International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 3, May-June, 2023 pp: 129-136 www.ijemh.com

Right To Privacy: The Impact Of Cyber Security On An Individual

Pallavi Sharma

Date of Submission: 20-05-2023 Date of Acceptance: 02-06-2023

The term 'Privacy' in its literal sense would mean the sense of being left alone without any disturbance or interference. In this state the person likes not to be watched upon i.e. free from the attention of the public. The major examples of privacy can be termed as under: -

(1) The right to be let alone,
(2) Limited access to the self,
(3) Secrecy,
(4) Control of personal information,
(5) Personhood and
(6) Intimacy

It is a right of a person to keep his/her personal matters and relationships secret. The ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

The right to privacy is a fundamental human right recognized by many countries around the world. It is the right to be free from unwarranted intrusion into one's personal life and affairs, and to have control over one's personal information.

The right to privacy is often protected by laws and constitutions. For example, in the United States, the Fourth Amendment to the Constitution protects against unreasonable searches and seizures, which includes the right to privacy in one's home. The European Convention on Human Rights also recognizes the right to privacy as a fundamental human right.

The right to privacy can apply to many different areas of life, including personal information, bodily integrity, and communications. Some specific examples of areas where the right to privacy is protected include:

- Personal data: individuals have the right to control their own personal information, including how it is collected, used, and shared.
- Communications: individuals have the right to privacy in their electronic communications, such as email and messaging apps.
- Medical information: individuals have the right to privacy in their medical information, including their medical history and treatment.
- Home and family life: individuals have the right to privacy in their home and family life, including the right to private and family life.

In general, the right to privacy is a crucial human freedom that gives people control over their personal data and affairs and helps shield them from undue interference.

Right to Privacy in legal terms means "no one shall be subject to arbitrary interference with his/ her privacy, home, family, nor be subjected to attack on his/her reputation and honor." Right to Privacy has also been recognized as a human right under Article 12 of the Universal Declaration of Human Rights Act, 1948.

The restrain imposed upon governmental and private actions by various legal traditions which threatens the privacy of an individual is what Right to Privacy stand for. Right to Privacy is recognized under more than 150 national Constitutions.

Constitution is the heart and soul of every discussion in law, as there cannot be laying down of any right without keeping a check on its constitutional value. The main reason behind keeping a check on the constitutional applicability is because Fundamental Rights in our constitution is subject to some limitations. So the most significant question regarding the application of the fundamental right is their applicability is the extent and its scope and how and when they can be limited by the state actions.

As said by Justice Nariman, when we talk about the restrictions of this right, the study of various rights to which this right relates must be looked into. This simply means that Right to Privacy is not merely a right under Article 21 but is also associated with other rights enshrined under Part III of the Constitution. Concluding the same we can say that the scope and extent of the right to privacy can vary depending on the country and legal framework in question. However, in general, the right to privacy is

recognized as a fundamental human right that protects individuals from unwanted or unwarranted intrusions into their personal lives, including their thoughts, beliefs, and physical spaces.

DIFFERENCE BETWEEN RIGHT TO PRIVACY AND INVASION OF PRIVACY

The right to privacy and invasion of privacy are two distinct concepts.

The right to privacy refers to an individual's fundamental right to keep certain aspects of their personal life private and free from interference. It is a legal concept that protects individuals from unwarranted or unwanted intrusions into their personal lives. The right to privacy may include, but is not limited to, the privacy of personal information, communication, physical spaces, personal identity, and thoughts and beliefs.

Invasion of privacy, on the other hand, refers to the violation of an individual's right to privacy. It occurs when someone intrudes upon another person's private affairs, discloses private information without their consent, or uses their likeness or personal information in a way that is offensive or harmful. In other words, invasion of privacy is a violation of the right to privacy.

- There are four main types of invasions of privacy:
  - Intrusion upon seclusion: This occurs when someone intentionally intrudes upon another person's private space or affairs, such as by spying or eavesdropping.
  - Public disclosure of private facts: This occurs when someone publicly discloses private and embarrassing information about another person, such as medical records or personal relationships.
  - False light: This occurs when someone publishes false or misleading information about another person that portrays them in a negative light.
  - Appropriation of name or likeness: This occurs when someone uses another person's name or likeness without their consent for commercial or non-commercial purposes.

WHY RIGHT TO PRIVACY?

Privacy is important for many reasons and we have to do away with the consequences of not having privacy. Privacy has become an important aspect of society due to several factors, as with the rise of digital technologies and the internet, personal information has become more accessible and shareable than ever before. This has led to concerns about data privacy and security, as well as the use of surveillance technologies by both private and public entities. Privacy is considered a fundamental right in many legal systems around the world, including in India. This means that individuals have the right to keep certain aspects of their personal lives private and free from interference. Also privacy is closely tied to personal identity, as it allows individuals to develop and express their personal identities without fear of judgement or interference. Privacy has become a social norm in many cultures, with people valuing their privacy and expecting others to respect it. Personal information is often collected and used by companies for marketing and advertising purposes. This has led to concerns about the economic value of personal data and the need for individuals to protect their privacy. All things considered, technical development, legal acknowledgment of individual rights, identity concerns, societal conventions, and economic value have all contributed to privacy becoming a significant part of society. It is believed that maintaining one's privacy is necessary to uphold one's dignity, independence, and autonomy.

The concept of the right to privacy can be traced back to ancient civilizations, such as the Greeks and Romans, who recognized the importance of personal privacy in their societies. However, the modern understanding of the right to privacy began to develop in the late 19th and early 20th centuries. One of the earliest discussions of the right to privacy in the modern sense was in a law review article written by Samuel Warren and Louis Brandeis in 1890, titled "The Right to Privacy." In this article, Warren and Brandeis argued that individuals have a right to be left alone and that this right should be legally protected. Their article was a response to the intrusive and sensationalist coverage of private individuals in the press, and it sparked a national conversation about privacy rights. The ideas put forth in the article eventually helped shape the development of privacy laws in the United States and other countries around the world. The concept of the right to privacy was not explicitly recognized as a fundamental right in India until the landmark Supreme Court judgment in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India in 2017.

However, the right to privacy was discussed in Indian legal and political circles long before this judgment. In the 1950s, the issue of privacy arose in the context of the government's attempts to establish a national identification system. The debate over the proposed system raised concerns about the potential violation of individuals' privacy rights.

In the 1960s and 1970s, the Indian judiciary began to recognize the right to privacy as

an implicit part of the fundamental right to life and personal liberty guaranteed by the Indian Constitution. In the 1975 case of Gobind v. State of Madhya Pradesh, the Supreme Court held that the right to privacy is a fundamental right under the Indian Constitution.

However, it was not until the Puttaswamy judgment in 2017 that the right to privacy was explicitly recognized as a fundamental right under the Indian Constitution, on par with other fundamental rights such as freedom of speech and religion.

While the right to privacy can have collective implications, such as in cases where privacy violations affect a group of people or a community, it is ultimately an individual right that is protected by law. For example, the right to privacy in the context of medical information can have collective implications for public health, but it is ultimately the individual's right to control their own personal health information.

The Indian Constitution does not specifically address the right to privacy. However, under Article 21 of the Constitution, which protects the right to life and personal freedom, it has been considered as a fundamental freedom. In its landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court of India declared the right to privacy to be a basic right protected by Article 21 of the Indian Constitution in 2017. The Supreme Court ruled that maintaining one's right to privacy is crucial for upholding one's dignity as well as their right to life and personal freedom. The ruling has given India's right to privacy a solid base on which to stand.

The right to privacy under the Indian Constitution is a fundamental right that is derived from Article 21, which guarantees the right to life and personal liberty. The right to privacy refers to the right of an individual to be free from unwarranted interference in their private life, including their personal affairs, thoughts, beliefs, and decisions. It also includes the right to control the collection, storage, and dissemination of personal information. The Supreme Court of India has recognized that the right to privacy is an intrinsic part of the fundamental rights guaranteed by the Constitution, and it has been interpreted broadly to include a wide range of personal liberties. The right to privacy has been recognized as a fundamental right not only by the Indian courts but also by international bodies such as the United Nations. The protection of the right to privacy is essential to safeguard the dignity and autonomy of individuals and to ensure that they are free from arbitrary interference by the state or other entities.

HISTORICAL BACKGROUND

The right to privacy in India has evolved over time through a combination of judicial interpretation, legislative action, and social change. Here is a brief overview of how the right to privacy has evolved under the Indian Constitution:

Early years: In the early years after independence, the Indian courts did not explicitly recognize the right to privacy as a fundamental right. However, there were some cases in which the courts recognized the importance of privacy in certain contexts, such as the right to be free from unreasonable searches and seizures.

1975-77 Emergency period: During the period of Emergency from 1975 to 1977, the government imposed strict controls on the media, limited personal freedoms, and conducted mass surveillance of citizens. This led to a growing awareness of the need to protect individual privacy and to resist government overreach.

1980s and 1990s: In the 1980s and 1990s, the Indian courts began to expand the scope of the right to privacy under Article 21, recognizing the importance of privacy in areas such as reproductive rights, medical treatment, and personal autonomy.

2017 landmark judgment: In 2017, the Supreme Court of India delivered a landmark judgment in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, recognizing the right to privacy as a fundamental right under the Indian Constitution. The Court held that the right to privacy is an essential part of the right to life and personal liberty under Article 21, and that it is necessary to protect the dignity and autonomy of individuals.

EVOLUTION OF RIGHT TO PRIVACY IN CYBER WORLD

The evolution of the right to privacy in India reflects a growing recognition of the importance of individual autonomy and dignity in a modern democratic society.

The Personal Data Protection Bill (PDPB) was introduced in the Lok Sabha, the lower house of the Indian Parliament, in December 2019, in response to growing concerns about the use and protection of personal data in India. The following are some of the factors that led to the development of the PDPB.

Increased use of technology in India has witnessed a rapid increase in the use of technology in daily life, with the proliferation of smartphones, social media, and e-commerce platforms. This has

led to the collection and processing of vast amounts of personal data, raising concerns about privacy and security. Lack of a comprehensive data protection framework in India did not have a comprehensive data protection framework before the PDPB was introduced. The existing laws, such as the Information Technology Act, 2000, were inadequate in addressing the complex issues related to data protection.

International developments of several countries around the world, including the European Union, have enacted comprehensive data protection laws, which have set a benchmark for data protection standards. The need for India to have a similar framework was felt to ensure that it remains competitive in the global digital economy.

Recommendations of the Justice Srikrishna Committee in 2017, the Indian government constituted a committee headed by Justice B.N. Srikrishna to study the issues related to data protection and provide recommendations. The committee submitted its report in July 2018, which formed the basis for the PDPB. The PDPB is based on the recommendations of the Justice B.N. Srikrishna Committee, which submitted its report on data protection in India in July 2018. The bill aims to establish a comprehensive data protection framework that is in line with global best practices while taking into account India's unique socio-economic conditions.

The PDPB proposes to establish a Data Protection Authority (DPA) to oversee the implementation and enforcement of the law. The bill also lays down rules for the processing of personal data by data fiduciaries, including the need for explicit consent, purpose limitation, data minimization, and data localization.

The bill includes provisions for the protection of sensitive personal data, including health and financial information, and imposes strict penalties for non-compliance, including fines and imprisonment. It also includes provisions for the protection of children's data and the right to be forgotten.

The introduction of the PDPB has been seen as a significant step towards protecting individuals' privacy in India, which has emerged as a major concern in recent years due to the rapid growth of the digital economy and increasing use of technology in daily life. The bill is expected to have far-reaching implications for businesses, government agencies, and individuals and is being closely watched by stakeholders in India and around the world.

INTRODUCTION OF IT RULES 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, commonly known as the IT Rules, 2021, are a set of regulations introduced by the Indian government in February 2021 under the Information Technology Act, 2000. The IT Rules, 2021 aim to regulate the digital media industry and social media platforms in India.

The rules mandate that all social media intermediaries, including messaging apps such as WhatsApp and Signal, appoint a resident grievance officer who must acknowledge complaints within 24 hours and resolve them within 15 days. Additionally, social media platforms must appoint two other officers - a nodal contact person and a chief compliance officer - who will be responsible for ensuring compliance with the rules.

The IT Rules, 2021 also require social media platforms to develop and implement a three-tier grievance redressal mechanism, which includes self-regulation by the platform, a grievance redressal officer appointed by the platform, and an oversight mechanism by the government.

The rules also require digital news media platforms to adhere to a code of ethics, which includes verifying the accuracy of the content, preventing the publication of misleading information, and providing a mechanism for complaints and grievances.

Critics of the IT Rules, 2021 argue that they could lead to censorship of online content, curtail freedom of expression, and increase government surveillance. However, the government has stated that the rules are necessary to combat fake news, hate speech, and other harmful online content. As of my knowledge cut off in September 2021, there have been a few amendments made to the IT Rules, 2021 in India. Some of these amendments include:

1. Compliance reports: Social media intermediaries and digital news media platforms are required to submit compliance reports to the Ministry of Electronics and Information Technology (MeitY) every month, detailing the number of complaints received and action taken.
2. Grievance officer: The rules now mandate that all social media intermediaries appoint a compliance officer, in addition to the existing requirement of a grievance officer and nodal contact person.
3. Content takedown: The IT Rules, 2021 require social media platforms to remove or disable access to unlawful content within 24 hours of receiving a complaint. The amended rules now

clarify that this timeframe does not apply to content that is blocked by a court order or an intermediary order.

4. Significant social media intermediaries: The amended rules define "significant social media intermediaries" as those with over 50 lakh registered users in India. Such intermediaries are subject to additional obligations, such as appointing a chief compliance officer, a nodal contact person, and a resident grievance officer.

5. Self-regulatory bodies: The amended rules allow for the formation of self-regulatory bodies by publishers of online curated content, subject to the approval of the government.

Critics of the IT Rules, 2021 continue to argue that the amendments do not adequately address concerns around censorship and government surveillance. However, the Indian government maintains that the rules are necessary to combat harmful online content and protect the interests of Indian citizens. Cybersecurity refers to the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, damage, and disruption. It involves a range of measures and technologies that are used to secure electronic devices, data, and networks from cyber threats. Cyber threats can come in various forms, including malware, phishing attacks, social engineering, ransomware, and denial-of-service attacks. These threats can cause significant damage to individuals and organizations, including financial losses, reputational damage, and legal liabilities.

To prevent such threats, cyber security measures are designed to protect electronic devices, networks, and data from unauthorized access, use, or modification. These measures may include firewalls, intrusion detection systems, encryption, access controls, and regular software updates. Cyber security is a crucial aspect of modern life, as we rely more and more on electronic devices and networks for communication, commerce, and information sharing. It is important for individuals and organizations to take appropriate measures to protect themselves from cyber threats and stay up to date with the latest cybersecurity best practices.

Cyber security and the right to privacy are closely related. The right to privacy is a fundamental human right that is recognized in various international human rights treaties and national constitutions. It protects individuals from unwarranted intrusion into their personal lives, including their personal data and communications.

Cyber security is concerned with protecting computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. With the increasing use of technology in our lives, the protection of our personal data has become an essential aspect of cyber security. Personal data can include sensitive information such as our names, addresses, financial information, and health records.

To address the increasing threat of data breaches and cyber attacks, there is a need for a new cyber security policy. Such a policy would outline the measures that individuals and organizations must take to protect their data and systems from cyber attacks. It would also provide guidelines for reporting and responding to cyber incidents, and establish penalties for non-compliance.

1. Risk Assessment: A comprehensive risk assessment of an organization's data and systems is essential to identify vulnerabilities and potential threats. The policy should require organizations to conduct regular risk assessments and implement appropriate controls to mitigate risks.

2. Data Protection: The policy should require organizations to implement adequate measures to protect sensitive data, such as encryption, access controls, and regular backups. It should also mandate data retention policies and data breach notification requirements.

3. Cyber Incident Response: Organizations should be required to have a cyber incident response plan in place that outlines the steps to be taken in the event of a data breach or cyber-attack. The policy should also require organizations to report cyber incidents to relevant authorities and affected individuals in a timely manner.

4. Compliance: The policy should establish clear guidelines and penalties for non-compliance, and require regular audits to ensure that organizations are adhering to the policy.

1. Education and Training: Organizations should be required to provide education and training to employees on cyber security best practices, such as password hygiene, phishing awareness, and safe browsing habits.

In conclusion, a new cyber security policy is essential to address the increasing threat of data breaches and cyber-attacks. The policy should focus on risk assessment, data protection, cyber incident response, compliance, and education and training to ensure that individuals and organizations are adequately protected from cyber threats.

Cybercrimes are criminal activities that are committed using the internet or other forms of digital communication technology. These crimes can take many forms, including:

1. Hacking: Unauthorized access to computer systems, networks, or devices with the intent of stealing or altering data, or causing damage.
2. Identity theft: Stealing personal information such as social security numbers, credit card numbers, and bank account details to commit fraud.
3. Phishing: Attempting to trick individuals into providing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity.
4. Malware: The installation of malicious software, such as viruses, worms, and Trojan horses, with the intent of causing harm to computer systems or stealing data.
5. Cyberstalking: Using the internet or other digital communication technology to harass, intimidate, or threaten someone.
6. Cyberbullying: Using the internet or other digital communication technology to bully or harass someone.
7. Cyberterrorism: The use of the internet or other digital communication technology to threaten or commit acts of terrorism.
8. Intellectual property theft: The unauthorized use or theft of copyrighted material, trademarks, trade secrets, or patents.

Cybercrime is a serious issue that can cause significant harm to individuals, businesses, and even governments. It is important to take measures to prevent and combat cybercrime.

The Indian Constitution has provisions to protect against cybercrimes, although the term "cybercrime" is not explicitly mentioned in the Constitution.

The Information Technology Act, 2000 (IT Act) is the primary legislation that deals with cybercrime in India. The act provides for various offenses and penalties related to computer-related crimes. The IT Act was amended in 2008 to expand its scope and include more cybercrimes.

Additionally, the Indian Penal Code (IPC) has provisions that can be used to prosecute cybercrimes. For example, offenses like identity theft, hacking, and unauthorized access to computer systems can be prosecuted under relevant sections of the IPC.

The Constitution of India also guarantees fundamental rights, including the right to privacy, which is relevant in cases related to cybercrime. The right to privacy has been recognized as a fundamental right by the Supreme Court of India in several landmark judgments, including the Puttaswamy judgment of 2017.

Overall, the Indian Constitution provides a framework for protecting against cybercrime through legislation and fundamental rights, although the effectiveness of these protections in practice may vary.

Cybersecurity and the right to privacy have a commonality under the Indian Constitution in that they are both recognized as fundamental rights.

The right to privacy is protected under Article 21 of the Indian Constitution, which states that no person shall be deprived of their life or personal liberty except according to a procedure established by law. The Supreme Court of India has held that the right to privacy is an integral part of the right to life and personal liberty under Article 21.

Similarly, cyber security is essential to protecting an individual's personal information and privacy. Cyber security measures aim to prevent unauthorized access to personal data, which can be used for identity theft, financial fraud, and other cybercrimes.

Thus, the right to privacy and cybers ecurity have a commonality in that they both aim to protect an individual's personal information and ensure that it is not misused. The Indian Constitution recognizes the importance of both these fundamental rights and provides a framework for their protection through legislation and judicial interpretation.

Pegasus is a type of spyware that can infect mobile devices such as smartphones, allowing an attacker to monitor and steal sensitive data from the device. Pegasus is a product of the Israeli cybersecurity company NSO Group, and it has been implicated in several high-profile cases of surveillance and espionage.

Pegasus works by exploiting vulnerabilities in popular messaging apps such as WhatsApp and iMessage to gain access to a target's device. Once installed, the spyware can track the device's location, record phone calls, capture screenshots, and even turn on the device's microphone and camera without the user's knowledge.

The use of Pegasus has been controversial because it has been alleged to have been used by governments and intelligence agencies to target journalists, human rights activists, and political opponents. The use of Pegasus for such purposes raises serious concerns about privacy, free speech, and government overreach.

NSO Group has claimed that it only sells Pegasus to government agencies for the purpose of combating terrorism and other crimes, and that it has strict human rights policies in place to ensure that its products are not misused. However, the use of Pegasus remains a contentious issue, and its

potential for abuse has led to calls for tighter regulation of the surveillance technology industry.

Pegasus is a significant threat to the right to privacy of individuals because it can be used to secretly spy on them without their knowledge or consent. The spyware is designed to infect mobile phones, collect data from them, and transmit that data to a remote server controlled by the attacker.

Pegasus can collect a wide range of data from a target's phone, including calls, messages, emails, photos, and location data. This data can be used to monitor the target's activities, track their movements, and even potentially blackmail or manipulate them.

The use of Pegasus to spy on individuals without their knowledge or consent is a clear violation of their right to privacy, which is protected under Article 21 of the Indian Constitution. The right to privacy includes the right to control the collection, use, and dissemination of personal information. The use of spyware like Pegasus undermines this fundamental right by allowing governments or other entities to collect and use personal information without the individual's knowledge or consent.

Moreover, the potential for misuse or abuse of such spyware is significant, as it could be used to target journalists, activists, or political opponents and curtail their rights to free speech and expression. The use of Pegasus highlights the need for robust legal and regulatory frameworks to govern the use of such technologies and to protect individuals' right to privacy.

While Pegasus is a powerful tool for collecting data from mobile phones, its use can also be a threat to cybersecurity and, consequently, the right to privacy.

Pegasus can be used to exploit vulnerabilities in mobile phone software, allowing it to gain access to the device's data and potentially compromise its security. Once installed on a device, Pegasus can give attackers access to sensitive information such as passwords, financial data, and personal communications.

This type of unauthorized access to personal data and information is a violation of an individual's right to privacy. The right to privacy includes the right to control the collection, use, and dissemination of personal information, and unauthorized access to this information can undermine this right.

Furthermore, the use of spyware like Pegasus to gain access to sensitive data can also pose a broader threat to cybersecurity. If attackers can gain access to sensitive information on one device, they may be able to use that information to compromise other systems or networks.

In summary, the use of spyware like Pegasus can be a threat to both the right to privacy and cybersecurity. Robust legal and regulatory frameworks are needed to govern the use of such technologies to protect individuals' privacy and prevent unauthorized access to sensitive data.

According to Article 21, the right to life and to personal liberty both depend on the right to privacy. In addition to a contract, a right to privacy may also result from a specific relationship, such as one that is business-related, marital, or even political. The right to privacy is not unalienable; it is subject to reasonable limitations for the reduction of criminal activity, the control of public order, the preservation of morality and health, and the defense of other people's freedoms and rights. When two derived rights dispute, the one that advances public morality and the common good wins out.

The pursuit of happiness includes the right to privacy, according to American Supreme Court judges. In order for us to act as we see fit while abiding by other people's rights, the pursuit of happiness necessitates certain liberties that we are legally given. The right to liberty is unbounded and unquantifiable. It is evident across the entire legal range.

The right to privacy is a fundamental right that has been recognized by courts and legal systems around the world. It is an essential component of individual autonomy, dignity, and personal freedom, and has been enshrined in various international treaties and national constitutions.

The right to privacy protects individuals from unwanted intrusion into their personal lives and activities, including their personal communications, medical and financial information, and relationships. It also protects individuals from surveillance and monitoring by the state or other entities, without a legitimate reason or a warrant.

In the digital age, the right to privacy has taken on new significance as individuals share more personal information online, and governments and private entities increasingly collect and use personal data. Cyber laws have emerged to address these issues, and to provide legal protections for individuals' privacy rights in the digital realm.

Cyber laws can be broadly categorized into two types: those that regulate the collection and use of personal data by private entities, and those that regulate the surveillance and monitoring activities of the state. These laws often require entities to obtain explicit consent from individuals before collecting and using their personal information, and provide

individuals with the right to access, correct, and delete their data.

However, the right to privacy in the digital realm is not absolute and may be subject to limitations for reasons of national security, public order, or the prevention of crime. Governments may also have the right to access personal data in certain circumstances, such as for law enforcement purposes or in the interests of national security.

One of the key challenges in protecting the right to privacy in the digital realm is the cross-border nature of the internet and the global nature of data flows. Cyber laws often vary across jurisdictions, and different countries may have different standards for protecting privacy. This can make it difficult to enforce privacy protections and ensure that personal data is used in a manner that respects individuals' rights.

However, the right to privacy is not an absolute right and may be subject to limitations in certain circumstances. For example, the state may restrict the right to privacy for reasons of national security, public order, or the prevention of crime. In addition, the right to privacy may need to be balanced against other competing rights and interests, such as freedom of speech or the public interest.

In recent years, the right to privacy has become increasingly important in the digital age, with the rise of social media, data collection, and surveillance technologies. Individuals are increasingly concerned about the collection and use of their personal information by governments and private companies, and there is a growing recognition of the need to protect privacy in the digital realm.

We frequently put being members of a society before being ourselves. Every person needs a private area for whatever activity they choose to engage in (if that activity is lawful, of course). As a result, the state grants each person the freedom to spend private time with anyone they choose away from prying eyes of the outside world. According to Clinton Rossiter, maintaining one's privacy is a unique form of independence that can be seen as an effort to achieve autonomy in at least some personal and spiritual matters. The most unique experience a person can have is this sense of independence. There, he is genuinely a free man. This is a right against the entire globe rather than the state.The person will benefit from this right since he does not wish to broadcast his ideas to the entire world. This right is growing more and more important in the modern world. We need security so that we can live our lives as we choose and not put the needs of others above our own. These days, everything about us is documented in the media, whether it's through social networking sites or surveillance cameras. After all, the only person we have an obligation to explain ourselves to is ourselves, not the rest of the world.

In conclusion, the right to privacy is a vital aspect of individual freedom and autonomy, and is essential for the protection of human dignity and personal identity. While it may be subject to limitations in certain circumstances, it should be protected and upheld as a fundamental right in a democratic society. The right to privacy is an essential freedom that holds true in both the real world and the digital one. Cyber laws have been developed to give legal protection for people's personal data and to handle the difficulties of preserving privacy in the digital age. However, the global nature of data flows and the cross-border nature of the internet make it difficult to enforce privacy regulations, and ongoing efforts are required to guarantee that people's private rights are respected and protected in the digital sphere.