AI, Data Privacy And Law

Manvi Singh
Research Scholar
SGT University, Gurugram
Email: manvisinghlaw@gmail.com

Abstract

Machine Intelligence is the last invention that humanity will ever need to make."

– Nick Bostrom

With the expanse of technology and scientific inventions, Artificial Intelligence is gaining a spurge. Be it Alexa, Siri, Grammarly, etc are making our life easier.

From a simple shopping experience to literary proofreading to an endless list of smart devices, we are constantly and increasingly shifting to AI i.e. anything that is done by a robot via human brain stimulation.

With these modern applications being used the consumer data being used is also increasing exponentially and so is the threat to our data privacy.

In simpler terms, applications that have location enabled are an easy target for individuals involved in data mining i.e. sale and purchase of data for profitable trading.

For this, we can take certain preventive measures like cleaning the cache regularly or browsing in incognito mode where data is not stored on the device but is still available on the web.

So there is a need to address data privacy issues in our modern apps in a more efficient and effective manner. Data is the new fuel that is required by cross-border trade activities, governmental economic activities and our own social media platforms.

As we are progressing more towards a digital world, The Data Privacy Bill which was taken back was a small step that couldn't be eventually rolled out and was taken back.

Keywords

artificial intelligence, data privacy.

Reference to this paper should be made as follows:

Manvi Singh

AI, Data Privacy And Law

Vol. XIII, No.2
Article No.24,
pp. 200-213

Similarity Check: 2%

https://anubooks.com/journal/journal-global-values

DOI: https://doi.org/10.31995/jgv.2022.v13i02.024

https://doi.org/10.31995/jgv.2022.v13i02.024

Introduction

"Is it possible for machines to think?"

Not even a decade had passed since Allied forces won the World War II by breaking Enigma – the Nazi Encryption, Turing[1] in his paper "Computing Machinery and Intelligence" established the fundamental goal and vision of what we know as Artificial Intelligence today had.[2]

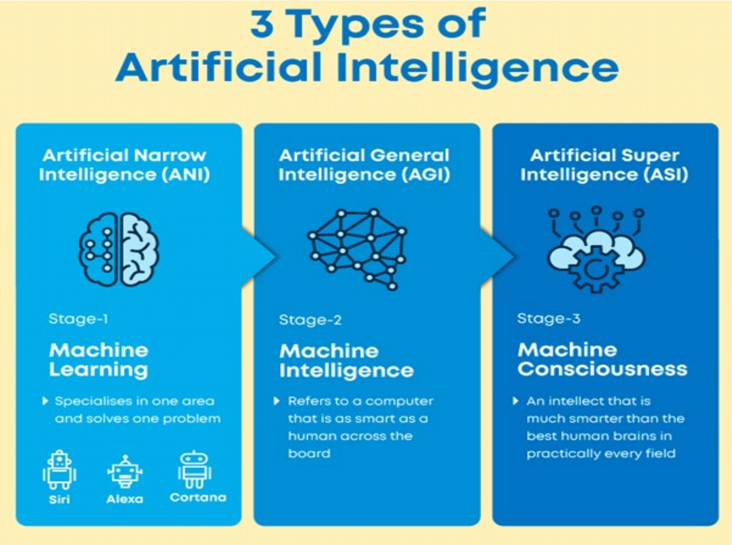
In today's fastest-growing modern world technology, one advancement that we see is in Artificial Intelligence.

As science and technology are continuously increasing at a rapid speed it is somehow difficult to say that what will the most advanced form of Artificial Intelligence but this is for sure that the future will be dominated by Artificial Intelligence and our life and all its aspects will involve this technology in some or the other way definitely.

Simply put, it refers to intelligence used by machines. This is machines using intelligence and performing functions of learning, planning, reasoning and problem-solving.

It is a kind of human brain being stimulated by the machines which will eventually help us in solving major challenges and crises which the human brain can't do effectively in proper channels.

From a shopping experience to literature editing, etc we see AI being used in diverse fields of our life. Be it Alexa or Grammarly we are not in existence in absence of AI.



3 Types of Artificial Intelligence

Artificial Narrow Intelligence (ANI)

Stage-1

Machine Learning

- Specialises in one area and solves one problem

Artificial General Intelligence (AGI)

Stage-2

Machine Intelligence

- Refers to a computer that is as smart as a human across the board

Artificial Super Intelligence (ASI)

Stage-3

Machine Consciousness

- An intellect that is much smarter than the best human brains in practically every field

To put one single definition of AI is difficult as not only that it is a multi-disciplinary subject with different approaches but it is one technology that is building intelligent machines and creating a paradigm shift in the industry.[3]

Analysis of The PDP Bill

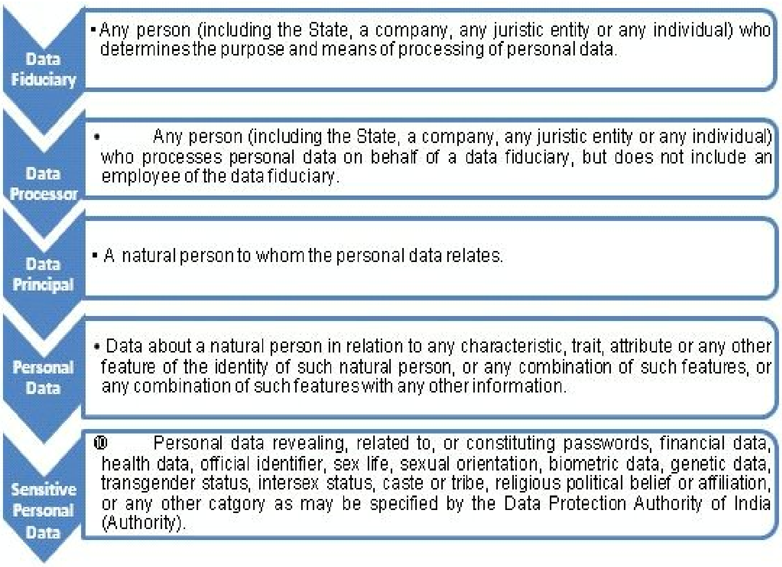
The major challenge that we see in AI is how our privacy is being invaded. Every day we become more prone to privacy being out in the common sphere.

Our primary concern today is to take effective and preventive steps so that while advancing with AI our privacy is not put at stake.

At present India has no codified rules, or regulations or guidelines for the regulation of AI.

Though to address the privacy issues in AI, the Data Protection Bill[4]2019 was introduced by Minister of Electronics and Information Technology – Mr. Ravi Shankar Prasad aiming to provide for data protection of individuals and also creating a Data Protection Authority for same.

Key Definitions Under The Draft Bill



Data Fiduciary

- Any person (including the State, a company, any juristic entity or any individual) who determines the purpose and means of processing of personal data.

Data Processor

- Any person (including the State, a company, any juristic entity or any individual) who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.

Data Principal

- A natural person to whom the personal data relates.

Personal Data

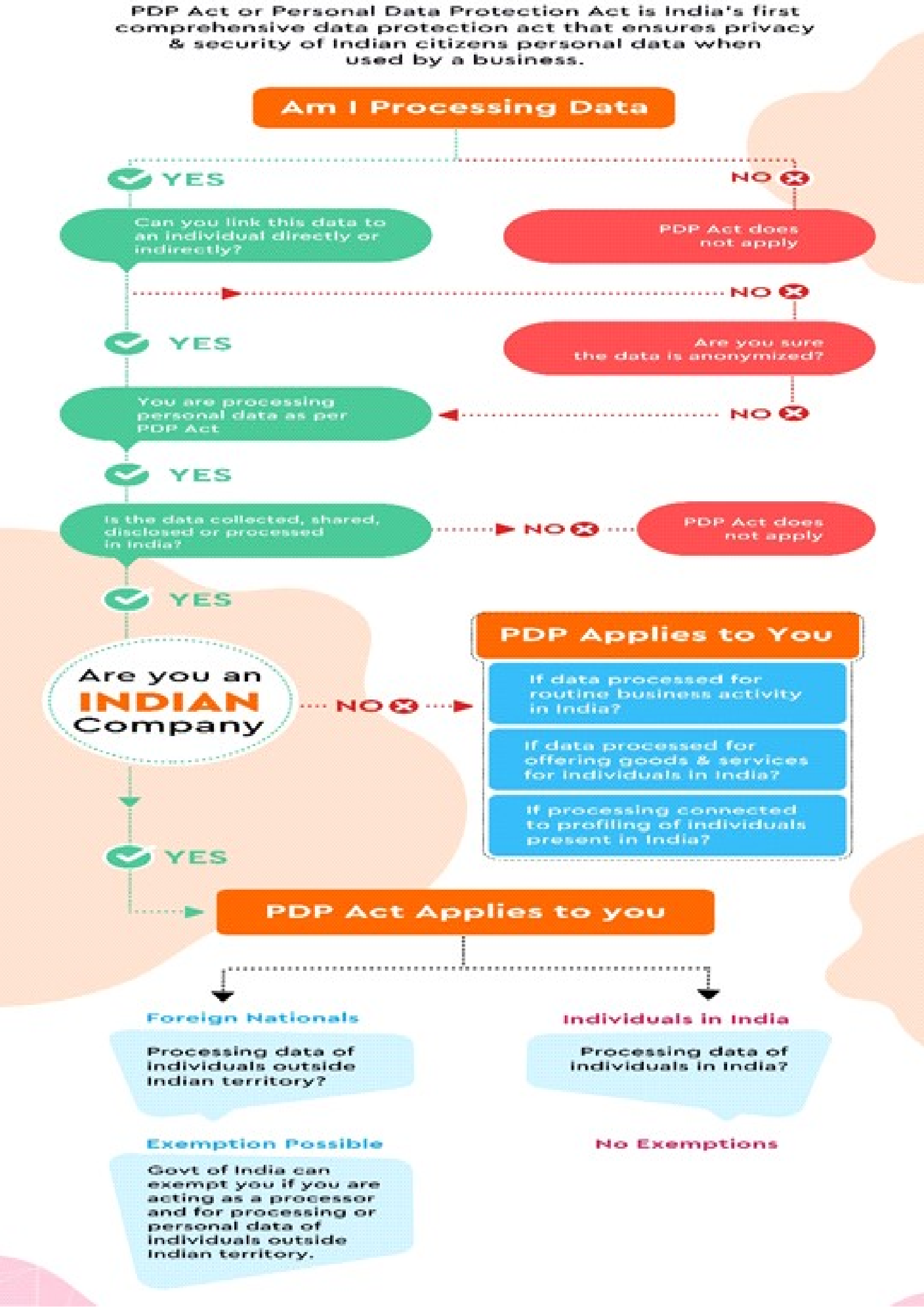
- Data about a natural person in relation to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

Sensitive Personal Data

⑩ Personal data revealing, related to, or constituting passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious political belief or affiliation, or any other catgory as may be specified by the Data Protection Authority of India (Authority).

Whether this Bill will have some intersection or not is still a question to be pondered upon. Whether this Bill will come out as a death band for AI or not is still to be reflected upon.

The Bill (initially rolled out in 2019) was withdrawn by Central Government on the ground that it carries with itself many loopholes and a "comprehensive legal framework" is required.



PDP Act or Personal Data Protection Act is India's first comprehensive data protection act that ensures privacy & security of Indian citizens personal data when used by a business.

Am I Processing Data
YES
NO
Can you link this data to an individual directly or indirectly?
PDP Act does not apply
NO
YES
Are you sure the data is anonymized?
You are processing personal data as per PDP Act
NO
YES
Is the data collected, shared, disclosed or processed in India?
NO
PDP Act does not apply
YES
PDP Applies to You
Are you an INDIAN Company
NO
If data processed for routine business activity in India?
If data processed for offering goods & services for individuals in India?
If processing connected to profiling of individuals present in India?
YES
PDP Act Applies to you
Foreign Nationals
Individuals in India
Processing data of individuals outside Indian territory?
Processing data of individuals in India?
Exemption Possible
No Exemptions
Govt of India can exempt you if you are acting as a processor and for processing or personal data of individuals outside Indian territory.

The major objectives of the Bill are as follows-

1. Effective and efficient personal and non-personal data management to enhance business value and also provide data security i.e. Data Governance
2. The practice adopted by the organization for the management of data in accordance with the objectives of data i.e. Data Management
3. Aligning the existing data privacy laws with data protected and secured i.e. Data Privacy and Protection

There are the following issues[7] as to which legal implications relate -

1. AI is borderless and the processing of data occurs in different geographical areas so there is not always a possibility that the state has **jurisdiction** over the same. So this extra-territorial applicability of the data protection framework poses great concern. There should be a legal framework in India so that regardless of where data is located the entity can be dealt with.
2. The **person** whose data is to be safeguarded i.e. one who possesses data should be clearly identified. Whether it is a natural (living) or a juristic (one given legal personality by law for example company)data protection framework would apply to both. For Example PAN of a company is the data of a juristic person which also needs protectionand and should be included in the data protection framework.
3. Reasonable identification of personal **data** is another concern that can be recognized in an indirect and direct manner regardless of the veracity of the same.
4. The **entity processing** the data should be held **accountable** for the same. That is this entity should bear the responsibility of ensuring the protection of both public and private data of entities. The process should have adequate transparency so that misuse of data is also prevented. Data processors and controllers should take it upon its shoulder to protect data used for AI algorithm.
5. The **consent** of the data subject should be acquired if the data is for use other than legitimate interest, public interest, major interest and other residuary grounds of interest. There should be no relaxation of consent without proper justification and reason.
6. Since children are now technology friendly, it has brought them to vulnerable scale of being attacked and so a cautious approach is to be adopted for same. Not only proper consent of parents or guardians is required but the organization using **child data** should take extra steps of security like verifying age with help of Government issued documents.

There should be proper framework for these pointers so as to provide a comprehensive legal and statutory framework.

Though the Bill categorized the data into the following categories –

I. Critical – This will be defined by the Government time and again which can be stored and processed in India only.

II. Sensitive – This includes an individual's health, sexual orientation, financial information etc and is allowed to be stored only in India. But with explicit consent can be allowed to be stored and processed outside India.

III. General –There is no constraint on the storage and processing of data and is one that doesn't fall into either of the above categories.

With AI increasing in consumer applications especially, the onus is on the service provider and government to ensure that people's trust and confidence are maintained in real-time when they use health devices, home smart devices, etc.

❖ **Government Exemptions**

For the interest of law enforcement, it is a well-established principle in all legal systems that states are entitled to exemption from data protection and data privacy laws so that they can effectively discharge their state functions.[8]But these exemptions should have a limited safeguard for their exemptions is another concern.

There are the following state exemptions in Bill-

1. Non - consensual processing of personal data by the state is permitted if required for service provision or benefit or for issuing permits and certificates to a person known as data personal (Section 12).

The consent of data personnel over his data is the central theme under the data protection framework and should not be taken lightly.

In Puttaswamy[9] judgment it is held that con-sensual processing of data can take place only if it is necessary and proportionate to achieve legitimate state aim. But in this Bill, if it doesn't specify the limits of proportionality, there is a risk of constitutional challenge.

2. For 'sovereignty and integrity of India, 'public order, 'friendly relations with foreign states and 'security of the state', the Central government has the power to suspend some or entire provisions of the Act (Section 35).

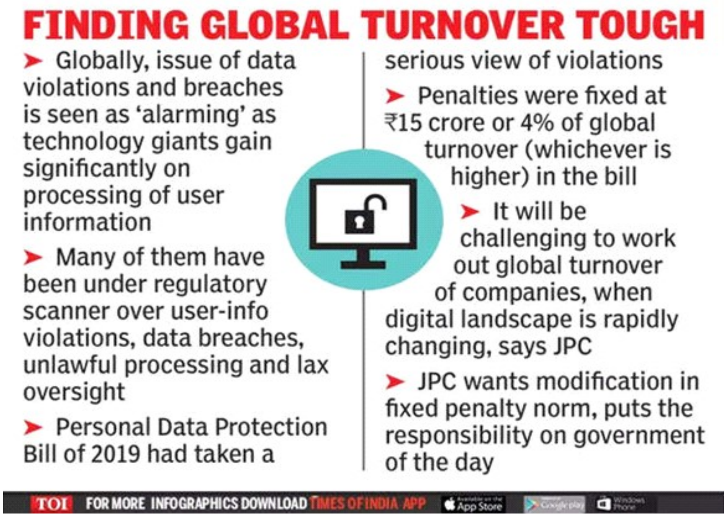
If for the above-mentioned reasons, any interrogation and investigation are to be carried out then the state is not liable to warrant consent for personal data information. This exemption is more expansive in nature than the previous exemption in the interests of prevention, detection and investigation of *any* offense or any other contravention of *any* law.

Penalties and Contraventions

For a major violation under the Bill, a penalty of Rs 15 crore or four percent of an entity's global revenue whichever is higher will be imposed. A penalty of Rs 5 crore or two percent of the global turnover of the entity whichever is higher will be imposed in case of a minor offense.

There is also provision for a jail term, for officers of the data entity.

Though there is uncertainty about how extra-territorial jurisdiction offenses will be covered under the Bill as the India Penal Code has no coverage of offenses committed outside the borders of India.



FINDING GLOBAL TURNOVER TOUGH

- Globally, issue of data violations and breaches is seen as 'alarming' as technology giants gain significantly on processing of user information
- Many of them have been under regulatory scanner over user-info violations, data breaches, unlawful processing and lax oversight
- Personal Data Protection Bill of 2019 had taken a serious view of violations
- Penalties were fixed at ₹15 crore or 4% of global turnover (whichever is higher) in the bill
- It will be challenging to work out global turnover of companies, when digital landscape is rapidly changing, says JPC
- JPC wants modification in fixed penalty norm, puts the responsibility on government of the day

TOI FOR MORE INFOGRAPHICS DOWNLOAD TIMES OF INDIA APP

Data Protection Bill Withdrawn

There were certain reasons for why this Bill which was introduced for a a comprehensive legal framework was withdrawn.

I. There might be encryption keys that are beyond the reach of national agencies and so physical data accession is difficult.

II. The issue of national security and the definition of reasonable security is subjective and open end terms that have different meanings for different individuals and so, as a result, the individuals might claim that the state is intruding in their private and personal sphere of theirs.

III. Google and Facebook known as the biggest technology giants have criticized this Bill as they claim that the data localization policy will have a domino effect i.e. accentuating situations in their country as similar to the ripple effect in their own country also.

IV. Reverse engineering will have to be practiced by start-ups that are essentially based on AI and this new Bill introduced will have to take steps to restrict data entry points or will have to recede in technology when data information is required.

V. The Bill will result in increasing compliance procedure increase for small enterprises and consequently they will not be able to cope up with data privacy laws.

VI. Content creators are not taken as intermediaries under the Bill but the content that they are publishing, for that the onus lies on them and they are responsible for it. So defining this and taking preventive steps for them is difficult.

VII. In our smart devices only 'trusted hardware' can be used which includes your smartphones, laptops, etc and it is again a difficult task with growing levels of competition among consumers and producers.

Data Leaks and Their Prevention

As the information is passed from one individual to another in today's modern world, the onus of data protection lies on the person who first had or gave the information.

Data is sensitive so it should be kept in mind by the distributor that data is secure and safe.[11]

Irrespective of age and gender data can be used by anyone for their malicious reasons and so strong preventive steps should be taken to avoid data leaks.

i. Latest Data Breach

ii. Food chain belt – Domino's has seen a data breach of about 18 crore order details including names of customers, their IDs, contact numbers, etc breached. Moreover, an estimate of 10lakh credit card details is also available for use which estimates to be about 13TB of a data database breach.[12]

iii. For passengers registered between August 2011 to February 2021 data has been disclosed in a breach which includes name, date of birth, etc but as such, no passwords and credit card details got leaked due to the hack of the Passenger Service System provider SITA in February 2021. [13]

Causes of Data Breach

i. Password hacking is the most common form of reason for data breaches. A weak or lost password is a vulnerable cause for the opportunist to hack.

ii. If any application or software is poorly managed or designed without an effective security system it is liable to be hacked first as opportunists can easily crawl into database.

iii. A malicious software that allows opportunists to peep into our system and cause harm to it and potentially connected systems.

iv. Allowing permissions and cookies without reading the terms, we allow access to suspected and opportunist hackers.

v. Threats are also coming from internal organizations and it is quite malicious and can be in any form like employees, business associates, etc as the data can be easily provided to hackers because they enjoy control of data.

How do Data Breaches Occur?

i. Any misplaced device like your laptop, phone or for that matter any paper document can be a huge disaster for the organization or individual the moment a hacker gets access to it.

ii. An unhappy or unsatisfied employee is one big threat to the organization He has some control of data and he knows the value of the same so he can use this data online or physically putting the organization at risk.

iii. There is software or spyware known as Crimeware which is here to steal sensitive and personal data. Crimeware also known as spyware is a software that is designed to steal our personal and sensitive data.

iv. Criminals keep hold of our locked files and don't give them access until we pay them which happens to be Ransomware which is a kind of malware that employs encryption to hold victims' information at ransom.

v. When the backend database is attacked, the information is manipulated after access and now the original user can't access information without the hacker's permission as the data is altered or modified by him and is known as SQL injections SQL injections(SQLi) which is a web security vulnerability.

vi. The hacker acting as a trusted source contacts the person via mail, WhatsApp, etc and tricks the person to install malware or give personal information and this is known as Phishing.

vii. We put our personal information when we sign in to a web application and that is where we make ourselves prone to data leaks.

viii. A skimming device is put on a card reader and all our information is accessible via that device and this is known as payment card skimming, usually occurring at ATMs or petrol pumps.

ix. Certain information is passed on cache that is personal information and may be confidential.

x. Without a holder of data, a strange person gets access to it and this is known as cyber espionage or cyber spying.

Where is Stolen Data Used?

1) Taking benefit from data i.e. using it for own
2) Spam and unwanted marketing
3) Blackmail and extortion
4) Apply for credit cards and loans. Distribute in the dark web.
5) Phone scams and Transfer of money illegally
6) Get medical care with your health insurance

Prevention and precaution of data leakage

We always need to keep our guard up so that our data is safe and secure as this data breach can be a serious harm to an individual's reputation in society. We intentionally and knowingly put our data accessible, thinking that it will be safe and will be used only for the purpose for which we are providing the data. But these light steps of ours make our data more vulnerable.

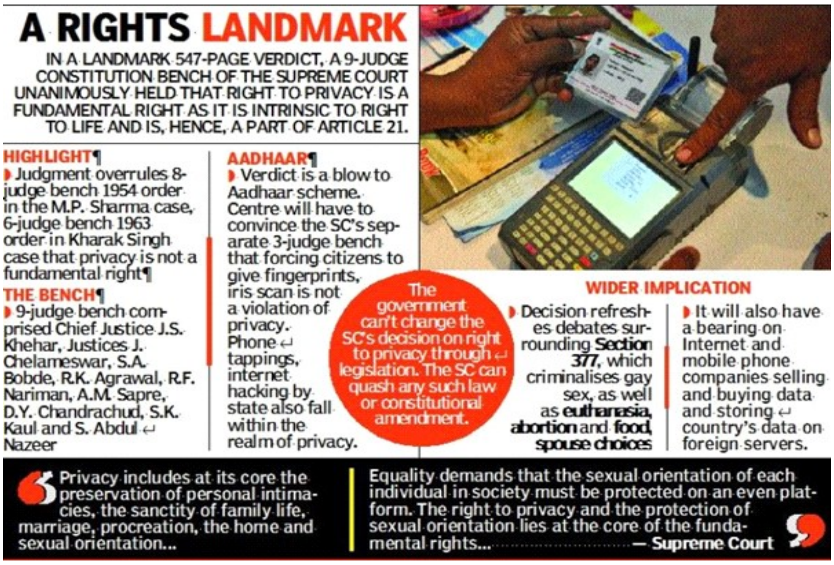
We should also follow the following steps for added security:-

- Shred documents
- Use safe and secure websites
- Give Social Security number only when absolutely required
- Create strong, secure passwords using uppercase and lowercase letters, non-sequential numbers, and special characters symbols
- Use different passwords on every different account. This will minimize the damage if one of our account passwords is revealed.
- Must upgrade computers and mobile devices to the latest versions of operating systems and applications.
- Frequently monitor online transactions and monthly financial account statements to make sure transactions are precise
- Regularly check credit reports to confirm that identity thieves are not using credit card accounts or loans in your name.

Right To Privacy

Under different legal traditions restraining private and governmental actions which are threatening the privacy of individuals is been talked about as the 'right to privacy.[14]

'A Free and Fair Digital Economy' was a report titled by B.N. Srikrishna's Committee's [16]which urged that Data Protection Bill should be treated as a dynamic and pervasive law and not a statutory regulation.



A RIGHTS LANDMARK

IN A LANDMARK 547-PAGE VERDICT, A 9-JUDGE CONSTITUTION BENCH OF THE SUPREME COURT UNANIMOUSLY HELD THAT RIGHT TO PRIVACY IS A FUNDAMENTAL RIGHT AS IT IS INTRINSIC TO RIGHT TO LIFE AND IS, HENCE, A PART OF ARTICLE 21.

HIGHLIGHT¶

- Judgment overrules 8-judge bench 1954 order in the M.P. Sharma case, 6-judge bench 1963 order in Kharak Singh case that privacy is not a fundamental right¶

THE BENCH¶

- 9-judge bench comprised Chief Justice J.S. Khehar, Justices J. Chelameswar, S.A. Bobde, R.K. Agrawal, R.F. Nariman, A.M. Sapre, D.Y. Chandrachud, S.K. Kaul and S. Abdul ↵ Nazeer

AADHAAR¶

- Verdict is a blow to Aadhaar scheme. Centre will have to convince the SC's separate 3-judge bench that forcing citizens to give fingerprints, iris scan is not a violation of privacy. Phone ↵ tappings, internet hacking by state also fall within the realm of privacy.

The government can't change the SC's decision on right to privacy through ↵ legislation. The SC can quash any such law or constitutional amendment.

WIDER IMPLICATION

- Decision refreshes debates surrounding **Section 377**, which criminalises gay sex, as well as **euthanasia, abortion** and **food, spouse choices**
- It will also have a bearing on Internet and mobile phone companies selling and buying data and storing ↵ country's data on foreign servers.

Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation...

Equality demands that the sexual orientation of each individual in society must be protected on an even platform. The right to privacy and the protection of sexual orientation lies at the core of the fundamental rights... — **Supreme Court**

The entire committee believes that a proper legal framework is required and that protection of personal data is the recognition of the 21st-century developing world which holds the key to development, innovations and empowerment.

It suggests that essentially India should adopt from best practices all over the world for data protection plowing for itself the ways to overcome the challenges it faces as a developing nation in the global south.

Under Article 21 comes our Right to Privacy wherein it is stated that is the duty of the state to bring a regulatory legal framework for the protection of its citizens from the dangers of data breaches.

The report suggests that a fiduciary relationship should be maintained i.e. the data being shared by an individual with the entity must be protected and it is assumed that their data will be used only for the legal and valid purpose for which it was primarily given.

Privacy can be restricted in the following circumstances:-

a. In restricting the right a legitimate state interest exists
b. To achieve interest restriction is necessary and proportionate
c. Law has provided for restriction

The following recommendations were made by The Committee:-

a. The processing of data which includes collection, recording, etc is to be done for a clear, definite and lawful purposes, in which only necessary data is to be collected.

b. Users will be able to restrict or prevent any data from being displayed once the purpose of data is being served or withdraw consent from the disclosure of data. "Right To Be Forgotten"

c. Personal data can be stored on Indian servers and transferred with consent whereas personal data of critical nature can be only processed in India. Moreover sensitive personal data like passwords, biometric data, etc can't be processed outside India without explicit consent.

d. Data Protection Authority has to be established which carries out the following functions:-

o Interest protection of data principals

o Prevent misuse and laws compliance

o Establish a grievance redressal mechanism

Points that are to be kept in mind, regarding the Right to Privacy-

a) This right is not guaranteed expressly under the Indian Constitution.

b) Greater personal information fosters greater privacy

c) This is a right guaranteed basic by the Universal Declaration of Human Rights,1948

d) The International Covenant on Civil and Political Rights Act, 1966 to which we as a nation (India) also have signed also states that no individual should be subjected to unlawful and arbitrary interference.

Conclusion

In today's world where data is always at risk due to individuals access continuously increasing for different types of Applications. And as a result of this, data breach is one major problem that we witness which is required to be addressed. Data protection and security are our rights as an individual so as to maintain individuals privacy. Moreover, data thefts are also increasing wherein data is being traded.

The right to privacy has to be addressed and balanced with other Fundamental Rights.

Moreover, we also have to analyze the following:

- How will the intention of the data entity and data processor be proved?
- Is it possible to predefine the implications of usage scenarios in a T&C document?
- Prevention of data access to the non-state actors e.g. malicious marketers, terrorist groups, anti-social elements, etc.
- Co-operation among International states – accountability gaps

- Digital platform/app product liability
- Individual criminal liability and strict liability

I would like to conclude that effective and efficient steps should be taken to protect data and prevent its theft, especially in today's time when Artificial Intelligence is garnering our life everywhere in all aspects.

References

1. Turing, A.M. (1950). Computing Machinery and Intelligence, Mind 49. 433. https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf.
2. BUILTIN, https://builtin.com/artificial-intelligence(last visited Oct. 25,2022).
3. My Great Learning. https://www.mygreatlearning.com/blog/what-is-artificial-intelligence/. (last visited Oct. 26,2022).
4. Writer Adda Data. https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf. (last visited Oct.29, 2022).
5. MONDAY. https://www.mondaq.com/india/data-protection/727776/decoding-the-personal-data-protection-bill-2018. (last visited Oct. 28, 2022).
6. PRIVADO. https://www.privado.ai/post/know-all-about-the-personal-data-protection-act. (last visited Oct. 30, 2022).
7. Majumdar, D., Chattopadhyay, H.K. (2020). Emergence of AI and its implication towards data privacy: From Indian Legal Perspective. Vol.3. *ILJMH.* 1. https://www.ijlmh.com/wp-content/uploads/Emergence-of-AI-and-its-implication-towards.pdf.
8. Goyal, Trisha. (2021). Personal Data Protection Bill: 4 Reasons Why Governments Bat for Data Localisation. News 18. December 06. 16.33. https://www.news18.com/news/opinion/personal-data-protection-bill-4-reasons-why-governments-bat-for-data-localisation-4525034.html.
9. Justice, K.S. (Retd). (2017). Puttaswamy vs Union Of India. AIR. SC. 4161.
10. Doval, Pankaj. (2020). Data protection panel against hefty penalties on tech giants. Nov 25. https://timesofindia.indiatimes.com/business/india-business/data-protection-panel-against-hefty-penalties-on-tech-giants/articleshow/87900358.cms.
11. Khan, Mantasha Wasi Ahmed. (2021). Data Leakage: Threats And Prevention. 9. *ICJRT.* 1. https://ijcrt.org/papers/IJCRT2109042.pdf.
12. FSMI. https://fsmi.in/sites/default/files/2021-04/fsmi-dominos-data-leak-press-release.pdf.
13. AIR India. https://www.airindia.in/images/pdf/Data-Breach-Notification.pdf. (last visited Nov. 1, 2022).

14. Central Information Commission. https://cic.gov.in/sites/default/files/Right%20to%20Privacy%20and%20RTI%20by%20Aditya%20Verma%20%20%281%29%20%281%29.p (last visited Nov. 1, 2022).
15. Venkateshan, J. (2022). Individual Privacy A Fundamental Right. Rules SC. Asianage. Nov. 1. 9:29 PM. https://www.asianage.com/india/all-india/250817/privacy-a-fundamental-right-says-supreme-court.html.
16. Ministry of Home Affairs. https://www.mha.gov.in/about-us/commissions-committees/ccsap-justice-retd-b-n-srikrishna-report (last visited Oct. 31, 2022).