PRIVACY AND DATA PROTECTION LAWS IN INDIA: A RIGHT BASED ANALYSIS

Adv Aakanksha Milind Alai, LLM, Modern Law College, Pune

ABSTRACT:

The advancement of technology and the evolving legal landscape provide new perspectives on privacy and data protection issues in today's era. Privacy is about avoiding interference with the interests of others. With technological advancements, privacy has become a concern for every individual, highlighting the need for data protection. Data protection emphasizes individual liberty, which is increasingly threatened by intrusions from strangers. It is crucial to halt unauthorized access to an individual's activities by any means. The basic legal requirements for any emerging issue can be validated through the constitution. The Indian Constitution places greater emphasis on rights than on duties. Therefore, data protection is considered from a rights-based perspective. As a developing nation, India requires time to implement and enforce this new area of law effectively. The issue of data protection intersects with various areas, including the Right to Privacy, Right to Information, Information Technology, the Indian Penal Code, National Security, Intellectual Property, Corporate Affairs, and Consumer Protection. The aim of this research is to examine the current legal status of privacy and data protection in India as a matter of right. The constitutionality of privacy and data protection has gained significant importance in recent times, underscoring the need to accord it special status within the legal framework. It is essential to analyze the effectiveness of the existing legal framework to ensure robust protection of privacy. This research explores how the nature of individual rights is impacted by data protection concerns in relation to other laws. The goal of presenting this theme is to align India's approach with that of other countries.

Keywords: Data Protection, Constitutional Law, Privacy, Information Technology, Indian Penal Code, Intellectual Property Rights,Bharatiya Nyaya Sanhita.

Introduction:

Rights, inherent and inalienable characteristics of human society, have been codified into visible and enforceable documents at both international and national levels.[1] Some rights are explicitly mentioned in these documents, while others are introduced through interpretative tools due to their intrinsic connection with recognized rights. Among these, the right to privacy stands out as one of the most significant and universally accepted personal rights, granting individuals protection from intrusion by others. The right to privacy is referenced in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Convention on the Rights of the Child.[2] It is considered a fundamental aspect of human life. In India, this right has been recognized as an integral part of the right to life and liberty and the right to freedom of speech and expression.

Every person is entitled to a 'personal domain' free from unjustified interference or surveillance by the State or other entities. Despite the widespread recognition of the duty to protect privacy, the specific details of this right have not been fully articulated by international human rights protection mechanisms. This lack of clarity has led to challenges in its application and enforcement. Since the right to privacy is a qualified right, its interpretation presents challenges, particularly in defining what constitutes the private sphere and what qualifies as public interest. The right to privacy can be encroached upon in the name of public interest, especially through communication mediums. The privacy of communications implies that individuals should be able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State. These rights enable individuals to exercise their right to privacy within communication systems.

The mid-20th century saw the documentation of a right related to non-interference in an individual's personal life, which has gained importance with the commodification of technology. Technology has permeated every aspect of human life. Intrusions into personal life through advanced technology have become a daily occurrence, whether through voluntary disclosure or involuntary acquisition of information. The surveillance capabilities of powerful computer systems have led to demands for specific regulations on the collection and handling

[1] Prakash Shah, "International human Rights: A perspective from India," Fordham International Law Journal, Vol. 21, Issue 1, Article 3, (1997): 24- 38.

[2] Article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Accessed on August 24,2024

of personal data. The origins of modern legislation in this area can be traced back to the protection of individual privacy, culminating in the world's first data protection law. Data protection, a subset of privacy, has now become an international concern. Establishing data protection from a human rights perspective is essential, as the right to privacy inherently includes the right to data protection. This area is continually evolving due to technological advancements.[3]

Concept of Data Protection:-

The concept of data protection is gaining significant importance worldwide. Gradually, nations are adopting data protection principles and enacting laws to regulate the use and misuse of personal information.[4] The term "data protection" is derived from the German word "Datenschutz." Data protection is closely linked to individual privacy, though it encompasses a broader set of norms that serve various interests beyond just privacy protection. It considers not only privacy but also concepts such as "freedom," "liberty," and "autonomy." A fundamental question that arises is whether data protection is considered a right. A key emerging issue in this field is the extent to which data protection laws should also safeguard organizations and groups. Data protection is predominantly focused on protecting individual information, often referred to as "data subjects," who are narrowly defined as "living individuals." Consequently, corporate entities, such as limited companies, do not have the right to access information about themselves, as they are not considered data subjects, and information about them is not classified as personal data.

Thus, the authoritative value of data protection remains a contentious issue. A key debate is whether the state, non-state actors, or individuals should protect data as a matter of right. For non-state actors, two essential aspects of data protection emerge. Firstly, the narrower perspective argues that legislation should cover organizations, especially smaller enterprises, as information about the organization may indirectly reveal details about its owners and controllers. Secondly, the broader perspective suggests that organizations have legitimate rights

[3] Nicholas D. Wells, Poorvi Chothani and James M. Thurman, Information Services, "Technology, and Data Protection," The International Lawyer, Vol. 44, No. 1, International Legal Developments Year in Review: 2009 (2010): 355-366

[4] Section 2 (o) of the Information Technology Act, 2008 provides "Data" means 'a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, and punched tapes) or stored internally in the memory of the computer"

regarding information held about them by others, similar to the rights individuals have concerning their personal data

The concept of data protection is guided by various directives across different countries. The European Union has established comprehensive data protection laws.[5] Under EU law, personal data can only be collected legally under strict conditions and for legitimate purposes. Additionally, individuals or organizations that collect and manage personal data must protect it from misuse and respect the rights of data owners as guaranteed by EU law. The lack of overarching privacy legislation in the U.S. is a significant concern for EU countries, making it unlikely for the U.S. to be deemed as providing an adequate level of protection. Although there are ongoing efforts within the U.S. administration to introduce privacy legislation covering various types of data[6], the numerous privacy-related bills in Congress indicate that the U.S. may continue to adopt a piecemeal approach to privacy legislation.[7]

Constitutional Status:-

The constitution of India has some provisions like, 'Freedom of Speech and Expression'[8] and 'Right to Life and Personal Liberty'[9]

These provisions impact the recognition of the right to privacy as a fundamental right. Numerous court cases[10] have also established privacy as a fundamental right. The concept is further linked to the emerging dimension of 'Data Protection.' The relationship between privacy and data protection is interdependent. The right to data protection is closely associated with an individual's 'information.'

[5] Handbook of European Union Data Protection laws, Accessed August 21,2024 https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection%02law-2nd-ed_en.pdf
[6] Secretary of Health and Human Services, Shalala made recommendations to Congress on the Confidentiality of Individually-Identifiable Health Information on September 11, 1997
[7] Rebecca Vesely "Cop-friendly Approach to Handling Medical Data," Wired News 12 (September 1997) Accessed August 22,2024 https://www.wired.com/news/news/politics/story/6824.html
[8] Article 19 (1) (a) of the Indian Constitution
[9] Article 21 of the Indian constitution
[10] R Rajagopal v. State of Tamil Nadu AIR 1995 SC 264; Sharda v. Dharampal, AIR 2003 SC 3450; District Registrar and Collector v. Canara Bank, (2005)1 SCC 496; State of Karnataka v. Krishnappa AIR 2000 SC 1470; State v. N. M. T. Joy Immaculate, AIR 2004 SC 2282; X v. Hospital Z AIR 1999 SC 495; Kottabomman transport Corporation Limited v. State Bank Of Travancore and others, AIR 1992 Ker. 351; Registrar and Collector, Hyderabad and Anr. v. Canara Bank Etc AIR 2004 SC 935;

The study examines constitutional provisions to understand the relationship between privacy and explicitly stated rights, along with the interpretations provided by the country's apex court.[11] It also explores how data protection issues are addressed under various legislations. Finally, it argues for approaching data protection issues from a rights-based perspective.

Regarding human rights, Sir John Simmons states, "Human rights are rights that all human beings possess [at all times and in all places] simply because they are human... [These rights] exhibit properties such as universality, independence [from social or legal recognition], naturalness, inalienability, non-forfeitability, and imprescriptibility. Only when understood in this way can the concept of human rights capture the core idea that these rights can always be claimed by any human being."[12] Therefore, protecting human rights inherently involves protecting data. The universality and independence of data protection are crucial for individuals, as data protection is closely linked to the right to privacy.

The most important and enlightening discussion is that privacy and data protection are linked but distinct concepts. These connections extend into various interrelated areas within these domains. Privacy relates to seclusion, solitude, and isolation, although it is not identical to these terms. It goes beyond merely descriptive aspects, such as withdrawal from the presence, curiosity, and influence of others, to include the right to exclusive control over access to personal spaces. The role of the courts in advocating for this evolving right has also been highlighted as a crucial aspect of recognizing it as a right.

[11] It has held that in a case of *Ram Jethmalani & Ors* v. *Union of India*, (2011) 8 SCC 1. “Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner. Revelation of bank account details of individuals, without establishment of prima facie grounds to accuse them of wrong doing, would be a violation of their rights to privacy. State cannot compel citizens to reveal, or itself reveal details of their bank accounts to the public at large, either to receive benefits from the State or to facilitate investigations, and prosecutions of such individuals, unless the State itself has, through properly conducted investigations, within the four corners of constitutional permissibility.”

[12] Beitz (2004): 196, Simmons (2001)

Individual rights can be acquired naturally, and the right to privacy should also be attained naturally. In his influential article, Are There Any Natural Rights?,13 jurist Herbert Hart distinguishes between 'general rights' and 'special rights.' Special rights emerge from 'special transactions [or] special relationships,' such as promises, contracts, or political society membership. In contrast, general rights are those that belong to 'all men capable of choice... in the absence of those special conditions that give rise to special rights.' This perspective raises the question of whether data protection is considered a general or special right, a topic explored in this work.

Analysis of the Right Based Approach:-

A rights-based approach to scrutinizing the issue of data protection can only be achieved through examining various laws. The objective of this approach is to analyze the position of the data protection regime in India. Recently, the issue of data protection has gained significant importance, driven by the growth of internet-enabled services, which has led to a surge in outsourcing activities such as data processing, business processes, call center services, accounting, and other business operations. While technology continues to evolve, laws are also being adapted to keep pace with these advancements. Therefore, data protection examines how well the information, details, and data of individuals and organizations are safeguarded under Indian laws, particularly the Constitution of India.[14]

The focus is on the protection provided under the Constitution of India, as it serves as the "basic and ultimate source" from which all other laws derive their validity and authority. Three key aspects must be addressed when discussing the constitutional dimension: (1) Privacy rights of individuals in both real and cyberspace; (2) The mandates of freedom of information under Article 19(1)(a); and (3) The mandates of the public's right to know under Article 21. These aspects clearly cover the right to privacy, the right to information, the right to know, electronic governance, trade secrets, intellectual property, and other related matters from different perspectives. This research is conducted to justify the relationship between these rights. Additionally, this work identifies a gap in achieving a balance between information and

[13] H L A Hart, "Are There Any Natural Rights?" The Philosophical Review Vol 64, NO 2 (1955): 175-191,
[14] Dr. Amit Ludri, Law on protection of personal & official information in India, The Bright Law house, New Delhi, 1st Edition, (2010).

data processes.[15] A rights-based approach can only be justified by examining these issues in relation to other laws, as outlined below.

Data Protection & Right to privacy:-

'Data protection' and the 'right to privacy' are closely related concepts. Effective data protection is only possible if invasions of privacy are prevented. Privacy laws, particularly those concerning informational privacy, have always been closely tied to technological advancements. In their seminal 1890 article, The Right to Privacy, Warren and Brandeis lamented how "instantaneous photographs and newspaper enterprises" had intruded upon the private and domestic spheres, warning that various mechanical devices could make the prediction come true that "what is whispered in the closet shall be proclaimed from the house-tops." This marks the genesis of privacy concerns, which have now evolved into the realm of 'data protection.'

The concept of data protection has several dimensions. These include the right to access data banks, the right to verify the accuracy of data, the right to update and correct information, the right to keep sensitive data confidential, and the right to control the dissemination of personal data. Together, these rights form what is now considered the modern right to privacy.[16] Therefore, the connection between 'data protection' and 'privacy' is highly relevant within a rights-based framework.

The evolution of the constitutional right to privacy in India began in the early 1950s, particularly in the context of police surveillance and domiciliary visits to individuals' homes. Such visits could be made at any time, day or night, to check for suspicious criminal activities. In the case of *M.P. Sharma v. Satish Chandra*,[17] the Supreme Court addressed the issue of whether search and seizure violated Article 19(1)(f) of the Constitution. The Court ruled that a mere search did not infringe on property rights, and while seizure did impact property, this effect was temporary and constituted a reasonable restriction on privacy rights.

[15] Praveen Dalal, "Data Protection laws in India: A Constitutional Perspective,"Accessed August 22,2024 https://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-IN%02INDIA.pdf.
[16] I. N. Walden and R. N. Savage, "Data Protection and Privacy Laws: Should Organizations Be Protected?"The International and Comparative Law Quarterly, Vol. 37, No. 2 (1988): 337-347
[17] AIR 1954 SCR 1077.

Over time, the right to privacy has been recognized and developed under Articles 19(1)(a) and 21 of the Indian Constitution. Additionally, the right to liberty under Article 21 was further addressed by Justice Subba Rao in the case of *Kharak Singh v. State*.[18]

In another landmark case[19], the Supreme Court of India further advanced the law on privacy by addressing issues related to police domiciliary visits and the disclosure of information. These concerns are closely related to modern data protection issues. In *R. Rajagopal v. State of Tamil Nadu*,[20] the petitioner, who was the editor, printer, and publisher of a Tamil weekly magazine in Madras, sought to prevent the State of Tamil Nadu from interfering with the authorized publication of an autobiography by Auto Shankar, a condemned prisoner awaiting execution, which was based on public records. In this case,[21] Justice Jeevan Reddy reaffirmed that the right to privacy is implicit in the right to life and liberty guaranteed by Article 21 of the Constitution. The Court also upheld the 'right to be let alone' for every citizen to protect their privacy. Thus, the 'right to privacy' has significantly contributed to the development of data protection issues. Both concepts are recognized as fundamental rights under the Constitution of India.

Data Protection & Right to Information Act, 2005:-

In India, the Right to Information (RTI) is established with the goal of allowing citizens to access information held by public authorities to enhance transparency and accountability. This objective is outlined in the preamble of the RTI Act, 2005, which aims to facilitate access to information related to public authorities and matters connected or incidental to it.[22] Section 2(j) of the Act defines the 'right to information.' The issue now arises as to whether the data held by public authorities is secure.

There is concern over whether digital data, as specified in clause (iv) of Section 2(j), is being properly maintained or if there are doubts about its security.

[18] AIR 1963 SC 1295.
[19] *Govind* v. *State of Madhya Pradesh*, AIR 1975 SC 1378.
[20] 1994) 6 SCC 632.
[21] (1994) 6 SCC 632.
[22] Ministry of Law & Justice (2005a), Accessed August,23,2024 http://lawmin.nic.in/legis.htm

The 'data protection' aspect addressed by this Act is regarded as an individual's right. In the case of Bennett Coleman v. Union of India,[23] the court affirmed that 'freedom of the press' encompasses the right of all citizens to speak, publish, and express their views, and that 'freedom of speech and expression' includes the right of all citizens to read and be informed. Similarly, in Indian Express Newspaper (Bombay) v. Union of India,[24] the Court held that the fundamental purpose of freedom of speech and expression is to enable individuals to form and communicate their beliefs freely. In essence, the core principle is the people's right to know.

Therefore, the connection between these two contexts can be established through the judgments of the apex court. In the case of *PUCL v. Union of India*,[25] the Court elevated the right to information to the status of a human right, essential for ensuring transparent and accountable governance. The Supreme Court has consistently affirmed that the right to information is inherent in Article 19 of the Constitution. This reinforces that the linkage between these two contexts is closely related to a rights-based approach.

Data Protection & Information Technology (Amendment) Act 2008:[26]

The relationship between 'data protection' and the 'Information Technology Act' is significant. The objectives of the Act address the protection of matters related to cyber activities, including safeguards against certain data breaches involving computer systems. The Act includes provisions to prevent the unlawful use of computers, computer systems, and the data stored within them. Several sections of the Act pertain specifically to data protection, including the new Section 43A and Section 72A, which clearly outline measures for data protection

The 2008 Amendment Act represents a significant step forward in addressing the various crimes associated with the cyber age. The changes made to statutory data protection in Indian laws have responded to the demands of the US and European nations over the past decade. Service providers now face imprisonment for disclosing personal information in

[23] AIR 1973 SC 60.
[24] (1985)1 SCC 641.
[25] (2004) 2 SCC 476
[26] Information Technology (Amendment) Act 2008, Accessed August,22,2024 http://www.cyberlawconsulting.com/itact2008amendments.pdf.

violation of contractual obligations. Additionally, the unauthorized disclosure of 'sensitive personal information'[27] makes the perpetrator liable for damages.

As a matter of right, data protection has been afforded significant status. The technological advancements have led to a focus on analyzing EU Data Protection legislation alongside the Indian Information Technology (Amendment) Act, 2008. This analysis covers various aspects such as corporate data handling—access, sharing, disclosure, publication, security measures, and penalties under the Information Technology Act, 2000. Additionally, the IT Rules, 2011, also reflect concerns about data protection rights in their provisions.[28]

The importance of the outsourcing industry in India and its potential impact on business relations with European Union companies is also discussed. The article reviews the recently notified regulations related to the protection of sensitive personal data and compares them with the UK Data Protection Act, 1998.[29] Overall, the emphasis is on asserting the individual right to data protection within a rights-based framework.

Overview of the Digital Personal Data Protection Act, 2023:-

The DPDP Act is a recent legislative measure in India that addresses the processing of personal data. It was enacted nearly six years after the Supreme Court acknowledged the fundamental right to privacy under Article 21. Drawing from global privacy laws such as the European Union's GDPR, the DPDP Act focuses on privacy and data protection obligations related to personal data. It is noted for incorporating several concepts directly from the GDPR and has a broad applicability that extends beyond India's borders. While the Act imposes strict obligations to prevent the unlawful processing of personal data, it also provides significant exceptions for governmental bodies. The DPDP Act establishes a comprehensive framework for personal data processing, effectively replacing the limited provisions previously found in the IT Act. Here are some key aspects of the DPDP Act:

Bodies Established Under the DPDP Act: The Act employs various terms that may initially appear confusing. It is crucial to understand the distinctions between terms such as data

[27] Under the Personal Data (protection) Bill 2013, Section 2 (p) "personal data"52 means any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data.
[28] Information Technology Rules 2011, Accessed August,20,2024 https://www.ijlt.in/pdffiles/IT-%28Reasonable-Security-Practices%29-Rules-2011.pdf.
[29] Raghunath Ananthapur, "India's New Data Protection Legislation", Volume 8, Issue 2, (2011).

processors, data fiduciaries, data principals, and data controllers. The individual whose personal data is collected is referred to as the data principal. The data fiduciary is the entity that determines the purpose and means of processing personal data, a role similar to that of a data controller.

Exceptions Permitted Under the DPDP Act: The Act allows for exceptions in matters related to the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, maintaining public order, and preventing incitement to commit offenses.

Applicability of the DPDP Act: The Act has extra-territorial applicability, meaning it applies beyond India's borders, and it places no restrictions on international data transfers.

Grounds for Lawful Processing of Personal Data: Consent is the primary basis for the lawful processing of personal data. Additionally, data fiduciaries can identify legitimate interests as grounds for the lawful processing of data.

Rights and Obligations of Data Subjects: Data principals have rights such as the right to access their data, the right to erasure, and the right to object to certain processing activities. There are also obligations imposed, and non-compliance with these obligations can result in fines and penalties.

Data Protection & Indian Penal Code:-

The Indian Penal Code (IPC) has its origins in the British colonial era, with its initial draft formulated in the 1860s under the leadership of Lord Macaulay. However, the IPC's provisions do not fully address the modern needs of data protection. Indian criminal law does not specifically target breaches of data privacy; instead, liability for such breaches must be inferred from related crimes.

For example, Section 403 of the IPC penalizes dishonest misappropriation or conversion of "movable property"[30] for personal use. Similarly, Sections 405 and 409 address criminal breach of trust when someone misappropriates another person's property. Section 378

[30] Movable property' has been defined as property which is not attached to anything and is not a land.

defines theft as dishonestly taking movable property without consent. Despite these provisions, there is no specific legislation within the IPC concerning electronic data protection.

Two primary approaches exist for addressing legal rights in this context. Generally, crimes are considered offenses against the state, which has a responsibility to maintain law and order. While the IPC outlines penalties for certain offenses, civil actions for damages, including the amount of damages, are determined by the court.[31]

Thus, while the relationship between data protection and the IPC is somewhat indirect, the state's role in protecting individuals' data remains a critical concern. The need for specific data protection measures within the legal framework is evident.

Data Protection and Bharatiya Nyaya Sanhita (BNS):-

As of now, there is no specific mention of data protection laws directly related to the Bharatiya Nyaya Sanhita (BNS). The BNS, which translates to the Indian Penal Code, focuses primarily on criminal law, defining offenses and prescribing punishments for them. However, with the increasing relevance of data protection in the digital age, there are intersections where data protection concerns could come under the purview of general laws or require new adaptations in the context of the BNS.

Here's how data protection laws might relate to or influence aspects of the Bharatiya Nyaya Sanhita:

1. **Criminal Offenses Related to Data Protection:**

Cybercrime and Unauthorized Access: The BNS could address criminal offenses such as unauthorized access to computer systems, hacking, data theft, and cyberstalking. Under the DPDP Act and other data protection frameworks, unauthorized access and misuse of personal data are considered violations, and appropriate criminal penalties could be integrated into the BNS.

Data Breach and Identity Theft: The BNS might need to accommodate specific provisions to deal with crimes involving data breaches, where personal data is accessed or exposed without

[31] Denis O'Brien, "The Right of Privacy," Columbia Law Review, Vol. 2, No. 7 (1902): 437-448.

authorization, leading to identity theft or fraud. Existing sections dealing with fraud, forgery, or misrepresentation might be expanded to cover these digital offenses.

2. Interplay Between DPDP Act and BNS:

Legal Accountability: Data protection laws like the DPDP Act impose obligations on data fiduciaries to ensure the security and lawful processing of personal data. If these obligations are breached, and the breach leads to harm or criminal activity, the BNS could potentially be invoked to prosecute those responsible for the harm.

Admissibility of Digital Evidence: Provisions within the BNS may need to address the standards for the admissibility of digital evidence, ensuring that evidence collected from data breaches or cybercrimes meets legal criteria for use in prosecution.

3. **Rights and Remedies for Victims:**

Victim Compensation and Remedies: The BNS, in coordination with data protection laws, could outline rights and remedies available to victims of data breaches or identity theft. This might include compensation mechanisms and rights to seek redress.

4**. Exceptions and National Security:**

Law Enforcement Access: While the DPDP Act provides a framework for data protection, exceptions related to national security, public order, and law enforcement are recognized. The BNS may play a role in defining the scope and limits of these exceptions, ensuring that data protection rights are balanced with the need to maintain public safety and order.

5. **Training and Awareness:**

Legal Awareness Programs: As data-related offenses become more prevalent, integrating knowledge about data protection laws into legal training programs related to the BNS could be crucial. This would ensure that law enforcement officers and the judiciary are well-versed in handling data protection issues within the framework of criminal law.

Data Protection & National Security:-

In today's world, the relationship between data protection and national security is highly

relevant. National security and law enforcement agencies play a crucial role in data protection across all countries. For example, in 2013,[32] Edward Snowden's release of sensitive privacy-related data from the United States sparked significant controversy and raised questions about individual privacy. The exposure of such data to the public highlighted concerns about the effectiveness of privacy protections.

The situation underscores that if data is accessible to individuals and publicly exposed, it challenges the notion of privacy. This issue is particularly pronounced in developed countries with advanced technology, but it also raises concerns for developing nations. The role of national security in protecting data is critical, and addressing this issue through a rights-based approach is essential for establishing proper privacy protections.

In similar situations, national security and law enforcement are often exempt from strict data protection laws or are broadly permitted to access data. This is the case in many countries, including those with advanced data protection frameworks. For instance, Dan Svantesson notes that Australian laws collectively grant law enforcement and national security agencies extensive access to private-sector data[33]. As a result, data collection and use for national security and law enforcement purposes are frequently excluded from the stringent oversight that applies to other data processing activities, or they are governed by less transparent standards and oversight regimes.

Protection against authorities is essential when examining a rights-based approach, especially regarding the police's ability to track cell phones, except in limited time-sensitive situations and emergencies. Modern technology allows law enforcement agencies to monitor individuals' movements continuously, including geolocation tracking. This issue involves the use of cellular location technology by police to monitor cell phone users, focusing on methods such as cell site tracking, GPS, and Wi-Fi technology. It highlights the need for legislation in this area, as cell phone tracking is becoming a widespread practice that might partially replace federally regulated wiretapping. While such surveillance can be justified for national security reasons, it also raises significant concerns about personal privacy.

[32] Law Enforcement, National Security, and Privacy, Accessed August,23,2024 https://cis-india.org/internet-governance/blog/law-enforcement-national%02security-privacy.pdf.
[33] Dan Jerker B. Svantesson, "Systematic Government Access to PrivateSector Data in Australia," 2/4 International Data Privacy Law, (2012): doi: 10.1093/idpl/ips021

In the case of District Registrar and Collector, Hyderabad v. Canara Bank,[34] the Supreme Court held that the search and seizure of registers, books, records, papers, documents, or other proceedings by enforcement agencies, conducted to collect evidence or uncover fraud and omissions related to stamp duty payments, constitute an infringement on individuals' rights. The Court emphasized that secrecy and confidentiality must be maintained in such situations.

Establishing individual rights, such as privacy and data protection, is crucial for addressing the growing issues of cybercrime and cybersecurity. Concerns about data protection and human rights are closely related and involve considerations of privacy and data security across all countries. The ongoing philosophical debate around the dichotomy of "security vs. privacy" or "interest vs. right" hinges on the idea that there must always be a balance, guided by some weighing rule that limits one in favor of the other. This discussion also introduces concepts such as data, data controllers, data processors, data storage, and proposed regulations.

Data Protection & Intellectual Property Law:-

The relationship between 'data protection' and 'intellectual property law' needs to be analyzed from a rights-based perspective, particularly concerning computer-related database work. Under Section 63B of the Indian Copyright Act, any person who knowingly uses an infringing copy of a computer program on a computer is liable for infringement. An individual's intellectual property rights are based on factors such as 'labor, skill, and judgment.' When literary, dramatic, musical, artistic, or cinematographic works are recognized by law, protecting the rights of the owner of those works becomes essential. However, distinguishing between data protection and database protection under the Copyright Act[35] can be challenging.

Data protection focuses on safeguarding individuals' informational privacy, whereas database protection serves a different purpose by safeguarding the creativity and investment involved in compiling, verifying, and presenting databases. Legal concepts such as access, privacy, ownership, and evidence are applicable across various relationships but can also be used to analyze the rights and obligations of those involved in professional and business recordkeeping. In this context, property law can be applied to records not just as physical objects but as entities representing legal relationships. Examples of differing needs among

[34]AIR 2005 SC 186.
[35] THE COPYRIGHT(AMENDMENT)ACT,20l2, Accessed August,21,2024 https://www.wipo.int/edocs/lexdocs/laws/en/in/in066en.pdf.

recordkeeping participants include access rights and intellectual property rights and obligations. Privacy protection must be balanced with the necessity of retaining identity information over time to establish rights and obligations.

A rights-and-obligations approach attributes responsibility for creating, documenting, and preserving evidence to various parties within a network of relationships, including the author, recipient, data subjects, and third parties, which is equally relevant in the online environment.[36]

Similarly, both data protection and intellectual property rights play crucial roles in protecting individual rights. They address four types of privacy: informational privacy, bodily privacy, privacy of communication, and territorial privacy.[37] Various models, including the intellectual property rights model, moral rights model, and trade secrecy model, form the foundation of the rights-based approach. In the broader context of intellectual property, an author's right must be established as a legal right, granting them control over the use or disclosure of personal data. Additionally, it is argued that the government should adopt a flexible and responsive approach to protecting personal data, including considering property rights-related solutions.[38]

Data Protection & Corporate affairs:-

The relationship between data protection and corporate affairs also aligns with a rights-based approach. Corporations are significantly impacted by issues related to data access, disclosure, sharing, and processing. The role of data processors or data controllers is crucial in the corporate sector, as they often face decisions about whether to share information. This creates a conflict between private and public organizations and enforcement agencies. In the commercial online environment, users are often required to submit personal information to access services or order products. This raises concerns about whether the authorities handling this data are adhering to public policies. For instance, in the banking sector, bankers have an obligation not to disclose client information, as this could breach their duty of secrecy and

[36] Property, privacy, access and evidence as legal and social relationships, Accessed August,20,2024 http://download.springer.com/static/pdf/977/chp%253A10.1007%252F1-4020-4714-2_5.pdf?auth66=1424433931_1c7e42dfa070decb666a36746471f322&ext=.pdf.
[37] Available at,https://gilc.org/privacy/survey/intro.html (Accessed August,21,2024)
[38] M M S Karki, "Personal Data Privacy & Intellectual Property,"Journal of Intellectual Property Rights, Vol 10. (2005): 59-63.

confidentiality. However, the right to privacy for banking customers can be limited when it conflicts with the right to information and the public's right to know.

In another area, the Securities and Exchange Board of India Act (1992) establishes the Securities and Exchange Board of India (SEBI) to oversee and regulate the use of individuals' credit information. Under the Act, the government's access to private-sector data related to the securities market is facilitated through SEBI, which is granted broad access. However, SEBI is only authorized to conduct inspections if there are reasonable grounds to believe that insider trading is occurring, fraudulent or unfair trading practices are being used, securities transactions are being handled in a manner detrimental to investors, or an intermediary or any person associated with the securities market is violating provisions of the Act. The Act reinforces the conditions for reactive access and disclosure of information by imposing penalties on those who fail to provide the required information.[39]

In another aspect of corporate affairs, the Credit Information Companies Regulation Act, 2005 (CICRA)[40] mandates that credit information related to individuals in India must be collected in accordance with the privacy norms established by the CICRA regulations. Entities responsible for collecting and maintaining this data are held liable for any potential exposure or alteration of the information. Drawing from the principles of the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act,[41] CICRA has established a rigorous framework for the handling of credit and financial information of both individuals and companies in India. The regulations under CICRA, which outline stringent data privacy principles, have recently been issued by the Reserve Bank of India. In this context, the relationship between ‘data protection’ and ‘corporate affairs’ aligns with the ‘rights-based approach.

Data Protection & Consumer:-

The relationship between consumers and organizations plays a crucial role in addressing the issue of data protection. In the case of Shakankarlal Agarwalla v. State Bank of India,[42] the Calcutta High Court ruled that bankers have an obligation to maintain

[39] Mr. K.J. Doraisamy v. The Assistant General Manager, State Bank of India and others, (2007) 136 Comp Cases 568 (Mad).
[40] SECURITIES AND EXCHANGE BOARD OF INDIA ACT 1992, Accessed August,23,2024 https://www.sebi.gov.in/acts/act15ac.pdf.
[41] Accessed August,22,2024 http://www.dataquick.com/wp-content/uploads/2013/02/GLB-outline.pdf.
[42] AIR 1987 Cal 29.

confidentiality. As per Lord Halsbury's Laws of England, "it is an implied term of the contract between a banker and a customer that the banker will not disclose to a third party, without the express or implied consent of the customer, either the state of the customer's account, any of the customer's transactions with the bank, or any information relating to the customer obtained through maintaining their account, unless compelled by a court order, a public duty of disclosure arises, or the protection of the banker's own interests necessitates it."

In the context of e-commerce, data protection faces significant challenges, with misuse increasing daily. A notable issue is BPO fraud, which falls under the penal provisions of the IT Act.[43]

Conclusion:-

The analysis of various themes underscores that data protection is increasingly recognized as a fundamental right from multiple perspectives. Key areas such as the right to privacy, right to information, information technology, Indian Penal Code, corporate affairs, and consumer rights all support the recognition of data protection as a fundamental right. This research aims to reinforce the concept of data protection as a fundamental right in the context of technological advancements. As technology continues to evolve, there is a growing need to enhance data protection regimes to safeguard individual liberties.

The goal of this research is to establish data protection and privacy rights as fundamental rights. It is justified to treat these rights as fundamental to protect against interference and infringement on individual liberties. Achieving institutional recognition of data protection can offer a universal approach to safeguarding these rights. To elevate data protection to a fundamental right, the legal framework should comprehensively address aspects such as data collection, processing, storage, security, and access. Raising global awareness about the rights-based approach to data protection and privacy is essential for widespread acceptance and implementation.

[43] Adv. Swati Sinha, "Data Protection Law in India-Needs and Position," Accessed August,24,2024

Bibliography:-

. Puttaswamy, K.S. (2014). Constitutionalizing Privacy. Eastern Book Company.

. Chandrachud, A. (Ed.). (2018). The Right to Privacy Judgment: The Supreme Court Opinion. Bloomsbury Publishing India Pvt. Ltd.

. Bhatia, G. (2017). The Transformative Constitution: A Radical Biography in Nine Acts. HarperCollins India.

. Mathew, T.G. (Ed.). (2014). Right to Privacy. Universal Law Publishing.

. Basu, D.D. (2007). Right to Privacy: Comparative Perspectives. Oxford University Press.

. Subramanian, K.S. (2016). The Domain of Privacy. Oxford University Press.

. Sengupta, R. (2019). Privacy and Right to Information: Comparative Perspectives. Cambridge University Press India.

. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

. The Personal Data Protection Bill, 2019.

. Shreya Singhal vs Union of India, (2015) 5 SCC 1.