Law Audience Journal, Volume 3 & Issue 3, 19th January 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 97 to 111,

Title: "How Data Protection Laws Helps in Bridging the Gap of Data Breach?", Authored By: Mr. Tejeshwar Pandey (B.B.A.LL.B), Symbiosis Law School, Nagpur,

Email Id: pandeytejeshwar@gmail.com.

Cite this article as:

MR. TEJESHWAR PANDEY, *"How Data Protection Laws Helps in Bridging the Gap of Data Breach?",* Vol.3 & Issue 3, Law Audience Journal (e-ISSN: 2581-6705), Pages 97 to 111 (19th January 2022), available at ***https://www.lawaudience.com/how-data-protection-laws-helps-in-bridging-the-gap-of-data-breach/.***

Law Audience Journal, Volume 3 & Issue 3, 19th January 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 97 to 111,

Title: "How Data Protection Laws Helps in Bridging the Gap of Data Breach?", Authored By: Mr. Tejeshwar Pandey (B.B.A.LL.B), Symbiosis Law School, Nagpur,

Email Id: pandeytejeshwar@gmail.com.

Publisher Details Are Available At:

https://www.lawaudience.com/publisher-details/

Editorial Board Members Details Are Available At:

https://www.lawaudience.com/editorial-board-members/

Law Audience Journal, Volume 3 & Issue 3, 19th January 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 97 to 111,

Title: "How Data Protection Laws Helps in Bridging the Gap of Data Breach?", Authored By: Mr. Tejeshwar Pandey (B.B.A.LL.B), Symbiosis Law School, Nagpur,

Email Id: pandeytejeshwar@gmail.com.

DISCLAIMER:

Law Audience Journal (e-ISSN: 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in ***Volume 3 & Issue 3*** *are the original work of the authors.*

Views or Opinions or Suggestions ***(if any)****, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.*

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

Law Audience Journal, Volume 3 & Issue 3, 19th January 2022, e-ISSN: 2581-6705, Indexed Journal, Published at https://www.lawaudience.com/volume-3-issue-3/, Pages: 97 to 111,

Title: "How Data Protection Laws Helps in Bridging the Gap of Data Breach?", Authored By: Mr. Tejeshwar Pandey (B.B.A.LL.B), Symbiosis Law School, Nagpur,

Email Id: pandeytejeshwar@gmail.com.

I. INTRODUCTION:

"Data protection is considered to be the most debatable topic rolling in today's world especially in Indian context. Although it is the most crucial topic sadly it is neither being safeguarded by any separate legislative support. The only and most prior of this very article is to make the readers understand the general and legal context behind the such laws which is primarily being understood by each and every person in the society who is using social media platforms and other modes of entertainment on the internet".

II. WHAT IS DATA?

Data can be defined as the collection of all the information and material produced and obtained in the performance of services which consists of ***survey plans, charts, recordings (video and sound), pictures, curriculum, graphic representations, computer programs, and printouts, notes, finished or unfinished documents*** which can be utilised to form the future of the entity or the individual.

Data can be of two types;

- **PERSONAL DATA:**

  It is the private information of the individual which can be used to trace/monitor him online. It is any information related to an identified individual. This information should not be disclosed to any third party. Personal data includes ***medical, biological, financial, and residential information***.

- **NON-PERSONAL DATA:**

  Everything other than personal data is non-personal data. It is the general information of an individual which can get the organizations to make strategies to make profits. Data that is collected by the government in course of publicly funded works.

III. WHAT IS PRIVACY/DATA PRIVACY?

The meaning of privacy changes according to its legal context. It can be said as the right of individuals concerning their personal information. It is freedom from unauthorized intrusion.

III.I WHAT IS DATA PRIVACY?

Users have the right to control their data, they have a right to limit the data a website or an organization collects. Data privacy is the regulation of a user's data like history, financial, and property information i.e., private information which can be used to monitor, trace the identity of the user from being accessed by anyone or any third parties on a website or an online platform. It regulates the processing of data and controls it from being accessed by a third party online. It is simply the right usage of data by a website or a platform. Internet users trust the intermediaries that the information collected by a website is protected and confidential. Trust is an important factor in a relationship, the relationship between the internet user and the intermediary should be trustworthy else it will be the exploitation and disclosure of the individual's web life and his privacy. In this digital era, there is no specified limit declared by the Indian legislature on the collection of data by a website or an organization. There are some types of data privacy listed herein.

III.II TYPES OF DATA PRIVACY:

III.II.I ONLINE PRIVACY:

Online privacy is important, websites have a privacy policy stating their usage and collection of data.

III.II.II RESIDENTIAL INFORMATION:

The information about a user's residence and cost of living should be kept private when collected.

III.II.III MEDICAL PRIVACY:

The medical information about a user should not be disclosed to any other person other than the organization and the user. The doctor-patient confidentiality should be maintained or it amounts to a breach of medical privacy.

III.II.IV FINANCIAL PRIVACY:

Financial privacy is the collection of financial information by a website. If it is not stored and protected, it leads to fraudulent use of credentials by hackers.

III.III ADVANTAGES OF DATA PRIVACY:

- *Prevent the Government from spying on the citizens;*
- *Ensure those who steal and misuse data are held accountable;*
- *Maintains boundaries;*
- *Ensure the control over personal data;*
- *Protect freedom of speech and expression.*

III.IV CONSEQUENCES OF DATA DISCLOSURE:

Data, if disclosed, can destroy a person's life. Education records and biological information also fall under personal data. Hackers can use personal data to defraud, buy illegal items using the credentials of the individual, which makes him accountable for the transaction, if not doubted early. Some websites sell information that results in unwanted advertisements, marketing. If a person is being tracked, monitored online, it prevents his right to freedom of speech and expression which is granted as a fundamental right under Article 19(1)(a) of the Indian Constitution. What is the reality of data privacy?

III.V THE REALITY OF DATA PRIVACY:

Achieving data privacy is hard for an individual. In a retrospective view, it can be achieved by regulating organizations in the matter of data collection and data storage. A lot of negatives prevail on privacy and regulation. In reality, not every organization maintains confidentiality. Confidentiality of data and measures of data security is essential in large organizations. But small-scale organizations are not up to the mark in confidentiality and accountability. Since the last decade, we've seen many data breaches and hacks of major companies' data like Facebook, Mobikwik, etc. The user data stored in the servers are being stolen and sold on the dark web. More than 1.1 million cyber-attacks were reported across India in 2020. This was a significant increase compared to the previous year's nearly 400 thousand. The country was amongst the top five with the greatest number of cyber security incidents that year. Furthermore, India's ranked third in terms of internet user numbers.

IV. DATA LOCALIZATION:

Localization is the act of adapting the procedure within its boundaries. It is the act of storing data on any device present within the borders of a country. If the data is stored within the country, there would be no barriers or permissions required to access the information. To access information stored in the foreign cloud, Mutual Legal Assistance Treaties should permit the country. Now, most of this data is stored in a cloud existing outside the country. Localization of data is an important factor of national security, as data will be stored in a server within the country and can be accessed anytime and can keep it safe from foreign surveillance. The entities around the world scrambled to comply with the RBI's deadline for localization of all sensitive data belonging to Indian users of various digital payment services. What is the importance of data security?

V. DATA SECURITY:

Data security is the protection given to the individual from unauthorized access from third parties and corrupted sites which steal information. Data Security ensures the integrity of data and helps in preventing malicious attacks and unauthorized entries into the user's personal information. ***Examples:*** Password of an individual's internet banking account, the encryption provided by the site are some examples of data security.

V.I SHOULD YOU PAY EXTRA FOR DATA SECURITY:

It is immoral to sell security measures for money. Privacy is an individual's right protecting the same is the duty of an organization to provide every user with the same level of security. Some commercial companies demand users to pay extra for protection from fraudulent and unauthorized transactions.

V.II SECURITY BREACH: SALE OF DATA ON DARK WEB:

In a major data security lapse by a private entity, 8.2 terabytes — the largest such breach in India — consisting of personal information of 3.5 million users, allegedly of payments platform MobiKwik, is up for sale on the dark web. While several independent cybersecurity researchers have been reporting about a likely data breach of MobiKwik's servers as early as February, French security researcher

VI. DIFFERENCE BETWEEN DATA PRIVACY AND DATA SECURITY:

Data Security is different from Data privacy. Data privacy regulates the flow of user data by a website or an organization whereas data security ensures the protection from unwanted access, Preventive measures of a data breach can be included in data security. In simple words, it is what is being protected and how it is being protected. To achieve data security organizations, use firewalls, encryption technologies. Letting the user know what data is being collected, and thereby giving him complete transparency about his data is the goal of data privacy. Privacy concerns are impossible to address without first employing effective security practices. ***Example:*** A process of de-identifying is an example of provisions of data privacy. A major data security technology measure is encryption, in which digital data, software/hardware is encrypted and rendered unreadable to unauthorized users and hackers.

VI.I GODADDY REPORTS DATA BREACH: DATA OF 1.2 MILLION CUSTOMERS IMPACTED:

Nearly ***"1.2 million active and inactive Managed Word Press customers had their email address and customer number exposed,"*** adds the filing. The reason email addresses are being stolen is a serious issue. It can increase the risk of phishing attacks where cybercriminals send emails to users in an attempt to trick them into leaking their other account details.

VII. LEGISLATURE:

In India, there is no legislative framework approved on Data Privacy.

VII.I RIGHT TO PRIVACY: A FUNDAMENTAL RIGHT:

Article 21*[1]*, is the heart and soul of the constitution and the heart of fundamental rights. The judicial intervention said that the rights are included within it, the scope of Article 21 is not narrow and restricted. It has been widening by several judgments. ***The court included the following rights that are covered under Article 21 based on its judgments :***

1. Right to privacy
2. Right to shelter
3. Right to go abroad
4. Right against custodial death
5. Right to pollution-free water and air
6. Right against solitary confinement
7. Right to social justice and economic empowerment
8. Right against handcuffing
9. Right against delayed execution
10. Right against public hanging
11. Protection of cultural heritage
12. Right of every child to full development
13. Right to health and medical aid
14. Right to education
15. Protection of under-trials.

In the case of Justice ***K.S. Puttaswamy vs .UoI (2017) 10 SCC,*** The Advocate General of India responding on behalf of the union, made a statement that the right to privacy is no fundamental right and was not mentioned anywhere, according to the constitution. The apex court unanimously held that the right to privacy is protected as a fundamental right and falls under Article 21 of the Indian Constitution. In this case, Justice K.S.Puttaswamy (retd. High Court judge) challenged the validity of the Aadhar Act and the usage of the personal data of individuals i.e., biometrics and other personal data. The court held that the collection is valid

[1] Protection of Life and Personal Liberty. Article 21 states that ***"No person shall be deprived of his life or personal liberty except according to a procedure established by law"***.

and will only be used for the welfare of the individual and the nation as it narrows down the scope of corruption in the nation.

VII.II RIGHT TO BE FORGOTTEN:

The right to be forgotten is the right of an individual to remove personal data from internet histories and other intermediaries, middlemen. The Honourable court, recently held that the right to be forgotten is a subset of the right to privacy.

VII.III SECTION 43(A) OF INFORMATION TECHNOLOGY ACT OF 2000[2]:

Vinit Kumar vs. CBI and Ors (2019), In this case, calls of businessmen were intercepted on the order of the Union home ministry, against which the petitioner challenged the orders in the High court of Bombay, i.e., the infringement of the right to privacy. The court held that there was no lawful justification for the orders and set them aside. There are 2 sections relating to data disclosure and failure to protect data, in the Information Technology Act, 2000.

VII.III.I 43A. COMPENSATION FOR FAILURE TO PROTECT DATA:

Where 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, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

VII.III.II 72A. PUNISHMENT FOR DISCLOSURE OF INFORMATION IN BREACH OF LAWFUL CONTRACT:

[2] a penalty of INR 10 million inter alia, for downloading data without consent.

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

The Act also provides that a body corporate (any company, firm) must provide a comprehensive privacy policy. The privacy policy must include:

- a clear, accessible statement on its practices and policies
- the type of information collected
- security measures
- Purpose of collection of data and the storage of data
- the disclosure policy for the information

To make a strong law satisfying the consumer, there is a requirement of provisions regarding:

- Data Collection and rights to share: No information should be disclosed to any third party.
- Consent: No information should be collected without the consent of the user.
- Data Minimization: Collect what is needed and specify why it is needed.
- Proper use of data: Using data is the right way and being ethical.
- Accountability of the controller of data.

VII.IV DATA PRIVACY AND PERSONAL DATA PROTECTION BILL, 2019:

The court made a special committee to produce a bill on personal data, The Sri Krishna Committee. The committee headed by retired Supreme court judge BN Krishna submitted a report on July 27, 2018. The bill of Personal Data Protection, 2019 was framed by the government and was immediately sent to ***Joint Parliamentary Committee (JPC)*** and is not implemented yet, the committee said that the framework is not precise and is not suitable for the dynamic environment of the technology. It took 5 extensions since 2019 to approve the made bill. The PDP, 2019 clause 35gives shelter to the government to access any information of any user and even trace information of the people of the nation. The government had absolute powers to track people and their information online (if necessary).

There should be a legislative framework on the matter as it has been becoming a concern of national security. The PDP Bill proposes the concepts of a '***data fiduciary' and a 'data processor'***. A ***'data fiduciary' and a 'data processor'*** are equivalent to the concept of controller and processor under the GDPR. The bill gives protection to individuals by penalizing entities for data collected without user consent.

The PDP Bill will not only apply to persons in India but also to persons outside India concerning business conducted in India, the offering of goods or services to individuals in India, or the profiling of individuals. The bill also specified provisions regarding the holding of user data.

VII.IV.I WHAT IS THE STATUS OF THE PDP BILL, 2019?

The Joint Parliamentary Committee had been deliberately working on the report since 2019, the committee was debating about several clauses and provisions, mainly Clause 35 of the bill, exemption of Government on the public order, and national interest. After 2 long years, On 22 November 2021, the committee adopted the bill and approved to send the bill to the parliament in the next session. The committee retained the exemption clause with a minor change, and even if the state is empowered to exempt itself from the application, it shall only be used under exceptional circumstances. The committee had also recommended that all social media platforms should have an office set up in India and a media regulation authority to regulate the flow of content. There are prevailing arguments that it has no adequate safeguards to protect the right of privacy of an individual. The committee had also stated that there is no provision related to the collection of data by hardware manufacturers.

VIII. MAJOR BREACHES OF INFORMATION PRIVACY:

VIII.I PEGASUS SPYWARE:

- It was created by the NSO(N stands for Niv, S stands for Shalev and O stands for Omri, the founders) group of Israel, it is known for its products of zero-click surveillance and faced many suits due to those products. Apps like WhatsApp, Facebook use end-to-end encryption by which they can't be traced or tracked. But the product made by the NSO group called Pegasus, surpasses the encryption barrier just by making a call to their number and it can delete the call after done, it also allows the user to read the encrypted messages, calls. Pegasus spyware enters through a backdoor into any device and the owner of the device will not know the existence of spyware. Once installed, it uses a zero-click exploit, can harvest any data from the device and the user gains full control over the data. An international media consortium had reported that over 300 verified Indian mobile phone numbers were on the list of potential targets for surveillance using Pegasus spyware. The NSO group specified that the spyware was built solely for governments and law enforcement agencies to gain useful hidden information, this fact alone does not guarantee the individual's privacy.
- The bench of the apex court had reserved an order on September 13, it wanted to know whether the Centre used the Pegasus spyware through illegal methods to snoop citizens. The pleas seeking independent probes are related to reports of alleged snooping by government agencies on eminent citizens, politicians by using Israeli firm NSO's spyware Pegasus. There should be a deeper probe into this matter, there should be an action as soon as possible as it might be a matter of national security.
- Apple sues NSO group, reveals new details on how Pegasus was used for attacking some iPhone users

VIII.II JOKER MALWARE:

- Joker Malware is malware that is created to steal private information like credit card and debit card data. Joker malware silently enters a device when a user installs an application infected by the malware, this malware is dangerous and has infected over 200 applications on the Google play store. Google took steps and deleted the apps that were exposing the users' data to malware. On 21 November 2021, the malware resurfaced and affected 15 applications on the play store. Reports suggest that the Joker malware steals money from affected users by subscribing to unwanted paid subscriptions without their consent. It simulates the device with advertisements without knowledge of the user and then steals the victim's SMS messages including OTP(One Time Password) to authenticate payments. This time, two new variants of the Joker Dropper and Premium Dialer spyware have been discovered in the Play Store. These were found hiding in some legitimate applications.
- It stated the malware ***"adopted an old technique from the conventional PC threat landscape and used it in the mobile app world to avoid detection by Google."***
- Joker malware discovered in multiple apps with thousands of installs on the Google Play Store

VIII.III EMOTET BOTNET:

- Emotet is a type of malware, also known to be the king of malware, as a type of botnet which enters into a computer system when a user opens the link sent by the attacker via email which looks legitimate. It spreads from one system to another, enabling it to be a bot in the botnet. A botnet is a group of infected systems which attack a specific computer or a server by sending more commands than it can handle. The infrastructure used by Emotet involved thousands of servers located across the world. All of these had different functionalities to manage the computers of the infected victims, and spread to new ones, to serve other criminal groups, and ultimately make the network more resilient against takedown attempts. The attacker used Emotet malware in emails, using keywords like healthcare and COVID 19 preventive measures, to clickbait the user and obtain access to their information. Eight law enforcement authorities in January 2021, combined and participated in taking down the infrastructure Emotet had been using to infect the ransomware.

- International team disables Emotet, world's most dangerous malware.

IX. WHAT CAN AN INDIVIDUAL LEARN FROM THE ATTACKS HAPPENING?

An individual can try to be safe by not clicking links from random spam and illegitimate emails. Individuals stepping onto websites or platforms, consider reading the privacy policy and accept the cookies only if needed. Individuals trusting everything they see on the internet is a victim of these attacks, as the attacker targets specific people. Observe the words and the email id, and ignore the spam section of the email interface.

X. WHAT CAN AN ORGANIZATION DO TO SECURE DATA PRIVACY?

"Data privacy software can help you achieve compliance by automating data privacy principles". Understanding the needs of the consumer is a vital part of every organization. Adding encryption, authentication, can help an organization secure data privacy. Privacy software tracks your deadlines for each data subject request and helps you understand customers better.

XI. NEED FOR A REFORM :

Data protection laws like GDPR are prevailing in other countries with appropriate measures to ensure data privacy and protection of its citizens. To ensure data privacy and protection of the citizens of India, India should consider the positives of GDPR approve a legislation in

India providing the punishments and descriptions accordingly. The parliament should bring the law into force, the PDP bill 2019 with a precise framework as soon as possible.

XI.I GDPR (GENERAL DATA PROTECTION REGULATION) OF EU[3]:

GDPR is the legislation brought in the EU (European Union) in May 2018, to ensure data privacy and processing. It applies to all organizations and businesses, those processing user data. This legislation provided strict rules and penalties. GDPR ensured that businesses processing users' data should protect it. If there is any misuse or exploitation of data, will be held liable and made to pay heavy compensation. GDPR ultimately places obligations on every processor(unit of the organization dealing with processing data) to maintain records of data and how it is processed, providing a much higher level of liability if breached.

Controllers (unit of the organization dealing with controlling data) are compelled to ensure that all contracts with processors comply with GDPR. One of the significant changes GDPR brought is by providing consumers with a right to know when their data is compromised. Organizations are required to notify the national authorities, as soon as possible to ensure citizens take measures to prevent their data from being abused. GDPR brought clarified the right to be forgotten, which provided additional rights and freedom to people who no longer want their data to be processed, to have it deleted, there is no ground for retaining it. Consumers are also promised perceptible access to their data in terms of how it is processed. Organizations should meticulously mention how they use customer information in a clear, precise, and understandable way.

Every organization should have a ***DPO (Data Protection Officer)***. It imposed a duty on all organizations, to report a data breach or misuse of obtained data, unauthorized access into accounts in under 72 hours. If the organization fails to comply, it will be held liable and accountable for any loss of personal information, and a heavy penalty will be imposed ***(10***

[3] EUROPEAN UNION.

million Euros or 4% of the company's annual global turnover), according to the severity of the breach.

XI.II RULES TO PROTECT CARD DATA:

Payment Card Industry Data Security Standard (PCI DSS), is a set of rules for protecting sensitive payment card information and cardholder data. The purpose of PCI DSS is to increase controls around cardholder data to reduce credit card fraud. The objective is to create an additional level of protection for card issuers by ensuring that they meet minimum levels of security when they store, process, and transmit cardholder data. After proper registration, private organizations can join the ***PCI DSS, MasterCard, American Express, Visa, JCB International, and Discover Financial Services established the PCI SSC*** in September 2006 as a governing entity that mandates the evolution and development of PCI DSS.

XII. CONCLUSION:

Data Protection is effective when done for the right purpose and with transparency. The data collected should be specific for the intended purpose. There should be a minimum data requirement and accountability of the website holder.

There is a need for accuracy. Internet privacy has attracted the attention of internet users, due to incidents of privacy breaches and the evolution of technology. Regularly assess privacy settings on your accounts. You may be sharing more information than just name and age with people you've never met.

REFERENCES:

I. Internet Sources:

- *https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/.*
- *https://indianexpress.com/article/technology/tech-news-technology/godaddy-reports-data-breach-data-of-1-2-million-customers-impacted-7636925/.*

- *https://timesofindia.indiatimes.com/business/india-business/security-breach-8-2tb-data-up-for-sale-on-dark-web/articleshow/81769741.cms.*
- *https://timesofindia.indiatimes.com/gadgets-news/apple-sues-pegasus-spyware-creator-nso-group/articleshow/87880298.cms.*
- *https://www.notebookcheck.net/Joker-malware-discovered-in-multiple-apps-with-thousands-of-installs-on-the-Google-Play-Store.581012.0.html.*
- *https://www.thehindu.com/sci-tech/technology/internet/international-team-disables-emotet-worlds-most-dangerous-malware/article33677419.ece.*