A CONTEMPORARY VIEW ON DATA BREACHES & DATA PROTECTION LAWS

Written by ***Ms. Akshay Pathak***

Chief Manager - Legal, Airtel Payments Bank Limited, India

INTRODUCTION

In this digital age of technologically advanced business world, where the concept of *'consumer is the king'* is emerging fast - not literally to treat consumer as the king - but acknowledging the value of data rich consumers to economically make companies proposer. The idea is to monetise the data which the consumers bring within the reach of the entities and who with the help of this data, enrich their business profitability and saleability. Both, the consumer and the companies, relish the relationship - where consumer enjoy the services and companies love expanding their revenue. All goes smooth until there comes a breach of data privacy of individual. The prominent examples of social networking companies like Facebook, Whatsapp or Twitter are the evident business models where the business is driven majorly on data of users, be it their personal details, photographs, whereabouts and working capacities - which often goes on to store and analysis their psychological data and political opinions too. While talking about technology, 'Artificial Intelligence' cannot be left behind of the newest technology to apply intelligence on the data feeds through machines. Certainly, it has proven to be the big boon for corporates to understand the patterns of consumers, their likings, dis-likings and so on to pitch their product or services. However, this comes with a flip side - when the issues of unauthorised data access and storage beam up and it infringes upon the fundamental right of privacy. The playful picture of kids, innocently playing around with their virtual friends 'Alexa' and 'Siri' when they aren't as mindful that the companies behind these intelligent friends, are actually recording and storing all the activities and conversation happening around them.

Presently, we are witnessing massive increase in the volume of data processed, stored or transferred across networks, cloud platforms, systems, users, or organisations dealing in digital market space beyond boundaries. This illuminating side of usage of data has, on a counter side, resulted in a huge upsurge in misuse of data and then mounting data security and privacy issues due to unauthorised access to such data by fraudulent networks and cyber attackers with their innovative methods evolving each passing day, of course with the help of very own technology. To address this alarming issue, many countries have enacted or in the process of enacting appropriate data privacy law that is to keep up to date with technological advancements and ever budding threats to data and information security. The latent risks of digital markets call for an effective statuary and regulatory regime on data protection.

The Internet has revolutionized and improved the way we live from using basic services such as email, social networking and online searches that enable us to communicate, socialize and access information in novel ways, from buying household items and groceries, to the stretch of managing finances and making investments. Everything is now available at the touch of your finger. Companies may engage in such data practices that are misaligned with consumer's expectations and this conflict between user expectations and data practices of companies may result in concerns regarding violation of data privacy. Today, all the industries from financial, telecom, education to healthcare, have adopted the digitisation of their services and keeping data records in a digital format. Health services are currently experiencing a growth in the total volume of data with regards to density, multiplicity and accuracy. However, issues such as patients' confidentiality and privacy have also become major challenges, where healthcare organisations are experiencing data breaches in recent years.

The regulatory model characterised by individualised consent and the necessity test, though a powerful mean, remains insufficient in fully protecting data. There is, thus, a pressing need for policymakers to review their regulatory toolbox in light of the potential threats. On the one hand, it is necessary to reconsider the possibilities to blacklist or whitelist certain data uses with mechanisms that are either in place in the legal framework or can be introduced additionally. On the other hand, it is crucial to realise the all range of policy options that can

be adopted to assist individuals in making informed decisions in the age of globalisation and data flow with no barriers.

Nowadays, millions of people are generating electronic transaction histories and becoming 'data-rich' at momentous rates, even before becoming financially rich or stable. Personal data benefits individuals in informing and building much needed trust with crucial institutions providing necessitated services, such as hospitals, banks, or potential employers. Opportunities in health markets, careers, and urban data have become more pressing in a post COVID word.

As per statistics, India has now over 687 million internet subscribers which is the second largest number in the world, an increase of 300% in just five years. Similarly, the number of mobile users has also seen a parallel pattern where India has 1.2 billion mobile connections, with about 600 million unique users - almost twice the number of 349 million unique users five years ago. If we look at the financial inclusion of customers in India, at least 647 million individuals have a formal bank account. According to the figure estimation released by World Bank, over half the total accounts opened in the entire world between 2014-2017 were opened in India.

THE DATA SECURITY BREACHES - SOME EYE-OPENER FACT

A global wave of cyberattacks and data breaches began in January 2021 after *zero-day exploits* were discovered in on-premises Microsoft Exchange Servers, giving attackers full access to user emails and passwords on affected servers, administrator privileges on the server, and access to connected devices on the same network. Attackers typically install a backdoor that allows the attacker full access to impacted servers even if the server is later updated to no longer be vulnerable to the original exploits. It was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom. Microsoft announced the discovery of '*a new family of ransomware'* being deployed to servers initially infected, encrypting all files, making the server inoperable and demanding payment to reverse the damage and publicised that in 92% of Exchange servers the exploit has been either patched or mitigated.[i]

As per news reports, some of the latest glaring cyber-attacks in India which presents a worrisome picture are:

Latest in row being, when Air India has suffered a major data breach caused by a "sophisticated cyberattack" affecting nearly 45 lakh people worldwide. The leaked data was collected between August 26, 2011 and February 20, 2021 and included people's personal details like name, date of birth, contact information, passport information, ticket details and credit card data.

Covid-19 lab test results of thousands of Indian patients including patients' full names, dates of birth, testing dates and test centers, have been leaked online in January 2021. It is worth noting that the leaked data hasn't been put up for sale on dark web, but was publicly accessible owing to Google indexing Covid-19 lab test reports.

In February 2021, personal identifiable information of 500,000 Indian police personnel was put up for sale on a database sharing forum due to cyber security lacks.

In April 2021, a hacker delivers 180 million Domino's India pizza orders to dark web for sale, by taking benefit of an information security incident.

Recently, Justdial – a company that provides local search options for different services – suffered a massive data breach in which user data was exposed. The leaked data included details such as names, email accounts, numbers, addresses and gender.

In 2018, a number of malicious Android apps posing as the popular game Fortnite were released; when users downloaded them, malware was installed on their smartphones, which retrieved users' calls, message logs, and contact information without their knowledge.

In 2017, food aggregator Zomato suffered a major data theft in which names, email IDs and hashed passwords of 17 million users were hacked and misappropriated. To add on, the Petya

Ransomware attack affected the container handling functions at a terminal operated by AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust.

In 2019, there was a cyber-attack on the Kudankulam Nuclear Power Plant in which a malware infection was identified on its network system containing administrative data activities.

In 2016, an employee of Union Bank of India received a phishing email that enabled hackers to gain administrator-level access to the bank's network, execute fund transfers and defraud the bank of $171 million.

According to the Indian Computer Emergency Response Team (CERT-In), the government agency responsible for tracking and responding to cybersecurity threats, in the year 2019 alone, over 313,000 cybersecurity incidents were reported.

The latest issues on updated privacy policy of Whatsapp, a message enabling app, has also beings into light the concerns around privacy of data. WhatsApp's upgraded privacy policy indicates it will share commercial user data with parent company Facebook. The update amended the way WhatsApp processes user data, how businesses can use Facebook (WhatsApp's parent) hosted services to store and manage WhatsApp chats, and how WhatsApp and Facebook intend to integrate their products. Several clauses of the revised privacy policy – such as storing media messages, automatic collection of information, sharing information with Facebook and third-party businesses and service providers – did not go down well with the masses and governments alike, leading to immediate and widespread backlash. Users were not comfortable with sharing information with Facebook without their authorisation, given its previous record in handling users' data. A petition was filed before the Delhi High Court arguing that removing the privacy of WhatsApp users' information and exchanging it with Facebook was in violation of users' basic freedoms guaranteed by Article 21 of the Constitution of India. While deciding on the situation, the Delhi High Court instructed that if users opt to delete the WhatsApp account entirely, WhatsApp will have to delete user data entirely from its servers and refrain from exchanging user data with Facebook, and as far as users who choose to stay in WhatsApp are concerned, the current information/ data/ details of such users will not

be communicated. The court also instructed the government to consider whether bringing messaging applications such as WhatsApp under some statutory legislative framework is viable.

WHAT IS DATA BREACH?

A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property. Most data breaches involve overexposed and vulnerable unstructured data – files, documents, and sensitive information. Data breaches can be quite costly to organizations with direct costs (remediation, investigation, etc) and indirect costs (reputational damages, providing cyber security to victims of compromised data, etc.). There are as many varieties of data breaches as much there are contemporary tools of technology which may not only include hacking, human error, cyber-attacks ranging from phishing, spams, bugs, viruses, malware to ransomware and password attacks but also thoughtful and intentional assaults carried out by the insiders

One study has estimated that cybercrime costs the global economy some $400 billion in annual losses through consumer data breaches, financial crimes, market manipulation, and theft of intellectual property[ii]. Hackers may also pose public safety and even national security risks. While companies are often at the forefront of ensuring cybersecurity, governments can invest in research, share information, model good security practices, and craft thoughtful rules. Governments may need to work closely with their global counterparts and with the business community to stay on top of new threats and share technology solutions. Regulators may need to mandate standards for securing consumer data, and public agencies need to safeguard their own assets.

Preventing a data theft or violation of sensitive confidential information is an essential, through difficult challenge for companies and cyber security professionals. With the rise of sophisticated cybercrime all over the globe beyond boundaries, as well as the proliferation of emerging technology and digital behaviours like IoT and BYOD, protecting sensitive data through straggling industries to better sustain the organisation's cyber security measures.

In a digitally connected society, individuals are constantly disclosing their identity and generating valuable data, which can be used to track their behavior, choices and preferences. The user data is generated not just by active sharing of information, but also in a passive manner including by way of accessing the vast digital content and being connected 24/7 on the internet. With every click on the internet, individuals are rapidly sharing their personal information and data at multiple levels and with multiple parties. As we move towards a digital economy and increase our reliance on internet-based services, deeper digital footprints are being created and personal information is becoming increasingly accessible in the public domain. As a result, the gap between personal and public domain is beginning to reduce rapidly. It is therefore imperative to establish an effective, robust and stringent regime surrounding privacy and security of customer information and data including storage and use of such data for commercial benefits. Such a regime is crucial for building confidence and trust among users for wider adoption of internet-based services and doing business in India.

INTERNATIONAL APPROACHES ON DATA PROTECTION

Governance and management of data is a global concern and many countries have garnered and made a number of initiatives to maximise data sharing and privacy.

The European Union's (EU) GDPR which became enforceable from 25th May 2018, presents robust data protection rules – to name a few - the right to be forgotten and the emphasis on collection of minimum data from individuals or entities. Since then, the GDPR has been a guiding post to other countries in outlining their data privacy rules - where the principal purpose is to offer individuals appropriate control over their personal data and to streamline the

regulatory environment, more notably, for global business by standardising and simplifying the regulation. Since the GDPR is a regulation and not a directive, it is directly binding and applicable to any enterprise – regardless of its location/place of business or individual's citizenship/residence – that is processing the personal data inside the European Economic Area (EEA). However, it does covers scope of flexibility for certain aspects of the regulation to be adjusted by individual member states.

The regulation became a model for numerous national laws outside the EU, including Chile, Japan, Brazil, South Korea, Argentina and Kenya. Notably, the California Consumer Privacy Act (CCPA), adopted on 28 June 2018, has many similarities with the GDPR. Some of the major directives under GDPR are:

- controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles.
- Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization wherever appropriate).
- Data controllers must design information systems with privacy in mind. For instance, using the highest-possible privacy settings by default, so that the datasets are not publicly available by default and cannot be used to identify a subject.
- No personal data may be processed unless this processing is done under one of the six lawful bases specified by the regulation i.e. (1) consent, (2) contract, (3) public task, (4) vital interest, (5) legitimate interest or (6) legal requirement.
- When the processing is based on consent the data subject (or individual) has the right to revoke it at any time.
- Data controllers must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA.
- Firms have the obligation to protect data of employees and consumers to the degree where only the necessary data is extracted with minimum interference with data privacy from employees, consumers, or third parties.

- Firms should have internal controls and regulations for various departments such as audit, internal controls, and operations.
- Data subjects have the right to request a portable copy of the data collected by a controller in a common format, as well as the right to have their data erased under certain circumstances.
- Public authorities, and businesses whose core activities consist of regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR.
- Businesses must report data breaches to national supervisory authorities within 72 hours if they have an adverse effect on user privacy.
- In some cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

Likewise, some of states in USA, Australia and China have also adopted solid cybersecurity and data privacy measures in their respective realm. The US Government has not implemented any national regulation or legislation on data protection per se, however, has adopted a *laissez faire* modal to deal with data privacy issues or disputes.

LEGAL POSITION OF DATA PROTECTION IN INDIA

The fundamental right to privacy (or data privacy), is not expressly provided in the Constitution of India, however, the courts have derived the right to privacy i.e. freedom of speech and expression under Article 19(1)(a)[iii] and right to life and personal liberty under Article 21[iv] of the Constitution of India. Though, the Fundamental Rights provided under Article 19(1) (a) are subject to reasonable restrictions given under Art 19(2) of the Constitution that may be imposed by the State against individuals. Proprietary rights are protected both by the **Constitution of India** as well as by several other statutory provisions. Article 21 of the Constitution of India, for instance, has two aspects - i.e. the one related to the personal side of the right to privacy

and the other protects the commercial angle of the right to livelihood. Right to privacy which integrally includes data privacy is a vital fundamental right of individuals and cannot be taken away without due process of law. Where the same is breached by any individual or entity, the liability lies under Article 21. Likewise, Article 300A of the Constitution guarantees individuals the right to own and enjoy their property. Therefore, a person's property (be it digital or physical) cannot be taken away except by the force of law and any violation of this right can be prosecuted by a court of law.

The historic judgment in **Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors** (Writ Petition (Civil) No 494 Of 2012), by nine-judge bench of the Supreme Court of India dated 24th August 2017, holds that the right to privacy is protected as a fundamental constitutional right under Articles 14, 19 and 21 of the Constitution of India. One would wonder why this question of - whether the right to privacy is a fundamental right or not, was brought before a nine-judge bench. The reason was that in 2017, a bench of five-judges in the Supreme Court hearing the case on Aadhaar Card and the right to privacy, referred for a nine-judge bench to first decide if privacy is a fundamental right or not, before deciding on the issue of Aadhaar Card. The Attorney General in the Aadhaar case had then argued that although several Supreme Court judgments had recognized the right to privacy, however, they had refused to accept that the right to privacy was a fundamental right in the Kharak Singh judgment (passed by a six-judge bench in 1960) and M. P. Sharma judgement (delivered by an eight-judge Constitution bench in 1954). It was, therefore, necessitated to constitute a nine-judge bench to decide whether or not right to privacy is a fundamental right. This broad interpretation by the Supreme Court led to a stream of initiatives by the government towards Personal Data Protection laws.

The specific relevant laws in India, currently, dealing with data protection are the Information Technology Act, 2000 and the (Indian) Contract Act, 1872.

The **Information Technology Act**, **2000 (IT Act)** provides legal recognition to transactions conducted through electronic data interchange and other means of electronic communication, commonly known as "electronic commerce", which include the use of alternative to paper-based methods of communication and storage of information to facilitate electronic filing of

documents with the government agencies and deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of data of individual.

The IT Act defines 'data' in Section 2(1)(o) – *"means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage of media, punched cards, punched tapes) or stored internally in the memory of the computer"*. Correspondingly, the 'computer database' means a formalized representation of information, knowledge, statistics, concepts or instructions in text, image, audio, video that are prepared or prepared in a formalized manner or generated by a computer, computer system or computer network and intended for use in a computer, computer system or computer network. The definitions of data and computer records, along with the requirements on their security and compliance, are satisfactory to combat data property infringements in cyberspace.

Section 43 of the IT Act, prescribes a penalty and compensation with no upper limit, for damage to computer, computer system, etc., against a person when involved in any of the following acts:

1. *"Accesses or secures access to such computer, computer system or computer network;*
2. *downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;*
3. *introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;*
4. *damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;*
5. *disrupts or causes disruption of any computer, computer system or computer network;*

6. *denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;*
7. *provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;*
8. *charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected;*
9. *destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;*
10. *steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage."*

Section 43A of the IT Act provides the rule of compensation in case of failure to protect the data and its states that – *"if a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or wrongful gain to any person, this body corporate will become liable to pay damages as compensation to the affected person".* Here, the term body corporate includes a company, a firm, sole proprietorship, or other group of people engaged in technical or commercial activities. The section prescribes compensation without any limitation on the amount which can be claimed by the aggrieved party – which must be due to the factors around based on sensitivity of information and quantum of damage causes due to any breaches cannot be ascertained beforehand and hence left at the judgement of court.

On the other hand, Section 69 of the IT Act is an exception to the general rule of maintenance of privacy and secrecy of the information which empowers the Government to intercept, monitor or decrypt any information including personal information in any computer resource and the government may warrant the disclosure of information if the information is of nature that ought to be disclosed in the public interest. The Section provides – *"that where the*

Government is satisfied that it is necessary 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 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".

The ***Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011***, - "deals with protection of "Sensitive personal data or information of a person", which includes personal information consists of information relating to - **Passwords; Financial information (such as bank account/credit card/debit card/other payment instrument details; Physical, physiological and mental health condition; Sexual orientation; Medical records and history; and Biometric information**. The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate, who collects, receives, possess, store, deals or handle information, is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, may be held liable to pay damages to the aggrieved person.

The Government has also notified the ***Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009***, under Section 69 of the IT Act, which helps the government authorities to investigate and track cyber-crimes rapidly increasing cause of online activities.

Similarly, the notification of the ***Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009,*** under section 69A of the IT Act, helps the government to deals with the blocking of websites. Recently in the year 2020, the Government has blocked the access of various websites and banned 161 Chinese mobile apps, referring to them as being "prejudicial" to India's sovereignty, integrity and national security. The list included TikTok, Helo, We Chat, Alibaba's UC Browser and UC News, Shein, Club Factory,

Likee, Bigo Live, Kwai, Clash of Kings, PubG and Cam Scanner besides others[v]. As per government, these mobile applications were raging concerns on aspects relating to data security and safeguarding the privacy of 130 crore Indians.

Section 72 of the IT Act provides for penalty for breach of confidentiality and privacy against any person who, in pursuance of any of the powers conferred by the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses such material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000, or both. Section 72A, on the other hand, has a broader scope than section 72 which covers disclosure of a person's personal details, without consent, when delivering services through a legal contract, not just disclosure of information gained by the use of powers provided under the IT Act. Under section 72A of the IT Act, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

It is important to understand the reference of the term 'intermediary' which is added to section 72A. This has been defined under the amendment to the IT Act to mean (with respect to any particular electronic record) *"a person, who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, Web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes".*

In addition to the IT Act, there are certain provisions under **Indian Penal Code, 1860 (IPC)** which relates to infringements of data indirectly and hence falling within the definition of an offence. Indian Criminal Law does not explicitly discuss infringements relating to data privacy, however, liability for any such infringements may be derived under related offenses as provided under the IPC. One of such provision being, Section 403 of the IPC, which imposes

a criminal liability against a person who dishonestly misappropriates or converts any movable property for his usage. Similarly, Section 22 of the IPC provides an expansive description of the word 'movable property,' which includes all corporal properties that implies any information stored in the form of document or on a device can be conveniently and safely treated as a movable property since it is capable of movement from one place to another. In the case of *R K Dalmia v Delhi Administration, 1962*, the Supreme Court held that – "the word 'property'' was used in the IPC in a far wider context than the phrase 'movable property.' There is no valid reason to restrict the scope of the word 'land' to the movable property only when it is used without any qualification. Whether an offense specified in a specific section of the IPC can be committed in respect of any specific type of property may depend not on the meaning of the word 'property' but on whether that particular type of property may be subject to the actions protected by that provision. There is also nothing that removes the data property from the concept of an IPC object".

On the intellectual property side, **the Copyright Act, 1957** stipulates that, unless the purpose otherwise requires, literary work comprises computer programs, tables, and compilations, including computer databases, and therefore the Act provides protection to data content evidently if an objective and correct interpretation of the provisions of the Copyright Act are given. Certainly, the protection of intellectual property rights (IPR) in data property is not easy to create, but any difficulty does not imply an absence or denial of protection and the responsibility to prove the breach lies upon the individual.

Asking businesses to compulsorily share raw data ignores IP protections. Databases, which comprise a collection or compilation of data, whether in machine readable formats or other forms, are given IP protection in international law, both by the WTO and the World Intellectual Property Organisation. This is because the selection and/or arrangement of the contents of a database are understood as intellectual creation. The IP protection is granted to the selection and arrangement of data itself, separate and apart from the contents of the data. Indian copyright law follows a similar approach. Databases are protected as literary works, when they satisfy the test of 'originality' – since businesses select, compile and curate even raw datasets. IP is also protected by the constitutional right to property, and any interference is to be justified

against constitutional safeguards. Further, mandatory data sharing regimes could violate India's obligations under international treaties which provide protection to datasets, for instance - Article 10(2) of the Agreement on Trade-Related Aspects of Intellectual Property **(TRIPS Agreement)** that requires compilations of data that are intellectual creation to be protected. A broad requirement for compulsory sharing of raw and processed non-personal data infringes business IP rights.

In another field of legislation, the **Securities and Exchange Board of India Act** (1992) creates the Securities and Exchange Board of India (SEBI) to control and regulate the use of personal credit records and allows for reactive government access through the SEBI, which is given limited access to private sector data relating to the securities market. As a protection against illegal reactive entry, SEBI is entitled to inspect if it has legitimate grounds to suspect that: an insider or illegitimate business is trading, deceptive trading practises are being used, or securities transactions are being handled in a way that is averse to the lender, the intermediary, or any individual affiliated with the securities. The Act encourages reactive knowledge access and dissemination by penalising someone who fails to supply the requested information.

In the 20th century, the world became more digital than ever before and due to the Covid pandemic, the normal life is altered manyfold. The spotlight on the importance of data, data flows and data privacy, was one of the silver linings of the current time. In 2020, the Indian government took major moves in tech policy and data regulation, including non-personal data, health data, financial data, and data associated to e-commerce and other consumer-facing businesses. The courts have also issued views on individual data privacy rights, and the long-debated **Personal Data Protection Bill, 2019 ("PDP Bill")** was a significant piece of legislation under consideration by the Government. The PDP Bill, which was inspired by the GDPR, was proposed in 2019 to restructure India's present data protection law, which today majorly tackled under IT Act. The present version of the PDP Bill establishes compliance standards for all types of personal data, expands individual rights, establishes a central data protection authority, and mandates data localisation for some types of sensitive data. If specific linkage conditions are satisfied, the PDP Bill extends extra territorially to non-Indian entities

and levies significant financial penalties in the event of non-compliance.

The main aim of PDP Bill is to protect the privacy of individuals through a protective mechanism governing the collection and use of information by businesses. Particularly, it focuses on the control of data usage activities. The PDP Bill would significantly expand the government's position in the data economy, dilute data property rights and increase state surveillance powers without providing appropriate checks and balances as the current system is unlikely to adequately protect privacy.

Specific data protection laws are ardently required in India, and even if they are imperfect, they are better than having no data protection legislation. This PDP Bill is a great first step toward establishing defined regulatory principles and when the PDP Bill would become law, the concepts of data protection rules in the EU, California, Canada, and India will be comparable. An orderly digital business market would be a win-win to citizens, governments, and global corporations alike.

The PDP Bill includes fundamental principles like as the right to be forgotten, data portability, and data anonymization, all of which will be critical in allowing digital empowerment. The PDP Bill proposes the establishment of a Data Protection Authority to guarantee that institutions uphold these rights. Most crucially, the Bill establishes 'consent framework' as the cornerstone of data sharing, collecting, and deletion, and calls for an electronic consent dashboard that would allow data controllers to track consent for processing in real time and operationalize the right granted to them under data protection legislation. According to the proposed law, personal data cannot be shared or processed unless an individual has provided consent at the start of the processing, which consent must be freely given, informed, precise, explicit, and revocable. The PDP Bill proposes the notion of "consent managers," who will use an accessible, transparent, and interoperable platform to manage a data principal's consent for data sharing. These consent managers would be "data blind," which means they won't be able to read or utilise personal data; instead, they'll act as a conduit for encrypted data flows. This ecosystem proposed to offer all participating institutions with procedural and best practise

standards, assist organisations in adopting and continue to stimulate innovation in data rights protection across the network through new common technological building blocks.

JUDICIAL DECISIONS

National Association of Software and Service Companies v Ajay Sood[vi] is a landmark judgment, in which the Delhi High Court declared 'phishing' to be an illegal act, and defined it as "a misrepresentation made in the course of trade, leading to confusion, as to the source and origin of the email causing immense harm, not only to the consumer, but even to the person whose name, identity or password is misused". The court found the act of phishing to constitute passing off that tarnished the reputation of the plaintiff, and awarded an injunction and compensatory damages.

Jagjeet Singh vs. State of Punjab, 2021, the Apex Court remarked that hacking or data theft, in addition to penal provisions under the IT Act, also attracts offences under IPC.

In the case of *K. S. Puttaswamy (Retd.) v Union of India*[vii], the Supreme Court developed a three-part test for the State's interference in constitutional rights. Where a State may intervene to protect legitimate State interests, (a) there must be a law in place to justify an infringement of privacy, which is an express provision of Article 21 of the Constitution; (b) the form and substance of the law enforcing a restriction must fall within the reasonableness specified by Article 14; and (c) the means adopted by the legislature must be proportionate. The decision of the Hon'ble Supreme Court empowers the citizens of India to obtain judicial relief if their data privacy rights are violated. It may have an effect on the privacy and security practises of Indian tech firms. Users may not only file complaints based on wrongdoing, but they may also assert their fundamental right to privacy.

In the landmark judgment of *Justice K.S.Puttaswamy(Retd) V. Union Of India*, the 'Aadhaar Card Scheme' was challenged on the basis that it violates a constitutional right to privacy enshrined in Article 21 of the Constitution by collecting demographic and biometric data. The

Supreme Court has stated that the state must carefully balance the privacy of personal data with the legal intent, at all costs, because constitutional rights cannot be given or repealed by statute, and all legislation and actions must comply with the constitution. The Court further claimed that the right to privacy is not an unconditional right and that any breach of privacy by the State or a non-governmental agent would meet three criteria: the existence of a legitimate purpose, uniformity, and legal status.

The need of the hour is evident from the above: comprehensive legislations controlling the acquisition and dissemination of personal data. There are no precise restrictions governing the processing of personal data that isn't classified as "sensitive personal data or information.

CONCLUSION

Data privacy has always been important. This is the reasoning that people put locks on filing cabinets and rent safety deposit boxes at their banks. But as more of our data becomes digitized, and we share more information online, data privacy is taking on greater importance. A single company may possess the personal information of millions of customers.

When data that should be kept private gets in the wrong hands, the evil-minded people take advantages of such access to data and exploit the data or the owner of such data directly or indirectly. A data breach at a government agency can, for example, put top secret information in the hands of an enemy country. A breach at a company can put proprietary data in the hands of a competitor. A breach at a school could put students' personal data in the hands of criminals who could commit identity theft. A breach at a hospital or doctor's can put personal health information in the hands of those who might misuse it. Data is an incredibly important asset, and collecting and sharing data can be big business in today's digital economy. But for a business to safely and successfully take advantage of the data they're collecting; they need to have safeguards in place to ensure data is under tight lock and key and consumers aren't subject to uninvited surveillance.

The method of ensuring that records and sensitive documents are not damaged or distorted is known as - data or information security. It can be difficult for others, but it provides advantages such as increased investment returns, better customer satisfaction, and more productive operations. It is obvious that the need for the hour is an extensive legislature governing the collection and dissemination of private information.

Indeed, information is the fresh currency in this era of universal and virtually free internet access. What's even more intriguing is that one doesn't know the complete information potential. Data is the "new oil", and has arguably replaced oil as the world's most valuable resource. Internet and smartphones have made data ubiquitous. Therefore, any legislation that is brought in to regulate the data protection must not be limited in its scope or be limited to service providers or sector specific alone, but rather address the issue of protection and privacy of personal data across all mediums and parties, holistically.

ENDNOTES

[i] "Microsoft warns of ransomware attacks as Exchange hack escalates". *IT PRO. 12 March 2021*. Retrieved 12 March 2021. *Also see:* "Microsoft: 92% of vulnerable Exchange servers are now patched, mitigated". *www.msn.com*. Retrieved 29 March 2021.

[ii] Net losses: Estimating the global cost of cybercrime, Center for Strategic and International Studies and McAfee, June 2014.

[iii] Art 19 of the Constitution of India - Protection of certain rights regarding freedom of speech, etc. - (1) All citizens shall have the right— (a) to freedom of speech and expression;

[iv] Art 21 of the Constitution of India - Protection of life and personal liberty. - No person shall be deprived of his life or personal liberty except according to procedure established by law.

[v] Press Information Bureau (pib.gov.in) and https://pib.gov.in/PressReleasePage.aspx?PRID=1650669

[vi] 119 (2005) DLT 596

[vii] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018 (indiankanoon.org)