"The Unusual Difficulties of Inherent Intelligence"

(MISS BHOOMI SHUKLA)

IPS ACADEMY COLLEGE OF LAW SANWER

ABSTRACT

Around the world, privacy has become a fundamental human right. In India, it has also been acknowledged as such by Article 21 of the Indian Constitution.
The right to privacy is intimately tied to data protection, which has become extremely challe nging in today's technologically advanced and globalized society.
Furthermore, the absence of legal protection for this right has made it feasible for the ruling majority to violate private rights through discriminatory legislation.
At first, this right was not acknowledged as a fundamental right in India, and no particular d ata protection legislation was passed to safeguard citizens' right to privacy.
Simultaneously, there were numerous claims of privacy rights violations in India occasionally committed by both the government and private commercial entities.

Allegations of this nature were also brought to the legal system, which rendered historic dec isions and recommendations.
Therefore, it is crucial to examine all of the legislative developments around the Right to Priv acy and Data Protection in order to comprehend the level of protection that the Indian legal system affords its citizens with regard to the right to privacy.
However, it has been discovered that the Indian legal system has adequately recognized the right to privacy, leading to important measures being taken to stop data theft and misuse of private information. However, a significant amount of progressive developments is still req uired to expand the scope of data protection in the modern era in order to secure the right t o privacy of Indian citizens.

Keywords:
Indian Penal Code, Information Technology, Indian Constitution, Data Privacy, Data Protecti on, Personal Data Protection Bill,

INTRODUCTION:

The Indian government recently envisioned a digital world with its "Digital India" effort, coin ciding with the global "Digital Revolution."
However, the question is whether this approach can be successful in a nation like India that has a dedicated data protection statute.
The significance of data protection now becomes apparent.
Every nation that aspires to full digitization and a digital economy must have its own stringe nt, open, and responsible data protection regulations.
I attempted to provide a thorough analysis of the idea of data protection, its significance in I ndia, the numerous laws discussing it, its impact on society, and the proposed bill on person al data in India through this research paper.

RESEARCH OBJECTIVES:

Individual rights, the intent behind data collection and processing, privacy choices.

How businesses handle personal data are all covered by data privacy.

Focuses on the legal methods for gathering, processing, sharing, archiving, and deleting data
.

RESEARCH QUESTIONS:

How Good have we strategized our data?

How good are we at building privacy and ethics in using the data?

Are there security solutions to manage your data privacy program?

Do we have mechanisms in place to destroy or delete data if requested to do so?

What will be the effects of Data Protection on Society?

CONCEPT OF DATA PROTECTION:

The appropriate treatment of data, including consent, notification, and regulatory requirem
ents, is the focus of data privacy, also known as information privacy, a subset of data securit
y. More precisely, the following are common practical data privacy concerns:
if and how other parties are given access to data.
How information is gathered or stored legally.

NEED OF DATA PROTECTION IN INDIA:

In this era of data economics, corporate entities and large corporations have begun to view data as an asset and see value in its distribution, gathering, and storage.
They began safeguarding their big data in order to realize this goal.

The right to privacy, which encompasses personal data, is a basic right in India. As such, the I
ndian government is required to create and enforce laws protecting personal data.

We need a particular law with severe penalties and a redressal system to fight the growing n
umber of cyberattacks, including identity theft, data theft, and more.

INDIAN LEGAL FRAMEWORK ON RIGHT TO PRIVACY:

As of right now, we are aware that India lacks clear laws that might address data protection and privacy in particular.
But even without such laws, there is still a legal structure that addresses privacy and data pr otection, albeit indirectly rather than directly.
In addition to statutory protection, the Indian Constitution also guarantees privacy.
Therefore, there are two ways to safeguard both personal information and privacy rights.

Constitutional protection

Statutory protection Constitutional protection

Privacy is neither specifically or explicitly guaranteed as a Fundamental Right by the Constitu tion. The Constitution makes no mention of it.
Nonetheless, it is inherent in the freedoms protected by Part III of the Constitution, includin g the right to life and personal liberty as stated in Articles 21 and 28. Even though a nine-judge panel in the Puttuswamy case29 acknowledged it as a fundamental right, the right can not be fully exercised. Article 19(2) allows for the imposition of rational limitation.
Since our birth, we have been granted the unalienable right to privacy.

As a result, the minority group of judges has maintained that the right to privacy is a fundam ental right guaranteed by Article 21 of the Constitution since the outset, when the idea of pr ivacy was a contentious issue.
Because Article 21 contains numerous rights that are necessary to grant constitutional legiti macy to newly emerging rights in response to the shifting needs of society, we can therefore claim that it is the central component of the Constitution. Legal safeguards
The Indian Contract Act of 1872, the IT Act of 2000, the Credit Information Companies Regul ation Act of 2015, and other laws that address data protection in the current environment a re briefly covered below.

IT Act, 2000: The first IT law in India, the IT Act, 2000 aims to address cybercrimes, e-governance, and e-commerce. In addition, it is the data protection legislation.
The Information Technology Act was created to prevent information violations caused by co mputer leaks.
It has several clauses, including Sections 65 and 66, that prohibit unauthorized use of techno logy, including computers, laptops, and data stored on them.

• Sec. 43 of the said IT Act contains punishment for any destruction of data kept in the computer. Under this Section, if any person uses computer data in an unauthorized manner or illegally then he will be liable for a penalty of 3 years imprisonment or 5 lakhs rupees as a fine or with both. • Section 65 protects those who knowingly or Besides, if any company violates the provision of the IT Act, then the managers of the company and directors are in person accountable for the offense.31 Later, the 2008 Act32 has been passed to handle the matters that the original Act failed to cover and to assist further development of IT and related security concerns.
Section 69(A) of the new Amendment Act grants the Indian government the authority to pro hibit electronic data stored on computer devices and to prevent, monitor, and decrypt comp uter systems and resources.

However, this caused a great deal of debate, and the Supreme Court later in 2015 ruled that Section 69(A), which gives the government the authority to order the blocking of websites, i s constitutionally acceptable because there are sufficient procedural safeguards in place.33 1860 Indian Penal Code The penal code does not specifically address data privacy violations. However, there are certain crimes from which an inference can be made that there exists a penalty for violation of privacy say eg, Under Article 408 of IPC liability arises out of dishonest misappropriation of movable property.34 Intellectual Property Law In India, the Copyright Act, 1957 deals with matters of copyrighted piracy (theft) and for such piracy impose compulsory punishment which is in proportion to the seriousness of the offense. Moreover, wherein an author produces books, records, or broadcast programs by collecting information from a different source by devoting time, money, labor, and skill amounting to work within the meaning of the Copyright Act are protected as being copyright of that person. Thus, the outsourcing parent entity may have recourse under the Copyright Act for any violation occurring to that database. 35 CICRA36 In India, any information relating to the credit of individuals is to be collected as per the privacy norms that are mentioned in the CICRA regulation.

DATA PROTECTION IS A RIGHT?

Since data privacy is a component of the right to privacy, which is a fundamental right in Indi a, data protection is a right.
Furthermore, without data protection, no data privacy is conceivable.
Thus, data protection is a right as well.

Indian Constitution:
The police monitoring of the accused and nocturnal house visits throughout the 1950s mark ed the beginning of the establishment of the Constitution's guarantee to privacy.
Even if search and seizure are part of a police officer's duties, the Supreme Court ruled in th e case of M.P. Sharma v. Satish Chandra1 that conducting one at midnight is against Article 1 9(1)(f) of the Constitution.
The Court further stated that the seizure associated with a police officer's search is only tem porary in nature and does not impact any right to property.
Therefore, it will serve as a legitimate limitation on the right to privacy.

Indian Penal Code, 1860:
During British control in India, the Indian Penal Code was established.
Lord Macaulay oversaw the creation of the initial draft in the 1860s.
The Indian Penal Code does not fully address the country's data protection requirements.
Data privacy violations are not the only issues covered by our Indian criminal code.
According to the Indian Penal Code, the associated crimes must determine who is legally res ponsible for such violations.

Information Technology Act (Amendment) 2008:

The Indian Parliament worked hard to include the idea of data privacy in the IT Act of 2000. To address the new issues brought about by the growth of the cyber world, this Act has und ergone numerous amendments. The 2008 Amendment Act is the most recent of these.

The terms "data protection" and "information technology," as defined by the Data Protectio n & Information Technology (Amendment) Act of 2008, have distinct meanings.

The protection of rights connected to cyberspace is specifically mentioned in the Act's objec tives.

This Act contains measures to stop unauthorized use of computers, computer networks, and the data they hold. Several other clauses pertaining to "data protection" are included.

Data protection is also included in the Act's recently added Sections 43A and 72A.

This legislation's primary flaw is that its current data security and secrecy measures are insuf ficient to address the recently discovered cybercrimes.

Right to Information Act, 2005:

In India, public authorities are in charge of putting citizens' right to secure information into p ractice in order to encourage accountability and openness.

The definition of "right to information"6 is covered in Section 2(j) of the RTI Act.

The question of whether the "data" that was retained by the public body is secure or not—particularly the digital data covered by clause (iv) of Section 2(j)—comes up here.

The protection of data under this Act is therefore a problem and is being handled as a matte r of an individual's right.

Evolution of PDB Bill:

The Personal Data Protection Bill 2019,

The submission of Bill50 in the Lok Sabha on December 11, 2019, by Mr. Ravi Shankar, Minis ter of Electronics and Information Technology, is another recent attempt to secure data.

Drafting a data protection regime to identify contemporary challenges and potential regulat ory protections was one of the Bill's primary goals.51

Furthermore, this is not the only bill that has been submitted; data protection bills were also introduced in Parliament in 2017 and 2018.

CONCLUSION AND SUGGESTIONS:

Due to a number of judicial rulings, the right to privacy has become a fundamental right in In dia.
However, if we look at the current situation, we will see that globalization has led to a signifi cant technological advancement.
As we can see, technology is becoming a part of our lives and has greatly benefited us, but it has also become a threat because as technology has advanced, numerous issues that directl y affect our privacy have emerged, such as cybercrimes, data theft, and misuse of data.
We are aware that in order to receive any kind of services, we currently have to give our per sonal information to a third party, whether it be the government or a private organization. H owever, doing so may make us more vulnerable to data theft or misuse, as India lacks suffici ent data protection laws, despite having some laws that address data protection indirectly r ather than directly.
The IT Act, criminal law, intellectual property law, and others are a few examples.
Such information may be considered a "breach of privacy" if it is unlawfully disclosed or use d by a third party.
A strict Data Protection Law is necessary to protect data privacy because the current laws ha ve many flaws. For example, internet service providers and data processors are not held acc ountable for any data processing violations if they can demonstrate that the data was proce ssed without their knowledge.

A few experts have proposed switching to smart cards, which would be optional, as an alter native to gathering biometric data.
Because biometrics may identify people even if they refuse to be identified, smart cards that require pins will require citizens' conscious cooperation during the identification process.
No one can use smart cards to identify a specific person after they are discarded.
Smart card adoption would eradicate or at least lessen the threat of terrorists and criminals, as foreign governments use the biometric database to identify Indians.

REFERENCES:

1.Romansky, R., I. Noninska. Challenges of the Digital Age for Privacy and Personal

Data Protection. Mathematical Biosciences & Engineering,ISSN 1551-0018, Vol. 17,

No. 5, August 2020, pp.5288-5303. DOI: 10.3934/mbe.2020286

2. Jason Asbury, Maria McClelland , Kris Torgerson, India Vincent & Jennifer Boling, Law and Business Technology: Cyber Security & Data Privacy Update, 20 Transactions: TENN. J. BUS. L. 1065, 1067-71 (2019).

3.Dhiraj R. Duraiswami, Privacy and Data Protection in India, J.L. & CYBER WARFARE 166, 169-72 (2017).

4.SC notice on privacy concerns to Google, WhatsApp,Amazon,HINDUSTANTIMES, UPIshttps://www.hindustantimes.com/india-news/sc-notice-on-privacy-concerns-to-googlewhatsapp-amazon-upis-101612192948826.html, (Last visited 12/02/2021).