IS YOUR PRIVACY RIGHT AS IT'S YOUR RIGHT

***Author**: Surinder Kaur Chawla, I year of Bachelor's of Technology in Instrumentation And Control Engineering from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar*

Abstract

Privacy is a fundamental human right. But as the technology got advanced and people got educated about the latest communication advancements and the Internet, the issue of privacy got highlighted. Privacy, which was earlier concerned with a person's property or choices of sexuality is now concerned with data over the web. The bigger tech companies like Google, Facebook, Instagram, WhatsApp, Amazon, Microsoft, etc are collecting their customer's data at a huge rate. And not only they are found guilty of collecting their user data but also selling it to third parties for their benefits. Nowadays, cyber crimes like leaking of data, using someone's photo or video, banking frauds, etc are increasing with the unawareness of the user. Technologies like HTML cookies, Web Beacons, Spyware, RFID, are used to keep an eye on the movement of the user. The user data is used to find the interest of the majority and can also be used to change the interest of the majority. Latest technologies like Biometrics, if leaked, can harm an individual brutally. The users are not even aware of their rights when their privacy is misused by someone else. The Indian Constitution provides the 'Right to Privacy' as a fundamental right to every individual of the country, either an Indian citizen or not. The country does not have a dedicated Data Protection Law, but it does have some rules and regulations governing electronic communications and businesses. There are prescribed punishments for almost every electronic or cybercrime as per the 'Indian Information Technology Act 2000' and the 'IT Amendment Act 2008'. The 'Personal Data Protection Bill' was introduced in the Parliament which does provide a lot of facilities to the user on how to privatize his or her data and introduces the concept of 'data localization within the country'. However, taking into consideration the integrity and sovereignty of the country, ensuring the safety of its people, and defence of the country, the Ministry of Electronics and Information Technology does take some of the harsh decisions like banning mobile apps which store personal data of the user. As a responsible individual, one should be aware of his or her rights and must stand for justice whenever required.

Introduction

Rights are an appanage that denotes what we are as citizens, as individuals, and as human beings. These are essential for leading a life of respect and dignity. Some rights find explicit mention in international and national documents while others are introduced through interpretive tools from the fundamental ones. The Right to Privacy is the most decisive and acceptable personal right that is identified as the most integral feature of Right to Life and Liberty and Right to Freedom and Speech.

Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively. The requirement for privacy is deep-rooted in human beings and hence the right to privacy is thought to be a fundamental right of every individual in society. It is a total of the Right to freedom of thought and conscience, the right to be alone, the right to control one's own body, the right to protect one's reputation, the right to live a family life, the right to have sexuality of one's own choice, the right to have limited access in the society, the right to have control over one's information, the right to get physically, mentally, emotionally, socially, intellectually separate from others.

Privacy barrier is a method by which one can ensure his or her privacy. Privacy barriers are categorized into three types; Physical barriers, Behavioral barriers, and Normative barriers to privacy. Physical barriers to privacy refer to preventing others from accessing and experiencing the individual in person. Behavioural barriers of privacy are related to behaviour that is reflected in one's communication through verbal language, body language, clothing, etc. Normative barriers of privacy are certain laws and social models of rules which restrain others from attempting to access or experience an individual.

Internet and Privacy

As technology got advanced, it transcended every sphere of human life. How privacy is protected and violated has changed with advancements in technology. The Internet Era and the advancements in wireless communication have brought new concerns about privacy by voluntary disclosures or involuntary acquisition of information. The curiosity of human beings for using the Internet and being connected with the world has led to a surprising fact that people share personal information over the Internet to an amusing degree.

Internet privacy is bothered about how the information of a user over the web is collected, stored, and used. Each digital machine like a computer, mobile phone, or laptop connected to the Internet has a unique IP address[1] which provides a unique identifier for every device that means the device, can be traced and this leads to significant privacy challenges. Your personal information is always at a risk of being shared even if it is stored in the best information security program because every time you visit a website, give out your email, do online transactions, fill out online forms, post on social media or even store your notes or photos online (or on the cloud storage), digital footprints are made which can be traced back. Just, for example, HTTP cookies[2]. These record the user's browsing history such as logging in and out, recording what pages are visited and for how much time, field names, passwords, addresses, and even payment card details (if allowed). By tracking cookies, especially third-party cookies, one can get a long-term record of the individual's browsing history.

Another example could be a web beacon[3] (also called a web bug or tracking bug) which is a technique used on web pages and emails to invisibly or secretly keep an eye over the accessed content by the user. Successful companies, therefore, use such technology to understand the targeted audience and advertise their product. As per the latest report, Microsoft said that nearly 75% of the U.S. recruiters and human resource managers use social networking sites, photos and videos sharing websites, personal websites, and blogs to research the candidates before recruiting. The same report revealed that 70% of the candidates are rejected based on their internet information. We all have identity proofs provided by the government, the information of which is stored in governmental controlled databases. If combined with the private organizations' databases[4] like hospitals, newspaper and magazine subscriptions, etc, one can create a large database of gender, age, income, lifestyle, marriage status, religion, details like Aadhaar Card number, Voter ID, interests, medical complications, and a lot which can be further used for data mining. Data mining[5] can have privacy implications which often involve using people's information in a way that they

[1] An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.
[2] An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data stored on the user's computer by the web browser while browsing a website.
[3] Also called a "pixel tag," "clear GIF" and "invisible GIF," it is a method for passing information from the user's computer to a third party website. Used in conjunction with cookies, Web bugs enable information to be gathered and tracked in the stateless environment of the Internet.
[4] A database is a systematic collection of data. They support electronic storage and manipulation of data.
[5] Data mining is defined as a process used to extract usable data from a larger set of raw data. It implies analysing data patterns in large batches of data using one or more software.

did not consent to or are not even aware of. Data profiling[6] can also be done in which one can identify, segregate, categorize, and generally make decisions about individuals known to the decision-maker only through their computerized profile.

Talking about the well-known identity proof Aadhaar Card, which uses biometrics such as facial recognition, finger scanning, and iris scanning. Biometrics[7] is the unique identity of an individual and needs to be protected but nowadays these are used either as primary or secondary methods of authentication and are replacing passwords. But like all other data forms over the internet, biometric data collection, processing, and storage are at the same level of risk. Just in case if an individual's banking details or job details are linked with biometrics, it could be a lot harmful to the individual. If the image or voice of an individual is being hacked by a hacker, it can be used for any criminal offence. Huge biometric databases have been exposed in the OPM hack, Biostar leak, and many other leaks. Hence, biometrics does provide the quickest way of authentication but does not provide the safest way of authentication and interfere with the privacy of an individual. Similarly, Spyware technology[8] enables an individual to gather information about the device's user and sell it to advertisers or other interested parties. RFID (Radio Frequency Identification) is a method that uses electromagnetic waves to automatically identify and track tags attached to different objects. It is one of the best methods of automatic identification and data capture but due to its small and compatible size and cheaper price, privacy issues due to RFID are increasing daily.

There are about 104.32 unique mobile number connections per 100 citizens globally, with India being at 110.18 mobile number connections over every 100 citizens. 53.6% of the 7.75 billion human population in the world are Internet users. Out of these 4.15 billion Internet users, almost 4 billion are only Google users, and such big companies store user data either as the name of the user or their email address. And the personal information is just increasing day by day. Social networking sites like Twitter, Facebook, Instagram, WhatsApp, Signal, etc. provide the space to share personal photos and videos that affect the user's privacy as cybercrimes. As per a recent report, 533 million Facebook users' data is leaked and is

[6] Data profiling is the process of reviewing source data, understanding structure, content and interrelationships, and identifying potential for data projects.
[7] Biometrics are physical or behavioural human characteristics that can be used to digitally identify a person to grant access to systems, devices or data.
[8] Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.

available over Dark Web for sale. About 80% of the user data including personal chats and photos were leaked and sold to third parties.

The dark web or sometimes called darknet is a subset of the Deep web[9] that has access to the Internet without disclosing the IP address or personal information of the user because it requires specialized web browsers and configurations. The interface is best meant for business deals but is also messy because the identities are not disclosed. Nowadays, the Dark web is mainly used for illicit data leakage, hacking, illicit financial trading either through Bitcoins or normal bank transactions, illicit drug deals, pornography, arms, violence, and a lot more.

Privacy in India (History)

Talking about the Indian scenario, earlier, privacy was meant to be concerned with a property only, especially land; but in the modern scenario, privacy has become a vast term covering fields like finances, sexuality, data security, and so on. In India, the right to privacy was not a fundamental act. Looking at the history, we have the M.P. Sharma V. Union of India (1954) case, in which a search and seizure warrant was issued in the offence of hiding the facts from the shareholders and submitting fake balance sheets. An eight-judge bench took the judgment declaring, for the security of the State was provided overriding powers of search and seizure. There is no such concept of the Right to Privacy in the Indian Constitution.

Similarly, in 1962, in the case of Kharak Singh V. State of Uttar Pradesh, Kharak Singh was convicted under the offence of Dacoity. But the police cannot find strong evidence against him, so they put surveillance over him under the UP Police Regulation which allows the police to suspect anyone having contact with Kharak Singh, domiciliary visits[10], and tracking. Kharak Singh filed a petition in the UP High Court asking for his Right to Privacy, Right to Movement, and Right to Life and Freedom. A six-judge bench states that domiciliary visits were unconstitutional but other visits were regulated. The Right to Movement under Article 19 (i)(D)[11] infringes with physical restrictions. The statement of Justice Subba Rao was a

[9] The part of the World Wide Web that is not discoverable using standard search engines, including password-protected or dynamic pages and encrypted networks.
[10] A visit to a private dwelling (as for searching it) under authority
[11] The right to move freely throughout the territory of India

remarkable one stating that Anybody can enjoy the freedom of movement anywhere for personal purposes. He questioned if the movement is being tracked, then how it is free?

Case Study - PUCL V. Union of India (1997)

One of the most remarkable cases in Indian history questioning the privacy of an individual in the country was the People's Union for Civil Liberty V. Union of India. In 1997, former Prime Minister Chandra Shekhar and 27 other politicians of the Indian National Congress accused the existing government of tapping their phones. A CBI investigation was done to unveil the widespread phone tapping by the government. Earlier, under Indian Telegraph Act 1885, Section 5 (2), the Central or the State government had the right to tap phone calls in the interest of integrity and sovereignty of the country or any public emergency. Against the unnecessary phone tapping, the People's Union for Civil Liberty filed a PIL in Supreme Court. The SC passed the judgment that the Right to Privacy is a fundamental right under the Right to Life and Personal Liberty under Art. 21 of the Constitution and tapping telephonic conversations hit the privacy of a person. In the Indian Telegraph Rules 1951, Rule 419(A) states that the ascendancy given by Section 5 (2) of ITA 1885 can be employed by the Union and State Home Secretaries only in case of emergency. But even after such a historical judgment by the court, the issue of privacy was not highlighted. Considering Niira Radia case of 2008-09, the Indian Income Tax Department taped the phone calls of the political leader, Niira Radia; then Telecom Minister, A. Rana; senior journalists, political leaders, and corporate house for around 300 days with over 5000 conversations, violating the Rule 419 (A) of Indian Telegraph Rules 1951 to collect evidence for 2G Scam. Moreover, the tapes were leaked out in the media and shown on television channels.

Case Study - Justice K.S. Puttaswamy V. Union of India

A phenomenal judgment was passed in the Aadhaar case of 2017. Justice K.S. Puttaswamy challenged the Aadhaar project of the Union of India. Aadhaar is the unique identity of the person issued by the Unique Identification Authority of India (UIDAI) to every citizen of the country in the form of an Aadhaar Card. The Aadhaar Card is an identity proof containing the personal information of a person like his demographic details, photograph, and even biometrics including fingerprints and iris scan. UIDAI states that it helps not only to identify the person but also has become a symbol of the digital economy allowing multiple avenues

for the common man. But many questions were raised by the petitioners that question the privacy of an individual as well as the security of the government databases.
In Dec. 2017, it was revealed that the large telecom company Bharti Airtel made use of Aadhaar-linked eKYC (electronic Know Your Customer) to open bank accounts for their customers without their knowledge or consent.

In Mar. 2018, a security researcher discovered that the state-owned utility company Indane had access to the Aadhaar database via an API[12], but they did not secure this way of entry. These incidents questioned the security and negligence of the government of India. Again, all such incidents and to prevent any harmful future incident, a writ petition was filed by Retd. Justice K.S. Puttaswamy and others against the Union of India. In the court, the petitioners said that the Aadhaar Act passed by the Government of India is unconstitutional and creates a tendency of the surveillance[13] state. Clearing the doubt of the petitioners, the honourable Supreme Court stated the Aadhaar Act does not tend to create surveillance as it stores minimal biometric data in the form of 'silos' which are prohibited for merging. It cleared that the UIDAI is purpose blind as it does not collect personal information like purpose, location, and details of transactions using an Aadhaar Card. Moreover, the authentication process is not exposed over the Internet and sufficient authentication security measures are taken by the government, which are supervised by the Technology and Architecture Review Board and Security Review Committee.

The petitioners questioned the magnitude of protection that needs to be accorded for the collection, storage, and usage of biometric data. The SC answered that Section 2(D) which pertains to authentication records would not include any metadata as mentioned in regulation 26(C) of the Aadhaar Authentication Regulation 2016. Therefore, this permission in the present form is 'Struck Down' retention of data beyond the period of 6 months is impermissible. Therefore, regulation 27 of the Aadhaar Authentication Regulation 2016 which provides archiving data for 5 years was forbidden. Further, the petitioners stated the Right to Privacy is not protected as per Art. 21 of the INDIAN CONST. The Supreme Court declared that all the matters of an individual do not qualify as being an inherent part of the Right to Privacy, only those matters over which there would be a reasonable expectation of

[12] Application Programming Interface is a software intermediary that allows two applications to talk to each other.
[13] The careful watching of somebody who may have done something wrong.

privacy are protected by Art. 21. The honourable Court declared a 'Triple Test' which a State has to pass before accessing any individual's personal information.

The Triple Test includes the following three rules,

1. Existence of a Law: This was backed by the State as the government had the Aadhaar Act.
2. A Legitimate State Interest: In the Aadhaar Act, the government wants to record your demographic information and biometrics to ensure the social benefit schemes reach the deserving candidates.
3. Test of Proportionality: The government provides the Right to Food, Right to Shelter, Right to Employment, etc. by taking an individual's Right to Privacy. In this way, there is a balance between the benefits of Aadhaar and the potential threat it carries to the fundamental Right to Privacy.

The petitioners inquired why Aadhaar is kept mandatory for getting government benefits? To get benefits and schemes of the government are basic rights of the citizen and Aadhaar should not be kept mandatory for the same. The government in its own words answered the question as The failure to establish the identity of an individual has proved to be a major hindrance for the successful implementation of government beneficiary schemes and programs. It was becoming difficult to ensure that the subsidiaries, benefits, and services reach the unintended beneficiary in the absence of adequate identity proofs.

Dashing ahead, the petitioners also asked why Aadhaar is kept mandatory for PAN services and filing Income Tax Return which hit the Right to practice any Profession or Trade or Business as per Art. 19 (1)G[14]. Moreover, Aadhaar was kept mandatory for availing PAN services by an individual and is not kept mandatory for non-individuals like businesses or firms, which hit the Right to Equality of the country. The SC answered that the Aadhaar Act and linking it with PAN services is not in violation of the fundamental right to equality or the fundamental right to practice one's profession or trade. Aadhaar is perceived as the best method of eliminating duplicate PANs and the decision of linking the Aadhaar Card with PAN is reasonable and rational. Moving on to making Aadhaar Card mandatory for filing ITR, the SC said it stood the Triple Test and did not violate the right to privacy. Continuing, the last question asked by the petitioners against the Union of India was why the Aadhaar Act

[14] The right to practise any profession, or to carry on any occupation, trade or business

passed as a Money Bill[15] as it does not qualify as a money bill because it contains permissions unrelated to government taxation and expenditure. The Supreme Court over this directed the government that 'benefits' and 'schemes' as mentioned in Section 7 of the Aadhaar Act should be those which have the colour of the same kind of subsidies, benefits, and welfare schemes of the government as earlier ones which are targeted for a particular deprived class. All these benefits and schemes have to be drawn from the Consolidated Fund of India.

However, the honourable Supreme Court declared Section 57 of the Aadhaar Act as 'UNCONSTITUTIONAL'. Section 57 of the Act states that any governmental agency or private firm can use Aadhaar Card for establishing the identity of a person for any purpose and nothing shall prevent this. The court said that the 'purpose' for which the Aadhaar number is to be used, should be defined properly. The part of this Section enabling body corporate and individuals to seek authentication is unconstitutional as establishing an identity for a purpose according to any contract is impermissible as it is not backed by law and therefore does not meet the test of proportionality suggested by the court. Also, the court said that authentication services based on a contract between individual and body corporate or person would not only enable commercial exploitation of individual biometric and demographic information by private entities but also impinge on the right to privacy of the individual.

Data protection in India

India is the second-largest online market globally with about 700 million internet users which are expected to rise to 974 million users by 2025. With such a huge number of users, it is difficult for any government or organization to handle such a huge amount of data[16]. Data is of two types, i.e, public and private data. Public data is the information of the user or customer of a company that is publicly visible over the internet or other sources like newspaper, television, etc. Private data is the collection of information of a user which is private to him or her and the information is used to identify the user. The private data can be of many types such as personal data used to identify an individual, sensitive data including financial data, biometrics data, interests, and beliefs about caste and religion, etc. The private

[15] Money bills are concerned with financial matters like taxation, public expenditure, etc

[16] Data is the systematic collection and storage of information over some time on a particular branch of knowledge or in respect of a particular field of activity.

data, hence, needs to be protected and leaking of that data is the failure of the government, private organization, or agency, whosoever is the owner of the database. It is an abuse of data, its users, and the owner of the database when private data or privileged data, or confidential data is plagiarized, stolen, pilferage, copied or misused in authorized manners. So, the concept of data protection is a must in any system in the modern era. Data protection is the set of laws and policies of the government or any firm that aims to provide security to one's data and privacy caused by collecting, storing, and disseminating personal data. The INDIAN CONST. does not specifically provide any Data Protection Law but it provides the provisions of 'Freedom of Speech and Expression' and 'Right to Life and Personal Liberty' in Art. 19 and Art. 21 respectively. Also, there are some rules and regulations on how the data is collected, stored, and secured in a database.

Article 19

Art. 19 of the INDIAN CONST. is a law that stands for the protection of certain rights of citizens of the country regarding freedom of speech and expression. It states that all citizens shall have the right to freedom of speech and expression, to assembly peacefully and without arms, to form associations or unions, to move freely throughout the territory of India, to reside and settle in any part within the territory of India, to practice any profession or to carry on any occupation or trade.

Article 21

Art. 21 of the INDIAN CONST. states that no person, either an Indian citizen or not should be deprived of his life or personal liberty except according to a procedure established by law. It embodies a constitutional value of supreme importance in a democratic society but the State can follow the procedures by the law to deprive the person of his right to life and personal liberty. Art. 21 secures two fundamental rights; the Right to Life and the Right to Liberty. The Supreme Court states that the right to life is not merely confined to the right to breathe and survival but also includes the right to live with human dignity and all those aspects of life which make it meaningful, complete, and worth living. It includes the right to privacy, right to go abroad, right to shelter, right against solitary confinement, right to social justice and economic empowerment, right against handcuffing, right against custodial death, right against delayed execution, right against public hanging, right to protect cultural heritage, right to pollution-free water and air, right to education to every child till his or her

full development, right to medical health and aid, right to reputation, etc. Art. 21 protects an individual from arbitrary executive actions as well as arbitrary legislative actions, giving the right to an individual to question the validity of laws.

Indian Contract Act 1872

The Indian Contract Act which came into force on Sept. 1, 1872, applies to every person who willingly or unwillingly does casual or business transactions with another person. The act was the first one in India that provides spaces to the parties to a contract to have appropriate clauses in the contract to protect confidential data.

Indian Information Technology Act 2000

The Parliament of the country enacted its first cybersecurity law on 9th June 2000 in the budget session named the Indian Information Technology Act 2000. Inspired by the model of the United Nations Commission on International Trade Law, it is the principal law in the country which deals with cybercrimes and electronic commerce. The fundamental objective of the Act is to provide legal recognition for transactions carried out through electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information", to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. The Act aims to provide a legal framework to electronic modes of communication and business. As per different sections of the Act, rights and penalties to corresponding offences are decided. Hence, the Indian Information Act gives the right to each person that he or she must be able to exercise a substantial degree of control over that data and its use. Data protection is a legal safeguard to prevent misuse of information about a person on a medium including computers.

Indian Information Technology (Amendment) Act 2008

The Indian Information Act 2000 was amended and passed on December 22, 2008. Section 66A and Section 69 were updated in the IT Amendment Act of 2008. Section 66A of the IT Act 2000 states that a person is found guilty and punishable if he or she sends an 'offensive message' to the other. It was a punishable act to post something violent and offensive on

social media as per Section 66A but this was in disagreement with Article 19 clause (i) subclause a, which gives every individual the fundamental right to speech and expression. So, in the IT Amendment Act of 2008, Section 66A was removed. Section 69 of the IT Amendment Act 2008 gives the power to the government to block the internet access of the individual who is found to harm the integrity and sovereignty of the country, defence of the country, or friendly relations with other countries. This was again in disagreement with the fundamental rights of the individual and hence it was amended introducing Section 69A and Section 69B.

Offences and Punishments as per Cyber Laws (IT Act and IT Amendment Act)

Some of the legal penalties for offences over the internet are as follows,

1. Under Section 65 of the IT Act, there is imprisonment up to three years or/and a fine up to INR 2 lacs in the offence of tampering with computer source documents.
2. In the offence of hacking with the computer system, Section 66 of the Act finds the culprit guilty and up to three-year imprisonment or/and a fine up to INR 5 lacs is a penalty to the criminal.
3. Under Section 66B, there is imprisonment of up to three years or/and a fine of INR 1 lac in the offence of receiving a stolen computer or communication device. Under Section 66C, up to three-year imprisonment or/and a fine of INR 1 lac in the offence of using another person's password. Under Section 66D, if a person is found guilty of cheating using computer resources, he or she will be imprisoned for three years or/and a fine of INR 1 lac. Under Section 66E, publishing a private image of any person is found a criminal offence, and imprisonment of up to 3 years or/and fine of up to INR 2 lacs is imposed over the criminal.
4. As per Section 66F, in the offence of cyberterrorism, the criminal is penalized with lifetime imprisonment.
5. Under Section 67, publishing information that is obscene in electronic form is a criminal act and as a penalty, imprisonment of up to five years or/and a fine up to INR 10 lacs.
6. If a person publishes images containing sexual acts over the internet, he or she will be found guilty under Section 67A and will be penalized with imprisonment of up to seven years or/and a fine up to INR 10 lacs.
7. In the offence of publishing child porn or predating children online, imprisonment of up to five years or/and a fine up to INR 10 lacs is penalized on the first conviction. Imprisonment

of up to seven years or/and a fine up to INR 10 lacs is penalized on second conviction under Section 67B.

8. Failure to maintain the record in the form of databases is also a criminal offence under Section 67C with a penalty of three-year imprisonment and a fine.

9. Breach of confidentiality and privacy is a criminal offence under Section 72. It states that 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.

10. Under Section 73, publishing an electronic signature certificate that is false in certain particulars is also a criminal offence with imprisonment of up to 2 years or/and fine up to INR 1 lac.

11. Under Section 74, publishing for fraudulent purposes is a criminal offence with imprisonment of up to 2 years or/and a fine up to 1 lac.

The Personal Data Protection Bill 2019

In July 2017, a committee of experts chaired by Justice B.N. Srikrishna was elected by the Supreme Court to examine various issues related to data breaches and data protection in the country. By the end of one year, the report on these issues along with a draft Personal Data Protection Bill 2018 was submitted to the Ministry of Electronics and Information Technology, Government of India. The draft was aimed to make provisions on how personal data related to an individual is regulated and monitoring of law and judiciary over the processing, collection, and storage of such data. The draft was further referred to a Joint Parliamentary Committee for some amendments. The Bill seeks to protect the personal data of individuals, creates a framework for processing such personal data, and establishes a Data Protection Authority in the country for the same purpose. The Bill talks about 12 types of personal data, data principles[17], data fiduciaries[18], data portability, and localizing of data[19]. If the bill got passed in Parliament, no foreign or home company will be allowed to access the

[17] The owner of the internet data
[18] An entity or individual who decides the means and purpose of processing personal data.
[19] Storing data within the country and not outside the territory of the State.

personal data of Indian users inside or outside the country for any wrong purposes. The Bill will provide much accessibility to the user, also known as data principal, on how he or she wants others to access their data.

Banning of 224 Apps

In 2020, the Ministry of Electronics and Information Technology, Government of India under Section 69A of the Information Technology Act with relevant provisions of Information Technology (Procedures and Safeguards for Blocking of Access of Information by Public) Rules 2019 and because of the emergent nature of threats to the integrity, sovereignty, defence, security, and harmony of the country, blocked 224 mobile apps within two months, earlier banning 59 apps than 118 more apps, which are supposed to collect personal data of the user.

Conclusion

The word 'privacy' has different meanings for every different individual. Also, the meaning of the word may vary from situation to situation. The technological growth in the field of communication has changed the perspective of privacy for every individual and emphasized the concept of 'data protection' in the ever-growing society. With the reach of Internet technology increasing, people are more prone to cybercrimes. And this is the responsibility of the government to take strict actions against these crimes, as well as the responsibility of the citizens to ask for justice. For this many laws and rules are made by the government but the individual also has to be a bit more conscious about his or her data on the Internet and how to privatize it.

References

1. Privacy and Data Protection laws in India: A right-based analysis by M. Jayanta Ghosh and Dr. Uday Shankar https://www.researchgate.net/publication/323958405_'Privacy_and_Data_Protection_Laws_in_India_A_Right-Based_Analysis
2. Global survey on Internet Privacy and Freedom of expression, UNESCO series on Internet Freedom. http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Rabat/images/CI/PDF/218273es.pdf

3. Privacy by Wikipedia https://en.wikipedia.org/wiki/Privacy
4. Internet Privacy by Wikipedia https://en.wikipedia.org/wiki/Internet_privacy#:~:text=Internet%20privacy%20involves%20the%20right,a%20subset%20of%20data%20privacy.&text=PII%20refers%20to%20any%20information,used%20to%20identify%20an%20individual
5. Data Protection Laws in India: Everything you must know by Vijay Pal Dalmia
6. Right to Privacy in Indian Perspective by Dr. P. K. Rana
7. Right to Privacy by Aaditya Verma RIGHT TO PRIVACY
8. Internet Privacy Laws Revealed - How Your Personal Information is Protected Online
9. Privacy Glossary
10. Understanding WhatsApp and its end-to-end encryption for privacy, securitys
11. The Personal Data Protection Bill, 2019: All you need to know
12. Data Protection 2020 | Laws and Regulations | India
13. ITR filing: 7 changes that affect income tax return filing this year
14. Section 57 of Aadhaar Act struck down: What it means
15. Unique Identification Authority Of India https://uidai.gov.in/
16. https://www.youtube.com/watch?v=hmkeVbIdw_M
17. Section 5(2) in The Indian Telegraph Act, 1885
18. Indian Telegraph Act 1885
19. What is Data Mining? Definition of Data Mining, Data Mining Meaning
20. What Is Data Profiling? Process, Best Practices and Tools
21. What is biometrics? 10 physical and behavioral identifiers
22. Duo Labs: The Good and Bad of Biometrics
23. What is spyware? And how to remove it.
24. Information Technology Act, 2000.
25. Information Technology (Amendment) Act,2008