DE JURE NEXUS LAW JOURNAL

Author:

Sherin Sneha R

VISTAS

3rd Year, BBA LL.B. (Hons.)

DATA PROTECTION BILL AND PRIVACY

ABSTRACT:

'If we don't act now to safeguard our privacy then we would become the victims of identity theft.'

In this world and in this time, we are all in the hands of the virtual world struggling to protect our privacy. With or without knowing we hand in our privacy to not one or two people but to more people that are uncountable and unseeable. Those people are the vultures that are flying above us waiting to get its prey.

Confidence in information and communication systems in this digital time has become crucial but this confidence is not possible without privacy-enhancing tools and technologies, nor without risk management framework.

This paper talks about the misuse of digital networks by disclosing the personal information of users and lack of privacy in virtual world and the need for social media in this Covid-19 pandemic.

KEYWORDS:

Privacy, Covid-19 pandemic, Misuse, data theft, Aadhar card.

INTRODUCTION:

Personal Data Protection ensures the safety of user's personal information and regulates the data provided. In this pandemic every work in this world depends on social media and everyone lives in it by handing in your personal data and losing your privacy with or without knowing. In few months, we are all going to be the victims in the hands of corporate firms. ***We become the prey, social media becomes the tool and the corporate firm becomes the king.***

Recently India has banned 118 Chinese apps under Section 69A of Information Technology Act due to illegal data collection of the users. These apps collected extensive data about users without their prior knowledge such as Wi-fi data names, password, account details, etc. Not only these apps have collected data but there are many other apps collecting our data's by placing cookies in our device and by various methods without our knowledge. Since, we all depend on social media due to this covid pandemic and it is our right to privacy under Indian Constitution Act, it is the duty of our government to protect our privacy and our personal data. In this paper I have talked about, why the PDPB is necessary, analysis of the victims of social media and how European countries and other countries have framed their Data Protection Act.

RESEARCH METHODOLOGY:

The descriptive and secondary-data based analysis method is used to know the importance of data protection bill and lack of privacy. The data in this paper is collected mostly from various journals, articles and statistics from all over the world.

REVIEW OF LITERATURE:

Data theft are happening not only in India but all over the world in each and every day. Unknowingly we all become one of the causes for the crime by disclosing our details in the hands of social media. According to a report by digital security firm Gemalto [1], in 2018 India ranked as the second highest country in data breach incidence globally. Compared to the first quarter of 2019, data theft has increased by 37% and minimum total cost of the leaks in India has cost over Rs. 14 crores in 2020[2]. As this pandemic has led to WFH (Work from Home) situation, over 15 billion of credentials has been up for sales in 2020 illegally[3].

"If you exchange information internationally, you must strengthen data protection. Those are two sides of the same coin" – Gris de Vries

This quote reflects the main objective of this research paper. When there is a change in this world then there should be a change in law to balance. In this pandemic it is necessary for everyone to share or collect data through online to earn money. It becomes one of the parts in our day to days life. In jurisprudence, there is a judgement saying, 'Privacy is when a Pardanashin women could access her balcony without fear of neighbourhood gaze'. Therefore,

in order to protect our privacy, we need the protection of Law. **These are two sides of the coin.**

"Privacy is dead, and social media holds the smoking gun."

– Pete Cashmore, CEO of Mashable

This author has greatly explained about how social media is dangerous in this world by calling it as **Smoking Gun**. This is an interesting quote since it focuses on today's digital world. We can tag this quote for our teenagers especially for women's. We see many reports on women attempting to suicide because of her private photos or videos such as nude pic or photos with her boyfriend being exposed all over the social media such as Twitter, Facebook, etc., without her knowledge which leads her life to an end.

"Privacy is not just sitting alone in a room, it covers many aspects like non-disclosure of personal information, original work, business secrets, personal relationship and life, etc. It is a violation of a person's right if his letters to another are published without his permission

-Personal computing pioneer and investor Mitchell Kapor

This quote explains what is real privacy in today's world. Before the invention of smartphone and digital world, privacy only means our personal information, our health, business secrets, relationship, life style, etc., but, after the invention of technologies and dark web, the meaning of privacy has extended to all silly things or actions we do in our daily life. Many times, with or without knowingly we allow many cookies to access our data which causes data breach. Manipulation is done not only through cookies but also by dark web and hackers by hacking cameras. Therefore, in this digital world privacy is not limited to our room but to the place where we can't reach.

"Getting information from the Internet is like taking a drink from a hydrant"

When watching videos in YouTube or while using some apps, we get lots of Ad. But, did anyone notice that those Ads are extremely based on the contents that we search through internet or apps? and how do they know about what we are searching. We are the answers for these questions. We give them permission to monitor us. We give them permission to intervene in our privacy. We trust internet but internet sells our information for profit. Internet is the poison we use to kill ourself.

IMPORTANCE FOR DATA PROTECTION BILL:

The draft bill, named Personal Data Protection bill has been proposed by former Supreme Court judge B.N. Srikrishna in the year, 2018 will be passed in the Parliament after the cabinet approval. This bill is requested to be passed as soon as possible in India, since this covid 19 pandemic has led us to WFH situation which makes us in need of social media. At this time there are many agencies who makes profit by selling our personal data to other corporate firms. India has become one of the top-ranking countries in cybercrime cases. According to Kaspersky's telemetry, the total number of brute force attack has jumped from 93.1 million worldwide in February 2020 that is before lockdown to 277.4 million in march 2020 that is after the start of lockdown- a 197% increase. In India the number of cases went from 1.3 million in February 2020 to 3.3 million in March 2020 and From April month onwards, cybercrime attack has never been below 300 million. Therefore, this data protection bill has a set of regulation on data collections. This bill provides us some basic rights to protect our data privacy such as, ***the right to be forgotten, right to correction, right to erasure and right to access data.*** Some of these rights are similar to the European General Data Protection Regulations. At many times there are number photos and videos are being abducted or morphed or being hacked by others and released in social media. For example, in New Delhi, a 17year old girl has killed herself after her morphed image were leaked on Facebook. Therefore, in order to prevent these from happening in future and to achieve threat free India, we need to have the rights to erasure, correction and the right to be forgotten.

Let's see some of the biggest data breach that happened in India.

1. **Debit card data breach:** This was reported [4] in the year 2016 stating that over 3.2 million debit cards from major Indian banks were compromised due to a malware injection in Hitachi payment service system and nearly 13 million INR are been transacted fraudulently by hackers.
2. **Aadhar card data breach:** This is a government database where data's such as, citizen's name, bank account number, password, biometric data, etc., are recorded. In 2018, Aadhar card was reported [5] to be leaking and over 1,000,000,000 people have been affected by this. This effect made a great blow on Right to privacy in Puttaswamy case and this led to data protection and privacy bill.
3. **SBI data breach:** In January 2019, it was reported [6] that SBI exposed its customer data such as, their phone numbers, account details, passwords, etc., from an unprotected server in its Mumbai Data center.

Therefore, in order to protect our data, we need to pass the data protection bill in India as soon as possible. Its already late but not too late if, it protects our privacy in future.

CROSS- COUNTRY GDPR:

There are more than 120 countries than gives importance to data protection and privacy of their country by implementing Data Protection Regulations. Some of the top countries with Data protection laws are,

EUROPE (GDPR): Personal Data Protection Bill of India which was proposed by former justice S.N. Srikrishna in the year 2018 was formed on the basis of European General Data Protection Regulation (GDPR).

European General Data Protection Regulation was adopted on 14th April 2016 and implemented on 25th May 2018. GDPR is not directive but it is a regulation. It is flexible and individuals can adjust in certain aspects. The European GDPR became a model for many countries including Japan, Brazil, Chile, South Korea, Argentina, Kenya and now it is also the model for India. The GDPR is enforceable to all data controllers and processors outside European Economic Area (EEA) who is engaged in work with EEA. This statement purposely gives Extra-Territorial Jurisdiction for non-EU members.

GERMANY: Germany was the first country to look up on the issue of data privacy. The Parliament of Germany requested its government to introduce a legal framework on regulating the computerized processing of personal information in the year 1969 but the bill was proposed in the year 1976 and enacted in the year 1977. It nearly took 8 years to frame the data protection regulations for Germany.

CHINA AND RUSSIA: China and Russia hold the first rank for implementing the best data protection laws in all over the world. They have their own version of internet and strictly controls the exchange of data, commercial availability, transfer of data, etc. For any collection of individuals personal data, consent is required. However, both countries strictly regulate their own country.

BRAZIL: Brazil has implemented *Lei General de Protecao de Dados* (LGDPD) on September 2020. It was modelled after European GDPR. LGDPD is identical in terms of scope and applicability but the penalty for non-compliance of the regulation is less in amount. Any companies willing to work with Latin America must comply with LGDPD or they will be imposed with fine over 50 million BRL.

JAPAN: Japan has amended Personal Information Protection Act in the year 2017 of May. This act is applicable to both foreign and domestic companies that involves the process of data

collections of Japanese citizens. The companies that located outside of Japan will also be subjected to follow the guidelines under the Act.

Recently Europe and Japan have joined hands in data protection laws by signing an agreement on "reciprocal adequacy". Japan has white listed the European companies since their data protection laws are strictly regulated and at the same time Europe also have white listed Japanese companies for the same.

There are still many countries that have implemented or still framing on data protection laws. Since the time is getting more speedier due to WFH situation the countries must also speed up their work on framing data protection laws.

CASE LAWS:

There are number of cybercrime cases recorded all over the world where India holding top rank list in recording cybercrime cases in this pandemic situation. Here are some of the cases that focused on Right to Privacy and data breach.

JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA [7]

Justice K.S. Puttaswamy is retired Madras High Court Judge, challenged against the constitutional validity of Aadhar card scheme. He argued that Aadhar scheme violates the constitutional rights of Right to Privacy. A nine judged bench decided this case.

In this case, the court considered whether Right to Privacy is one of the Right to life and Personal Liberty under Article 24 of the Indian Constitution.

The Court held that *privacy is an attribute of human dignity. The right to privacy safeguards one's freedom to make personal choices and control significant aspects of their life*. Further, the Court held, *"similar to the right to life and personal liberty, the right to privacy may be limited by a procedure established by law. The invasion of privacy must be through a fair, reasonable and just procedure. It must meet the three conditions of legality, the existence of a legitimate state aim and proportionality. Legitimate state aims would include national security concerns, preventing and investigating crime, and preventing the dissipation of social welfare benefits."*

PUNE CITIBANK MPHASIS CALL CENTER FRAUD:

This was the first cybercrime case that is in Pune. In this case, some of the ex-employees of Mphasis Ltd has abducted Rs. 1.5 crores from US customers using "non-authorised access" to the "electronic account space" of the customers.

The court held them under section 66 and section 43 of the information Technology Act 2000. They are held liable for both fine and imprisonment. They are also liable to pay damages of up to Rs.1crore per victim for 'Adjudication Process' can be invoked.

SMC PNEUMATICS (INDIA) PVT. LTD (VS) SHRI JOGESH KWATARA[8] :

This case was the first cyber defamation case (12th February, 2014) recorded in India. In this case the defendant Jogesh Kwatara an employee of SMC Pneumatics Pvt. Ltd, has sent vulgar, obscene, filthy and abusive emails to all its employees and its other subsidiaries in all over the world with the aim to destroy the reputation of the plaintiff's company.

The court held on behalf of the plaintiff, that the email sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Therefore, the court passed an ***ex-parte ad interim injunction***, observing that the ***prima facie*** case had been made out by the plaintiff.

STATE OF TAMIL NADU (VS) SUHAS KATTI[9] :

This case was about posting obscene, defamatory and annoying message about a divorced women in Yahoo and also sending the same through email to the victim by opening a false email account in the name of the victim. This resulted in annoying phone calls to the lady says that she was soliciting. Later, she filed the case and the accused was tracked down by the police in few days. The accused was the well-known family friend who was interested in marrying her and got rejected. So, he took up harassment through the internet.

Later, the court held him to pay fine of Rs.500 and 2 years of rigorous imprisonment under 469 of IPC and 1-year simple imprisonment and fine of Rs.500 for offence under 509 of IPC and also 2 years of rigorous imprisonment with fine of Rs.4000 under Section 67 of IT act 2000.

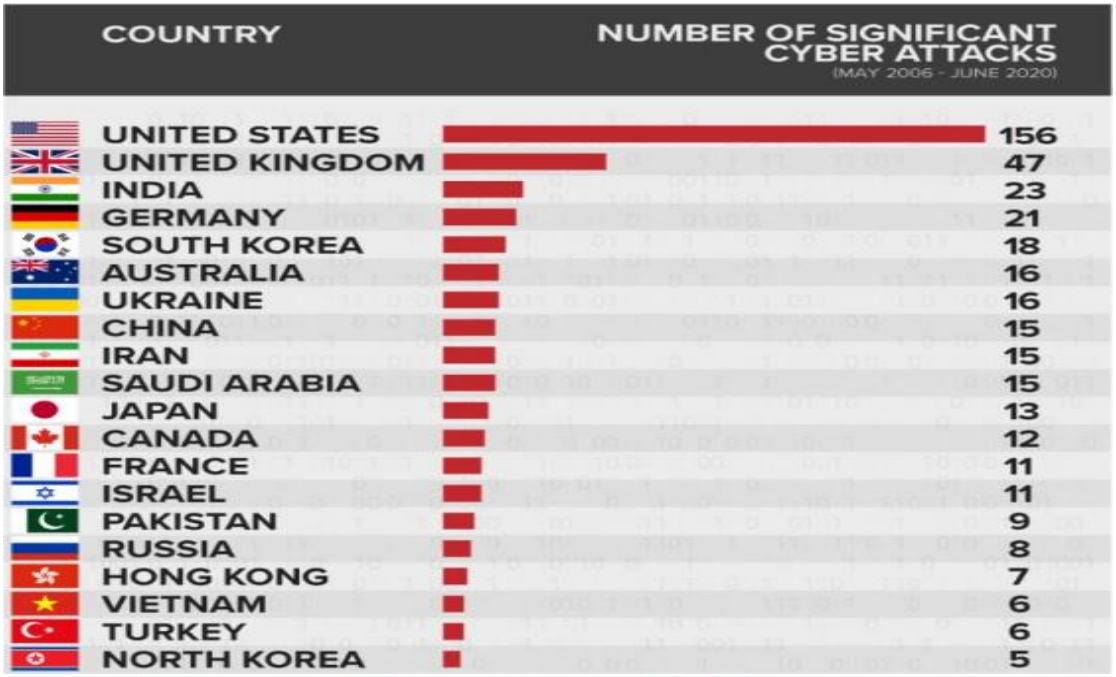
PERSONAL CASES:

- Cyber police have arrested a husband who hired a hacker to hack into his wife's FB account to find evidence of her bad character.
- A boy who broke up with his girlfriend has posted her phone number in 24/7 dating site to take revenge and was arrested in leading cybercrime case
- A famous Gujarati singer filed a case claiming that an unknown man is using her photo in social media saying that he is married and had a child with her.
- Using a trojan or malware, a woman's webcam was hacked to take private pictures and videos of her and posted it on an illegal website.

STATISTICS:

Let's see some of the statistical data that is collected from all over the world by various researchers.

First, lets see the countries that are ranking top in recording cybercrime cases.



As we all can see, India is ranking 3rd in cybercrime cases. It might be a bit releif since its in 3rd and not in 1st but, time goes very fast. There is no much time for us to come in first since we have not yet passed PDPB.

United kingdom holds the 2nd place with having 47 cyber attacks between May 2006 to June 2020 and US holds 1st with having 156 cyber attacks.

As for India in the year 2021 the number of cases went from 1.3 million in February 2020 to 3.3 million in March 2020 and From April month onwards, cybercrime attack has never been below 300 million.

Here are some of the data breach that mostly affected India:

		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

In India Aadhar breach was the most highest data breach in the year 2018. Aadhar card scheme contains most sensitive personal data of the citizens such as, retina biometrics, fingerprints, account details, passwords, Pan card ID, Voter ID, license, etc. More than 1,000,000,000 people's data have been disclosed illegally to corporate firms for the purpose of earning profit. This issue became a great sensational new in 2018 by justice Puttaswamy case and this case led to the idea of Right to privacy and data protection

CONCLUSION AND SUGGESTIONS:

"***VAST POWERS COME WITH RESPONSIBILITY"***

Everyone wants powers but when power comes then responsibility must also come. Powers without responsibility is not the power but the destruction. Internet is our power. Personal Data Protection Bill is our responsibility. Internet without responsibility only gives destruction to this country. If we want to enjoy the full rights to access to data without fear of being hacked, we need the personal data protection bill. Its already late, WFH situation has already destroyed the lives of many, but, unless and until the bill protects our future, then it's not too late to bring the bill into act. Take action to enact the Act. Some of the suggestions to protect our privacy are,

- ✓ Proper security and training awareness
- ✓ Right to Erasure
- ✓ Guidelines to regulate the data
- ✓ Data destruction plan, and,
- ✓ Appropriate access control.

REFERENCES:

[1] Gemalto was an international digital security company providing software applications, secure personal devices such as smart cards and tokens, and managed services.

[2] IBM study report

[3] Digital monitoring firm report

[4]Debit card data breach

[5] Aadhar card data breach

[6] SBI Data breach

[7] (2017) 10 SCC 1

[8] RFA 268/2014

[9] C No. 4680 of 2004