RIGHT TO PRIVACY AND DATA PROTECTION

Written by ***Pallavi Patel***

2nd Year BA LLB Student, ICFAI University, Dehradun, India

ABSTRACT

The epidemic has changed the life of each and every individual, 2020 was the year in which the globe turns into digitalization globe. The necessity of data and data movement was highlighted as being one of the years with the bright spots. The proportion of internet users around the world throughout the world has increased around 298 million additional users were added from January 2019.[i] So with the upheaval in digitalization concerns about the security of data, in other words, the right to privacy, are indeed widespread. The right to privacy pertains to a person's individual ability to regulate how data is captured, used, and disclosed. Furthermore, the evolution of technology (specially in epidemic period) has created a new set of privacy and data protection concerns.

A person might be readily damaged by the availability of deceptive digital data that could be transmitted to an unauthorized third party at fast speed. This increase in the use of personal data has numerous advantages, but it also has the potential to cause issues (For example Pegasus spyware issue which is going on in India).

The subject of data protection has proven to be rather hard in Europe, as well as the rest of the globe, for several decades and much more so now. We come forward with so many stories every now and then about huge data breaches from well-known organisations and corporations, which causes serious damage to an individual's privacy.

Tracing back to the past the **General Data Protection Regulation** (GDPR) took four years to get it authorised, and it was eventually approved on April 14, 2016. On May 25, 2018, the EU (European Union) General Data Protection Regulation, or GDPR, went into effect[ii]. The major goal is to guide and regulate how firms across the world manage their customers' personal information, as well as to create stronger and unified data protection for all EU citizens.

One of the key change was made in respect to privacy. Privacy by design is a popular informal concept that states that each new service or business activity that uses personal data must address how that data is protected. Privacy by default simply implies that when a client purchases a new product or service, the tightest privacy settings are applied automatically. This implies that the user should not have to modify their privacy settings manually to pick the most restrictive option. As a result of the GDPR, including data protection as a fundamental design feature becomes an inherent goal of every system design, right from the start. Data security is also inextricably connected to the implementation of comprehensive cybersecurity measures to fight against all types of cyberattacks, and so necessitates the investment in appropriate security processes and alternatives.

Apart from forcing firms and organisations implement greater data protection and overall security postures, one significant effect of these rules is the convergence of efforts across many industries and sectors all over the world.

On the other hand **The Asia-Pacific Economic Cooperation (APEC) Privacy Framework**[iii] is an essential instrument for supporting the establishment of adequate information privacy safeguards and guaranteeing the free flow of information in the Asia Pacific region. The framework began in 2003, was adopted by APEC in 2004, and was executed in 2005. The necessity of developing adequate privacy safeguards for personal information, notably against the detrimental repercussions of unwanted intrusions and abuse of personal information, was recognised in the development of this Framework on information privacy protection.

Though both of these regulation are based on earlier privacy protection regimes from the 1970s.

But India is still lacking somewhere in data privacy protection law which have to be addressed earliest because privacy is a fundamental right of each and every individual and it has to be primarily placed.

Information Technology Act, 2000 was one of the initiative for data privacy. As per that companies that handle sensitive personal data or information are responsible for any loss caused by their failure to adopt and maintain appropriate security policies and procedures, according to the IT Act. The Sensitive Personal Data Information(SPDI) Rules, which were enacted in response to the IT Act as IT Act does not cope to define reasonable security, provide basic data protection requirements for sensitive personal data. The SPDI Rules aren't meant to

be complete, but they do mandate that businesses establish a privacy policy and get consent before collecting or transmitting sensitive personal data or information.

Further and recent initiative which is still awaited is Personal Data Protection Bill, 2019.

RIGHT TO PRIVACY IN VIEW OF INDIAN CONSTITUTION

The first effort to safeguard an individual 's right to privacy from undue governmental intervention occurred in the Constituent Assembly, when Mr. Kazi Syed Karimuddin introduced an amendment to protect persons from unreasonable search and seizure, similar to the American and Irish Constitutions. Despite the fact that this clause already exists in the Criminal Procedure Code, Dr . B. R. Ambedkar approved the modification, calling it a "useful proposal" that must be "beyond the grasp of the legislature." The right to privacy, on the other hand, did not find a clear and unambiguous position in the Constitution.

Under the Indian Constitution the right to privacy has been considered as an unarticulated basic right. The Indian Judiciary was driven to exert extra effort in preserving this right by the State's increasing violations of it on grounds. "No individual shall be deprived of his life or personal liberty except in according to procedure established by law[iv]," according to Article 21 of the Indian Constitution.

The fundamental goal is to prevent infringement on personal liberty and deprivation of life unless it is done in accordance with legal procedures. When a person is robbed of life or personal liberty by the state, as stated in Article 12 of the Indian Constitution, he may utilise.

Leading case which brings in light the Right to Privacy is

M.P. Sharma & Ors. vs. Satish Chandra and Ors- It was one of the Supreme Court's initial decisions on the right to privacy in India. After a company went into liquidation in 1952, the Government of India initiated an investigation into its activities under the Companies Act, 1913. The business had sought to steal cash and conceal the actual state of affairs from shareholders by fabricating balance sheets and records, according to the inquiry. In the instance of the case the court rejected to apply the Fourth Amendment's provisions in the form of a right

to privacy, stating that the Indian Constitution lacked a basic right to privacy comparable to that of the US Constitution's Fourth Amendment.

Kharak Singh v. State of Uttar Pradesh[v] (1962) in this instance, the right to privacy was raised to oppose the police's surveillance of an accused person. Kharak Singh was detained for dacoity, but owing to a lack of proof, he was freed. He was thereafter placed under observation by the Uttar Pradesh Police according to Regulation 236 of Chapter XX of the Uttar Pradesh Police Regulations, this was permissible. Kharak Singh then challenged the constitutional legitimacy of Chapter XX and the powers it gave police officers, claiming that they infringed on his basic rights under Article 19(1)(d) (right to freedom of movement) and Article 21 (right to equal treatment under the law) (protection of life and personal liberty).

The six-judge panel ruled that domiciliary visits throughout the right were illegal, which violate Article 21 but upheld the remainder of the Regulations. More crucially, the court ruled that the right to privacy is not a constitutionally protected right.

The concept of informational privacy has gained traction in recent years, but as this article demonstrates, India has a long history of privacy law. The majority of it focuses on privacy in the context of the harms that can be produced by a breach of privacy.

Govind v. State of Madhya Pradesh[vi], similar to Kharak Singh versus State of Uttar Pradesh, Govind challenged the constitutionality of the Madhya Pradesh Police Regulations pertaining to surveillance, including domiciliary inspections. Govind claimed bogus allegations against him, and as a result, he was placed under police observation.

R Rajagopal and Ors v. State of Tamil Nadu- Which acknowledged tortious remedies for privacy intrusions as well as the capacity to sue for damages.

Justice K.S. Puttaswamy v. Union of India(2017) On August 24, 2017,

The lawsuit was brought by retired High Court Judge Puttaswamy, who was challenging the government's proposed standard biometrics-based identity card, which would be required for access to government services and benefits. The government contended that the right to privacy was not specifically protected by the Constitution. A 9-judge Supreme Court bench gave a unanimous decision in Justice K.S. Puttaswamy vs. Union of India and several related issues,

stating that each individual has a basic right to privacy under the Indian Constitution. Despite the fact that the judgement was unanimous, there were six unique concurring decisions.

The Supreme Court's wide interpretation prompted a flurry of government measures aimed at enacting Personal Data Protection regulations.

Moreover, in July 2017, in response to calls for a thorough data protection law, the Ministry of Electronics and Information Technology (MEITY) formed a 10-member committee to research data protection concerns and draught legislation. The committee was leaded by Justice B.N. Srikrishna, issued a report outlining the justification for a data protection legislative framework, as well as a draft **Personal Data Protection Bill in 2018**. The bill, on the other hand, is founded on the same core ideas that were initially laid forth in 1973 which further serve the basis of two major privacy protection frameworks in other countries,

- The General Data Protection Regulation (GDPR)
- The Asia-Pacific Economic Cooperation (APEC) Privacy Framework

Hence, the report served as the foundation for the measure that was finally introduced in parliament. The Ministry of Electronics and Information Technology presented the Personal Data Protection Bill, 2019 (the "2019 Bill") in the Lok Sabha on December 11, 2019. Before being introduced in the Lok Sabha, the 2019 Bill will be investigated and evaluated by a Joint Parliamentary Committee (JPC).

The 2019 Bill has made numerous enhancements and modifications to the 2018 Bill, but there are still certain issues that haven't been addressed that were fiercely disputed and discussed under the 2018 Bill. The JPC has already taken numerous extensions after consulting with experts and stakeholders, and the final draft was anticipated to be submitted during the present Monsoon session of Parliament.

The Personal Data Protection Bill establishes a legal framework for collecting and using personal data[vii]. Personal data and information provided or received in a spoken, written, or electronic form are not protected by a stand-alone personal data protection law in India. Though there are safeguards in place, they are spread among a variety of legislation, standards, and recommendations. Except when the government used its ability to designate "particular categories of personal data" as exempt from the local storage obligation, the 2018 draft required

"data fiduciaries[viii]" (known as data controllers, the entity that determines the purposes, conditions, and means of processing the personal data under GDPR).

A new requirement for data protection authority ("DPA") rulemaking might give more possibilities for public engagement and stronger right to privacy, duties for "anonymous data," and explicit requirements for "social media intermediaries."

Despite the obligation to keep a copy in India, personal data may be transmitted outside the India only if data fiduciaries have put in place additional measures, but the transmission of personal data is limited to some extent. For personal data protection the bill established a three-tiered system.

- **Personal Data[ix]-** This data might be stored wholly outside of India, with no limits on its transmission.
- **Sensitive Personal Data[x]-** This data may be sent outside of India, but it must be kept in India.
- **Critical Personal Data-** This data may not be transferred outside of India unless it is necessary to preserve essential interests.

While "privacy by design policy[xi]" was mentioned in the 2018 draft, the Bill would codify the need by forcing data fiduciaries to "prepare a privacy by design policy," thus outlawing "privacy by accident." The bill also establishes a process by which the Data Protection Authority (DPA) might approve privacy by design policies, subject to future laws, in which case the policy would be disclosed on both the data fiduciary's and the DPA's websites.

The Bill would introduce a new concept for "anonymized data" that would allow the DPA to set standards of anonymization by which data may be made no longer personal data, in keeping with rising interest in India in defining regulations for non-personal data.

Individual rights would be strengthened under this bill. The bill's broad application is one of its most appealing features. Except for those explicitly exempted, it will apply to all businesses in India if it is enacted. This would cover any company that collects data through automated ways. It broadly suggests that the personal data should only be handled with the consent of a free, informed, and particular individual, with the ability to withdraw that consent.

Furthermore, the bill aims to close the knowledge gap between customers and data fiduciaries on the use of personal data. It attempts to do this by restricting the goals of data processing and providing users with the right to access and know how their personal data will be used.

Personal data can be used without consent for certain justifiable reasons as authorised by the Authority, according to the 2018 bill.

The 2019 Bill expands the definition of "reasonable purposes" by include "functioning of search engines" in the list, which might be disclosed as a reasonable purpose under specific situations.

RIGHTS PROVIDED TO INDIVIDUAL (DATA PRINCIPAL) UNDER 2018 BILL

Individual rights would be strengthened as a result of the bill. The bill provided the rights as set out in the GDPR

- **Right to confirmation (Section 24 of The Personal Data Protection Bill, 2018)-** The data principal [xii]has the right to seek confirmation that the data fiduciary is processing or has processed his or her personal data, as well as a summary of the personal data being processed and the data fiduciary's processing actions.
- **Right to correction (**Section 25 of The Personal Data Protection Bill, 2018**)-** The data principal has the right to demand correction of inaccurate or misleading personal data, completion of the personal data, which is incomplete and an update any personal data, which is out of date.
- **Right to data portability (**Section 26 of The Personal Data Protection Bill, 2018**)-** The data principal has the right to receive personal data:
    - that the data principal has provided to the data fiduciary,
    - that the data fiduciary has generated in the course of providing services or using goods, and
    - that forms part of any profile on the data principal, or that the data fiduciary has obtained in any other way.

- **Right to be forgotten (**Section 27 of The Personal Data Protection Bill, 2018**)-** The bill gives data principals a limited right to limit or prevent the data fiduciary from continuing to disclose personal data where that disclosure
    - (i) has served its purpose and is no longer required,
    - (ii) the consent on the basis of which it was done has been revoked, or
    - (iii) the disclosure was made in violation of the Bill's or any other legislation in effect.

Recently the government revelation on Pegasus crisis grapples India. Pegasus spyware, created by Israeli cybersecurity, has made headlines when news outlets such as the Washington Post and the Guardian reported on suspected monitoring. According to the findings, this spyware was employed by over ten governments on journalists, activists, and other significant media figures. According to the claims, the spyware was used to target the phones of numerous important journalists and politicians in India. In the context of this report, it has been said by Justice B.N Srikrishna that "Privacy is a basic right under Article 21, anybody can file a petition in the Supreme Court under Article 32, claiming that their fundamental rights have been violated."

Due to the continuous development and consequences of international trade, particularly in light of the Internet's influence, it is critical that India work with the international community to create strong privacy and personal data protection regulations. The danger of privacy is also a barrier to providing a safe environment for Internet communication. Unless these challenges are solved, India will be unable to fully profit from the enormous potential and benefits that e-commerce offers emerging countries like ours. Though various attempts have been continuously coming forward but now India doesn't need an attempt but a successful attempt as privacy is a fundamental right of each individual and with enormous increase in internet it has to be placed primarily. A legislative framework must be developed that establishes clear criteria for the techniques and purposes of personal data assimilation both offline and online. Consumers must be informed about the risks of providing information willingly, and no data should be gathered without their express agreement.

Other sections in the Personal Data Protection Bill show the preventative approach used in the bill, which considerably raise compliance requirements for all companies that process data in India. Because the term "processing" has such a broad definition, these rules would apply to

all organisations. Privacy by the news media have become routine part of coverage of public figures.

The bill undoubtedly overprotects informational privacy at a considerable cost to the economy by restricting the space for innovation. As stated in the prologue, the bill protects individuals' privacy in regard to their personal data, prescribes the transit and use of personal data, establishes a trust relationship between persons and entities processing personal data, and preserving the rights of persons whose personal data is handled, establishing a framework for organisational and technical measures in data processing, establishing rules for social media intermediaries, cross-border transfer, and responsibility of entities processing such personal data The bill also aims to offer redress for unlicensed and damaging processes via the DPA.

REFRENCES

- As introduced in Lok Sabha, Bill No. 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
- Vijay Pal Dalmia, Partner India: Data Protection Laws In India - Everything You Must Know, Mondaq Connecting knowledge and people(13 December,2017), https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know
- Anirudh Burman, Will India's Proposed Data Protection Law Protect Privacy And Promote Growth?, CARNEGIE INDIA(March 9, 2020), https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217
- Ashish Aryan, Justice Srikrishna: Data protection law would have held govt to account, The Indian Express(July 23, 2021 1:31:04 pm), https://indianexpress.com/article/business/project-pegasus-justice-srikrishna-data-protection-law-would-have-held-govt-to-account-7417689/
- THE PERSONAL DATA PROTECTION BILL, 2018 KEY FEATURES AND IMPLICATIONS, INDUSLAW(August 2018), https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf

- Kurt Wimmer & Gabe Maldoff, India Proposes Updated Personal Data Protection Bill, COVINGTON (December 12, 2019), https://www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill/
- Aashit Shah and Nilesh Zacharias, RIGHT TO PRIVACY AND DATA PROTECTION Nishith Desai Associates, http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Right_to_Privacy_-_data_protection.pdf
- Personal Data Protection Law In India, Legal500 K&S Partners(October 2, 2020), https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/
- Simon Kemp Digital 2020: Global Digital Overview(30 January, 2020), https://datareportal.com/reports/digital-2020-global-digital-overview

BIBLIOGRAPHY

Books

- M.M. Eboch, Big data and privacy rights (Abdo Publishing [2017])
- Gaurav Goyal, Ravinder Kumar the Right to Privacy in India Concept and Evolution (2016) Websites
- As introduced in Lok Sabha, Bill No. 373 of 2019 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
- Vijay Pal Dalmia, Partner India: Data Protection Laws In India - Everything You Must Know, Mondaq Connecting knowledge and people(13 December,2017), https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know
- Anirudh Burman, Will India's Proposed Data Protection Law Protect Privacy And Promote Growth?, CARNEGIE INDIA(March 9, 2020). https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217
- Ashish Aryan, Justice Srikrishna: Data protection law would have held govt to account, The Indian Express(July 23, 2021 1:31:04 pm)

https://indianexpress.com/article/business/project-pegasus-justice-srikrishna-data-protection-law-would-have-held-govt-to-account-7417689/

- THE PERSONAL DATA PROTECTION BILL, 2018 KEY FEATURES AND IMPLICATIONS, INDUSLAW (August 2018) https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf
- Kurt Wimmer & Gabe Maldoff, India Proposes Updated Personal Data Protection Bill, COVINGTON (December 12, 2019) https://www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill/
- Aashit Shah and Nilesh Zacharias, RIGHT TO PRIVACY AND DATA PROTECTION Nishith Desai Associates http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Right_to_Privacy_-_data_protection.pdf
- Personal Data Protection Law in India, Legal500 K&S Partners (October 2, 2020) https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/
- Simon Kemp Digital 2020: Global Digital Overview (30 January, 2020), https://datareportal.com/reports/digital-2020-global-digital-overview

ENDNOTES

[x] Available at https://datareportal.com/reports/digital-2020-global-digital-overview
[ii] Available at https://www.trendmicro.com/vinfo/in/security/definition/eu-general-data-protection-regulation-gdpr
[iii] Available at https://www.apec.org/publications/2005/12/apec-privacy-framework

[iv] Available at https://indiankanoon.org/doc/1199182/
[v] 1963 AIR 1295, 1964 SCR (1) 332.

[vi] AIR 1975 SC 1378, 1975 CriLJ 1111, (1975) 2 SCC 148, 1975 3 SCR 946.

[vii] Personal Information has been defined as any information about an identified or identifiable individual in APEC Privacy Framework. And in GDPR Framework Personal Data or Personal Information has been defined as any information related to a natural person, or data subject, that can be used to directly or indirectly identify the individual/person.

[viii] data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data; as defined in Sec.3(13) of The Personal Data Protection Bill, 2019

[ix] Defined in Sec 3(29) of the personal data protection bill, 2018.

[x] Defined in Sec 3(35) of the personal data protection bill, 2018.

[xi] Elaborated in Sec (29) of The Personal Data Protection Bill, 2018

[xii] "Data principal" means the natural person to whom the personal data relates as defined in Sec.3(14) of The Personal Data Protection Bill, 2019