveillance of the employees' activities online.

Often, employers would like to retain the right to monitor and audit company assets and their use (internet, mobile, laptop etc), including the right to review / search devices as part of audits or investigations.

With increasing requirements to allow employees to work from home, many IT companies are being asked to place more physical security safeguards as an alternative to a highly secure paperless office environment. Many companies therefore resort to webcams or biometric driven software tools that can identify persons, record their biometric data, and could potentially intrude into employees' home environment.

All or any of the above could lead to the company inadvertently collecting or accessing personal or sensitive data of the employee or any other third party, and even potentially accessing information or data that may amount to a crime that may be required to be reported to the authorities.

This will have to be dealt with as set out under Section 43 A[47] of the Information Technology Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[48]. Following requirements will have to be met by the employers:

[47] Full text of Sec 43 A of the Information Technology Act, 2000 with its amendments can be accessed at https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf

[48] the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 can be accessed at

(i) Companies are required to maintain a policy for privacy and disclosure of information, including sensitive personal data or information and ensure that the same are available for viewing by such providers of information. Such policy is also required to be published on the website of the body corporate.

(ii) The employer should also obtain written consent prior to obtaining and processing any sensitive personal data or information regarding purpose of usage before collection of such information.

(iii) A body corporate or any person on its behalf is not permitted to collect sensitive personal data or information unless — (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and (b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(iv) While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of — (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.

(v) The body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(vi) The information collected shall be used for the purpose for which it has been collected.

Typical retention period for surveillance data, such as CCTV footage could range to 30 or 60 days, with the fresh data overwriting the old data on the hard disk. Screen grabs or videos from webcams monitoring the employees too may be retained for a similar term. However, the Company should maintain a process and policy to be able to extract any part of the footage to be retained for a longer period, in case of a legal hold issued on such footage.

5.2 Oversight by Board of Directors:

https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf and clarifications at https://www.meity.gov.in/writereaddata/files/PressNote_25811.pdf

The Board of any Company who directly or indirectly collects, processes or transfers personal data needs to be aware of the security and privacy risks that come with such any kind of surveillance activity carried out by the Company.

Such risks are usually identified when a Data Privacy Impact Assessment (DPIA) is performed, which is currently not mandatory under the law. However, the Board must be made aware of the key risks that the Company is assuming, as part of such activity, and be sensitised and made aware of the potential penalties and fines that could accrue to the company or to individual officers, in the event of any breach. It is expected that the new Personal Data Protection Bill, once passed may mandate companies to conduct a Data Privacy Impact Assessment, for information that the companies control or process.

Under Section 134 (3) of the Indian Companies Act, 2013[49] all Companies are required to publish a statement indicating development and implementation of a risk management policy for the company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company, along with its annual accounts. Usually, such risk management policy and review would include Information Security and Privacy related risks. However, the extent of the Board's involvement and level of risk that the company will be willing to take will vary from company to company, depending on the company's business, financial strength, management vision, customer requirements and such other factors. Companies in banking, insurance, finance and healthcare will have to also comply with the sector specific laws, in addition to the above. Section 177 (4) of the Companies Act, 2013 requires all public companies (both listed and unlisted) to constitute an Audit Committee, which is required to evaluate, inter alia, the Risk Management System of the Company. Schedule IV of the Companies Act, 2013 also requires public companies to appoint Independent Directors who are also required to satisfy themselves on the integrity of the Risk Management System, among others. Clause 49[50] of the Listing Agreement (applicable to companies listed on Indian stock exchanges) provides for the company to lay down a procedure to inform the Board Members about risk assessment and minimization procedures. The Securities and Exchange Board of India (SEBI) prescribes constituting a Risk Management Committee and this committee will be responsible to oversee the Enterprise Risk Management program adopted by the Company. Companies may adopt the COSO Framework for Risk Management (Committee of Sponsoring Organizations of the Treadway Commission) to ensure it

[49] Full text of the Indian Companies Act, 2013 can be accessed at: https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

[50] Full text of Clause 49 can be accessed at: https://www.sebi.gov.in/sebi_data/commondocs/cir2803an1_p.pdf

has identified various risks, including the risks associated with employee or vendor or third party surveillance that may be carried by the Company, and to consider how the threats posed by such risks are duly mitigated, and reported to the Board on a regular basis. Depending on the risks involved and the risk taking appetite of the Company, the Board may consider regular internal testing or third party audits or certification to suitable standards such as ISO 27001 by the Company, as may apply to the business and operations of the Company.

Under the current Indian regulatory regime, there is no requirement to appoint a DPO. However, certain companies may be required to appoint a DPO under the new data privacy regime expected to be unveiled in India in the course of the year.

A company that collects, processes, stores or otherwise deals with any kind of surveillance data should also consider the nature of the data / information to determine the risks associated with storing, collecting and processing such data. Regulatory authorities could potentially get a warrant issued for information that may be relevant to any case or ongoing investigation and the Company will have to disclose such information to such authority(ies), as may be required.

*****

CHAPTER: VI

SUGGESTIONS TO MAKE CHANGES IN INDIAN SURVEILLANCE LAWS

6.1 Information Technology Act, 2000

Section 44: This section imposes penalties on anyone who fails to provide requested information to authorities. The section should be amended to include the legal specifications of the requested information, so that its abuse may be limited.

Section 67C: This section requires the retention of data, but does not specify its period, should be amended to specify the data retention period.

Section 69: The Information Technology (Amendment) Act, 2008, removed the preconditions of "public emergency" and "public safety" for interception and monitoring from Section 69, and expanded the power of the Government to order the interception of communications for the "investigation of any offense". This is a very wide power and is open for abuse by investigating agencies.

Hence, it should be made mandatory on the law enforcement agencies to bring documentary evidence to court and obtain a warrant for interception or monitoring of communications, so as to comply with the principles of legality, legitimate aim, necessity, adequacy and proportionality.

Clause (4) of Section 69 and Rule 25(5) of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which provide punishment for not providing access to Government agencies, for interception and monitoring should be amended in such manner that it should protect the individual from unjustified harassment and respect right to privacy.

Section 80: This section confers powers on the investigating officers to conduct searches and seize suspects in public places without a warrant. The conditions under which suspects can be seized in public places should be listed in this section. It is also necessary that a judicial warrant should be necessary such cases.

6.2 License Agreements:

6.2.1 ISP License Agreement

Clause 2.2 of the ISP License Agreement prohibits bulk encryption, as well as encryption that exceeds 40 bits in symmetric key algorithms. This section further

provides that users can use encryption over 40 bits only if they have acquired written permission from the service provider and disclosed their private encryption keys. It is to be noted that encryption below 40 bits in symmetric key algorithms is extremely limited. The requirement to disclose their private encryption keys in order to legally gain permission to use encryption exceeding 40 bits in symmetric key algorithms deprives individuals from their right to online anonymity, right to privacy and freedom of expression.

On the other hand, the Reserve Bank of India Guidelines on Internet Banking require banks to use a minimum of 128 bit SSL encryption. This is apparently violative of the terms of the ISP License. Therefore, it is suggested that bulk encryption should be allowed and encryption exceeding 40 bits in symmetric key algorithms should be permitted under this clause. Even the requirement for users to disclose their private encryption keys to service providers should be done away with.

6.2.2 CMTS License Agreement

Clause 22.2 of the Cellular Mobile Telephone Service (CMTS) License Agreement requires the installation of "necessary facilities" to aid the interception of messages by service providers. However, it remains unclear what "necessary facilities" constitute, as well as what type of monitoring equipment would generally be used for such purposes. Types of such equipment and purpose of installation should be legally specified in the "necessary facilities", to curb their abuse.

6.2.3 UAS License Agreement

Cause 41.10 of the UAS License Agreement requires data to be automatically transmitted from service providers to the Central Monitoring System (CMS) through MPLS connectivity. Bypassing service providers and enabling the automatic transmission of data to the CMS, creates a centralised point for cyber-attacks. Hence this clause needs reconsideration.

*****