*Page 1038 - 1052* **DOI:** *https://doij.org/10.10000/IJLMH.114155*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 6 | Issue 1**

**2023**

# Critical Analysis of Right to Privacy in India

J. NISSHA[1]


## ABSTRACT

*The current state of privacy and data protection concerns can be viewed in light of technological development and legal dynamism. Privacy means not interfering with other people's interests. Because of advancements in technology, privacy has become a concern for every individual, and it also places a strong emphasis on data protection. Individual liberty is a focus of data protection, and the intrusion of a stranger jeopardises this liberty. The individual's activity must cease in any way possible by the stranger to the individual. The constitution can be used to confirm any new phenomenon's fundamental legal requirement. The Indian constitution places a greater emphasis on the right than on duty. Consider it a right-based strategy for placing an emphasis on data protection. The new area of law will take some time to become effective because India is a developing nation. The Right to Privacy, Right to Information, Information Technology, Indian Penal Code, National Security, Intellectual Property, Corporate Affairs, Consumer, and other areas are the primary focus of the data protection issue. The research project's goals are to investigate the rightful legal status of privacy and data protection in India. In recent times, the constitutionality of data protection and privacy has received a lot of attention.*

*Because of this, it is necessary to provide a unique status within the legal framework. To provide sophisticated privacy protection, it is necessary to investigate the effectiveness of the current legal framework. It investigates how the encroachment of data protection in relation to other laws has affected individuals' rights. The idea behind this topic is to link the concept of India to other countries.*


***Keywords**: Data Protection, Constitution, Privacy, Information Technology, Indian Penal Code, Intellectual Property.*

## I. INTRODUCTION

In the international and national spheres, rights, an inherent and inalienable characteristic of human society, have been reduced into a visible and implementable document[2]. Some rights are explicitly mentioned in such documents, while others are introduced through interpretative tools due to their integral connection to those rights. The right to privacy is one of the most significant and laudable of these rights. It grants individual snooping by others authority. The Universal

[1] Author is a LL.M. (Constitutional Law and Human Right) student in India.

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

 [ISSN 2581-5369]

Declaration of Human Rights and the International Covenants of Civil and Political Rights, as well as the Convention on the Rights of the Child, both make mention of the right to privacy[3]. The right to privacy is the most essential aspect of human life[4]. In India, this right has been identified as an essential component of the right to life, liberty, and freedom of speech expression.[5]

Every person has the right to a "personal domain" where the State or other actors can't interfere or watch them unjustifiably. International human rights protection mechanisms did not fully develop the specific content of this right, despite widespread recognition of the obligation to protect privacy.

As the right to privacy is a qualified right, its interpretation raises challenges regarding the organization of the private sphere and the establishment of notions of what constitutes the public interest. This has contributed to difficulties in its application and enforcement[6]. The right of the human person was violated through the medium of communication as a matter of public interest. Individuals are able to exchange ideas and information in a space that is out of reach of other members of society, the private sector, and ultimately the State itself, according to the privacy of communications conclusion. These rights only permit an individual to exercise their right to privacy within a communication system[7].

At the middle of the 20th century, a right that related to non-interference in one's personal life was documented. It has gained significance as technology has become a commodity. Every facet of human existence has been affected by technology[8]. The intrusion of advanced technology into human life is now a common occurrence. It takes place either through the voluntary disclosure of information or through the involuntary acquisition of it. Specific guidelines for the collection and use of personal information were demanded as a result of

[3] 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 October 21, 2016,http://www.un.org/en/documents/udhr/, Article 17 (1), "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." Accessed October 21, 2016, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspxArticle 16 (1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. Accessed October 21, 2016,http://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

[4]Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (1890): 193-220.

[5] Article 21 & 19 (1)(a) of the Indian Constitution, See also Udai Raj Rai, Fundamental Rights and their enforcement, PHI Learning Private Limited, New Delhi, (2011) p.19. See also Kharak Singh v. The State of U.P. and Ors. AIR 1963 SC 1295

[6] UNESCO, Global Survey on Internet Privacy and Freedom of Expression, (2012): 51.

[7] S.K. Sharma, Privacy Law: A Comparative Study (Atlantic Publishers & Distributors: 1994).

[8] Austin, Lisa Michelle, "Privacy law and the question of technology." Ph.D. Thesis, University of Toronto; 2005, ProQuest Dissertations and Theses

powerful computer systems' surveillance capabilities. Data protection is the species of privacy and is now a global phenomenon[9]. The idea of establishing rights perspectives data protection as a human right. The genesis of modern legislation in this area can be traced through individual privacy to the first data protection law in the world.

A person's right to data security goes hand in hand with their right to privacy. Due to current technological advancement, the field of data protection is expanding[10].

## II. CONCEPT OF DATA PROTECTION

Data security is becoming increasingly important all over the world. The term "data protection" is derived from the German term "Datenschutz."[11] Gradually, all nations are adopting the concepts of data protection and enacting laws regulating the use and misuse of personal information.[12] The idea of data protection has less to do with the privacy of an individual[13] and more to do with a set of norms that serve a wider range of interests than just privacy protection[14].

Data security has taken into account more than just privacy concerns. The terms "freedom," "liberty," and "autonomy"[15] have also been mentioned, some of which overlap with one another. In this case, whether or not data protection is a right is the most important consideration for the individual.[16] This raises the question of how much organizations and groups should be protected

[9] Lee A. Bygrave, "Privacy and Data Protection in an International Perspective," Stockholm Institute for Scandinavian Law, (2010).

[10] 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.

[11] Further on the origins of "Datenschutz", Smitis, S. (ed.), "Bundesdatenschutzgesetz, Nomos Verlagsgesellschaft, Baden-Baden," 6th edition, (2006): 62–63.

[12] 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"

[13] Lutha R Nair, "Data Protection Efforts in India: Blind leading the Blind?," The Indian Journal of Law & Technology VOL 4 (2008).

[14] Bygrave, L.A., "Data Protection Law: Approaching Its Rationale, Logic and Limits," Kluwer Law International, The Hague / London / New York (2002).

[15] Westin, A.F., "Privacy and Freedom," Atheneum, New York (1970); Miller, A., "The Assault on Privacy: Computers, Data Banks and Dossiers," University of Michigan Press, Ann Arbor (1971). The title of Westin's seminal work, Privacy and Freedom, is a case in point. Indeed, as pointed out further below, "privacy" in this context has tended to be conceived essentially as a form of autonomy – i.e., one's ability to control the flow of information about oneself.

[16] In the case of The Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal & Anr. It is been held that "the right to access public information and processing of this information by the state agencies and governments, in democracies is an accountability measure empowering citizens to be aware of the actions taken by such state "actors". This transparency value, at the same time, has to be reconciled with the legal interests protected by law, such as other fundamental rights, particularly the fundamental right to privacy. Certain conflicts may underlie particular cases of access to information and the protection of personal data, arising from the fact that both rights cannot be exercised absolutely in all cases. The rights of all those affected must be respected, and no single right must prevail over others, except in clear and express circumstances. There are two types of information seen as exceptions to access; the first usually refers to those matters limited only to the State

by such laws. Regarding the individual's information security, this data protection concept is generally accepted. The protection of information laws for "data subjects," which are narrowly defined as "living individuals," is also included in the scope of data protection. Because the organization is not a data subject and the information about it is not personal data, a corporate body, such as a limited company, does not have the right to access any information about itself.[17]

As a result, data protection issues of authoritative value are regarded as a contentious issue. the actor, whether state or non-state, or the individual who will legitimately safeguard it. The two most important aspects of data protection for non-state actors are, first, the narrower meaning based on the argument that legislation should cover organizations, especially smaller ones, since information about the organization may indirectly be information about the owners and controllers of the organization. Second, the broader meaning is that organizations have the same legal rights as individuals regarding information about them that is held by others[18].

In various nations, the concept of data protection is regulated in some way. The Data Protection Law of the European Union is very sophisticated[19]. According to EU law, personal data can only be collected legally under very strict conditions and for a legitimate purpose. Additionally, individuals or organizations that collect and manage your personal information are required by EU law to respect certain data owners' rights and safeguard it from misuse. The EU nations are extremely concerned about the absence of generic privacy legislation in the United States, making it unlikely that the United States will guarantee an adequate level of protection. The large number of privacy-related bills in Congress suggests that the United States may continue to take a piecemeal approach to privacy legislation, despite the administration's concerted efforts to pass legislation covering a variety of data types[20].

## III. CONSTITUTIONAL STATUS

The "Right to Life and Personal Liberty"[21] and "Freedom of Speech and Expression"[22] clauses in India's constitution have an impact on the right to privacy as a fundamental right. The right

in protection of the general public good, such as national security, international relations, confidentiality in cabinet meetings, etc. The second class of information with state or its agencies, is personal data of individual citizens, investigative processes, or confidential information disclosed by artificial or juristic entities, like corporations, etc. Individuals' personal data is protected by the laws of access to confidential data and by privacy rights."

[17] Supra Note 13.

[18] Supra Note 13.

[19] Handbook of European Union Data Protection laws, Accessed October 21, 2016, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protectionlaw-2nd-ed_en.pdf.

[20] Secretary of Health and Human Services, Shalala made recommendations to Congress on the Confidentiality of Individually-Identifiable Health Information on September 11, 1997.

[21] Article 21 of the Indian constitution.

[22] Article 19 (1) (a) of the Indian Constitution

 [ISSN 2581-5369]

to privacy is also recognized as a fundamental right in a number of cases[23]. This proposition's conceptuality has also been linked to the new "Data Protection" dimension. The connection between data security and privacy is dependent on one another. The individual's "information"[24] is closely related to the right to data protection.

The study of constitutional provisions to understand the relationship between privacy and rights that are explicitly spelled out, as well as the interpretation given by the country's highest court.[25] It also looks at how different laws deal with the issue of data protection.[26] Finally, it makes a case for approaching the issue of data protection from a right-based perspective.

According to Sir John Simmons, "Human rights are rights that are possessed by all human beings [at all times and in all places], simply by virtue of their humanity....[They] will have the properties of universality, independence [from social or legal recognition], naturalness, inalienability [from social or legal recognition], naturalness, inalienability, non-forfeit ability, and imprescriptibility." [Citation needed] An account of human rights will only be able to capture the central concept of rights that can always be claimed by any human being if it is understood in this way.28 As a result, the concept of protecting human rights also includes protecting data. Individuals place a high value on the independence and universality of data protection. The right to privacy is also facilitated by data protection.

The most significant and instructive argument is that data protection and privacy have distinct connections. These interconnected links or shadows between various areas and the regime. Although not synonymous with these terms, privacy is a concept related to solitude, isolation, and seclusion; far beyond the purely descriptive aspects of privacy, such as withdrawing from

[23] 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;

[24] In a case, The CPIO, Supreme Court of India v. Subhash Chandra Agarwal and Anr. the Information Technology Act 2008, laid down the Definition of 2(f) "information" means ‘any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force’.

[25] 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.”

[26] Justice A P Shah Committee Report, “Report of the Group of Experts on Privacy”, (2012), Accessed October 21, 2016, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

 [ISSN 2581-5369]

company, being curious, and being influenced by others, which would imply the right to exclusive access control to individual realms. The court's activism as the pioneer of this developmental right is also being emphasized as a matter of right.

Individual rights can be acquired naturally, so the right to privacy must also be acquired naturally. The influential work of jurist Herbert Hart titled "Are There Any Natural Rights?" distinguishes between "general rights" and "special rights"29. Special rights come from "special transactions [or] special relationships" like promises, contracts, or membership in a political society, whereas general rights belong to "all men capable of choice...in the absence of those special conditions which give rise to special rights."30 This view that data protection is a general right or a special right is also being taken into consideration in this work.

## IV. ANALYSIS ON RIGHTS BASED APPROACHED

The various laws are the only means by which the right-based approach to the "data protection" issue can be examined. This strategy aims to examine India's "data protection" regime from a particular perspective. With the rise of internet-enabled services and the issue of data security taking center stage recently, outsourcing of data processing, business processes, call center services, accounting functions, and other business operations has skyrocketed. However, as technology has advanced, improvised laws have also been developed to accommodate it. Because the Constitution of India is the "basic and ultimate source" from which all other laws derive their validity and force, data protection examines the extent to which individuals' and organizations' information, details, and data are protected under Indian laws, particularly the Constitution of India[27]. (1) Privacy rights of interested parties in real space and cyberspace must be addressed for discussion of constitutional aspect concern. 2) Freedom of information requirements outlined in Article 19 (1) (a). 3) The requirements of the right to know of the general public under Article 21 The right to privacy, the right to information, the right to know, electronics governance, trade secrets, intellectual property, and other rights are all explicitly mentioned. in light of a variety of perspectives.

This research has been done to justify the relationship with rights. Another flaw in this work is that there is no equilibrium between data processing and information processing[28]. The right-based approach can only be supported by discussing other laws like the ones listed below:

## V. DATA PROTECTION AND RIGHT TO PRIVACY

[27] Beitz (2004): 196, Simmons (2001)
[28] H L A Hart, "Are There Any Natural Rights?" The Philosophical Review Vol 64, NO 2 (1955): 175-191

 [ISSN 2581-5369]

The terms "right to privacy" and "data protection" share many similarities. The so-called "data protection" can only be achieved if the invasion of privacy is stopped. In their seminal 1890 article titled "The Right to Privacy," privacy law in general and informational privacy in particular have always been closely linked to technological advancement.[29] Warren and Brandeis lament the "instantaneous photographs and newspaper enterprise that have invaded the sacred precincts of private and domestic life;" and numerous mechanical devices pose a threat to fulfill the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[30] This is currently being developed within "data protection." There are numerous aspects to the concept of "Data Protection."

The various rights associated with data protection, such as the right to access data banks, the right to verify their accuracy, the right to update and correct them, the right to keep sensitive data confidential, and the right to authorize their dissemination: As a right-based approach, the linkage of "Data Protection" and "Privacy" status is very much appropriate in this case. Together, all of these rights today make up the new right to privacy[31].

In the early 1950s, police surveillance of the accused and domiciliary visits to a person's home sparked the development of the Constitutional right to privacy. The domiciliary visits could be made at any time, day or night, to see if anyone was committing a suspicious crime. The Supreme Court ruled that the claim that search and seizure violated Article 19(1)(f) of the Constitution in the case M.P Sharma v. Satish Chandra[32]. Even though a seizure did have an effect on the right to property, the Court held that this effect was only temporary and was a reasonable restriction on the right to privacy. The right to privacy was then incorporated into the Indian Constitution under Articles 19 (1) (a) and 21. The right to liberty guaranteed by Article 21 of the Constitution is also discussed by Subba Rao, J. in the case of Kharak Singh v. State. In another significant case, the Supreme Court of India further developed the privacy law by ruling that a domiciliary police visit and the disclosure of information are the same thing. These disclosures of information approach the contemporary concern regarding data protection. Based on public records, the petitioner in R Rajagopal v. State of Tamilnadu[33] was the editor, printer, and publisher of a Tamil weekly magazine in Madras. They sought an order preventing

[29] Ibid, pp.183-188.
[30] Dr. Amit Ludri, Law on protection of personal & official information in India, The Bright Law house, New Delhi, 1st Edition, (2010).
[31] Praveen Dalal, "Data Protection laws in India: A Constitutional Perspective,"Accessed October 21, 2016, http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-ININDIA.pdf
[32] Graham Greenleaf and Sinta Dewi Rosadi, "Indonesia's data protection Regulation 2012: A brief code with data breach notification," Privacy Laws & Business International Report, Issue 122, (2013): 24-27.
[33] Supra Note 3.

the State of Tamilnadu from interfering with the authorized publication of Auto Shankar's autobiography, a condemned prisoner awaiting the death penalty. In this case[34], Jeevan Reddy, J. reaffirmed that Article 21 of the Constitution guarantees the right to life and liberty implicitly includes the right to privacy. The "right to be let alone" for every citizen of this nation to protect their privacy was also confirmed by the Court.

As a result, the issue of "data protection" is developed in a manner specific to the "right to privacy." In a similar manner, both concepts are covered by the Indian Constitution as a right.

## VI. DATA PROTECTION AND RIGHT TO INFORMATION ACT 2005

"The practical regime of right to information for citizens to secure information under the control of public authorities in order to promote transparency and accountability... for matters connected therewith or incidental thereto"[35] is the premise of Right to Information in India. This is the Act of 2005's preamble, and Section 2(j) discusses the definition of the "right to information."[36] Now, the question of whether the "data" that was kept by the public authority is safe or not arises. It is highly speculative whether the digital data specified in clause (iv) of Section 2(j) are being properly maintained.

The individual is entitled to the protection of their personal data under the terms of this Act. In the case of Bannett Coleman v. Union of India[37], the court ruled that "freedom of speech and expression includes within its compass the right of all citizens to read and be informed" and that "it is indisputable that by freedom of press meant the right of all citizens to speak, publish, and express their views." "The basic purpose of freedom of speech and expression is that all members should be able to form their beliefs and communicate them freely to others," the Court ruled in Indian Express Newspaper (Bombay) v. Union of India[38]. In conclusion, the fundamental idea at stake here is the right of the public to know.

As a result, the supreme court's decision is the only way to connect these two contexts. In a similar vein, the decision in PUCL v. Union of India[39] held that the right to information should be elevated to the level of a human right because it is essential for making government

[34] 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.
[35] AIR 1954 SCR 1077.
[36] (1994) 6 SCC 632
[37] (1994) 6 SCC 632.
[38] Ministry of Law & Justice (2005a), Accessed October 21, 2016, http://lawmin.nic.in/legis.htm
[39] "Right to Information" means 'the right to information accessible under this Act which is held by or under the control of any public authority and includes the right to: (i) Inspection of work, Documents, Records; (ii) Taking notes, Extracts or Certified copies of documents or records; (iii) Taking certified samples of material; (iv) Obtaining information in the form of Diskettes, Floppies, Tapes, Video cassettes or in any other electronic mode or through printouts where such information is stored in a computer or in any other device'.

 [ISSN 2581-5369]

transparent and accountable. Because the Supreme Court has consistently held that Article 19 of the Constitution guarantees the right to information, it stands to reason that the connection between these two contexts is closely related to the right base approach.

## VII. DATA PROTECTION AND RIGHT TO INFORMATION (AMENDMENT) ACT, 2008[40]

The "Information Technology Act" and "data protection" each have their own implication in relation to one another. The protection of online relationships is explicitly mentioned in Act's[41] objectives. It safeguards computer system data against a number of potential breaches. The aforementioned Act[42] contains provisions to prevent the illegal use of computer systems, data, and programs. The term "data protection" has been the subject of several new provisions. The Act's new sections 43A[43] and 72A[44] make it abundantly clear that data security is a priority.

The 2008 Amendment Act[45] is a significant step in the fight against the plethora of cybercrimes. The statutory data protection amendments made to Indian laws over the past decade finally met the demands of the United States and Europe. The service provider now faces jail time for breaking a contractual obligation by disclosing "personal information"52. Additionally, the disclosure of "sensitive personal information"53 entitles the offender to damages.

As a result, data protection has been given the same status as usual. The development of technology is the primary focus of the investigation into the EU Data Protection Act and the Indian Information Technology Amendment Act 200854. In light of the Information Technology Act 2008[46], it discusses corporate data exercise, such as excess, share, discloser, publication security measures, and penalties. The importance of the outsourcing industry in India and how this may affect the flow of business from European Union companies are two additional examples of provisions in the IT Rules 2011 that give the impression of right concern[47]. This article also discusses the Indian regulations regarding the protection of sensitive

[40] AIR 1973 SC 60.
[41] (1985)1 SCC 641.
[42] (2004) 2 SCC 476
[43] Information Technology (Amendment) Act 2008, Accessed October 21, 2016, http://www.cyberlawconsulting.com/itact2008amendments.pdf.
[44] Ibid.
[45] Ibid.
[46] Section 43A, It represents a radical change in the law which may have taken place due to the industry's contention that there was no adequate protection of data in India as compared to Europe and that this was adversely affecting outsourcing. Under this provision when a body corporate processing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls and operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby cause wrongful loss and wrong full gain to anybody corporate shall be liable to pay damages by way of compensation to the person so affected.
[47] "Section 72A. Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is

personal data and compares their provisions to those of the UK Data Protection Act 1998 at various points[48]. As a result, the primary right base approach is asserted to the individual right to data protection.

## VIII. DATA PROTECTION AND INDIAN PENAL CODE

The British era in India is where the Indian Penal Code got its start. In the 1860s, Lord Macaulay served as chairman and drafted the initial introductory draft. As a result, the connection between "data protection" and the "Indian Penal Code" provision does not fully satisfy all requirements. Data privacy violations are not specifically addressed by Indian criminal law. Liability for such breaches must be inferred from related crimes, according to the Indian Penal Code. For instance, dishonest misappropriation or conversion of "movable property"[49] for one's own use is subject to a criminal penalty under Section 403 of the Indian Penal Code. When it comes to the liability of the other, the question of who is entitled to protection arises. According to Sections 405 and 409, misappropriation of another person's property constitutes a criminal breach of trust. Another section, Section 378, states that no one may dishonestly remove any movable property from a person's possession without that person's consent. If a person does this, he is considered to have committed theft and will be punished, but electronic data protection legislation has not yet been enacted. There are two approaches to addressing a person's legal right in this situation. In fact, the crime is committed solely against the state. This raises serious questions about the state's authority to uphold order. Penalties are mentioned in the Penal Code, and in civil actions, damages laws, including the number of damages, must be decided by a jury[50]. The suggestion to mention this is extremely pertinent to addressing the appropriate issue. On addressing the right, the relationship between "data protection" and "Indian Penal Code" is appropriate. In this context, the state is also responsible for safeguarding individual data.

## IX. DATA PROTECTION AND NATIONAL SECURITY

The terms "data protection" and "national security" are extremely relevant in the world of today. When it comes to "data protection," national security and law enforcement agencies play a

likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.''

[48] Supra Note 46.

[49] 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.

[50] Under the Personal Data (protection) Bill 2013, Section 2 (x) "sensitive personal data"53 means personal data as to the data subject's – (i) Biometric data; (ii) Deoxyribonucleic acid data; (iii) Sexual preferences and practices; (iv) Medical history and health; (v) Political affiliation; (vi) Commission, or alleged commission, of any offence; (vii) [Ethnicity, religion, race or caste]; and (viii) [financial and credit information].

 [ISSN 2581-5369]

crucial role in every nation[51]. For instance, the story that another individual named Edward Snowden leaked information about the privacy of Americans surfaced in 2013[52]. This story raises the question of whether or not a person has any privacy at all. What kind of privacy will prevail if the data is made available to anyone in the public domain? According to their technological advancement, the developed nation would be the most powerful in this scenario, whereas the developing nation would be in a similar predicament.[53] National security has no bearing on this. The concept of proposing the appropriate base approach is of the utmost significance in nature in order to achieve parity with this circumstance.

Similar circumstances dictate that national security and law enforcement are frequently exempt from laws or that such access is permitted for widely accepted purposes. This proved to be the case in every nation, even in those with the strongest data protection laws. For instance, according to Dan Svantesson's writing, "taken together... provide Australian law enforcement and national security agencies with broad access to private-sector data." As a result, data collection and use for national security and law enforcement purposes frequently fall outside of the scope of oversight that applies to other data processing activities or are subject to much less transparent standards and oversight regimes[54]. To investigate the right-based approach, individuals must be protected against authority. That authority, like the police, can't track a cell phone unless it's in an emergency or a time-sensitive situation. Enforcement agencies now have access to every moment's snooping and every individual's geolocation thanks to cutting-edge technology. The issue is about the technology used by police to monitor citizens who use cell phones, which uses cellular location. In particular, the technology behind cell sites, the Global Positioning System, and Wi-Fi will be discussed in this commentary. Cell phone tracking is a widespread practice that may eventually replace federally regulated wiretapping to some extent[55]. The issue is that this encroachment is genuine for the purpose of national security to some extent, but the personal privacy-related issue also peeps into the door. This will demonstrate that legislation is required in this area.

According to the Supreme Court's argument in the case of District Registrar and Collector, Hyderabad v. Canara Bank[56], the search and seizure of any registers, books, records, papers, or other proceedings by the enforcement agency for the purpose of collecting evidence and

[51]Supra Note 46.
[52] Supra Note 46.
[53] Information Technology Rules 2011, Accessed February 20, 2015, http://www.ijlt.in/pdffiles/IT-(Reasonable%20Security%20Practices)-Rules2011.pdf.
[54] Raghunath Ananthapur, "India's New Data Protection Legislation", Volume 8, Issue 2, (2011).
[55] 'Movable p1roperty' has been defined as property which is not attached to anything and is not a land.
[56] Denis O'Brien, "The Right of Privacy," Columbia Law Review, Vol. 2, No. 7 (1902): 437-448.

 [ISSN 2581-5369]

discovering the fraud and omission of stamp duty payable or not of an individual fall under the infringement situation, and confidentiality must be maintained.

In order to combat the ever-increasing policies of cybercrime and cyber security[57], individual liberties like privacy and data protection are now considered an essential phenomenon. Human rights and the protection of data are on the same periphery. It involves data security and privacy in all countries. The philosophical debate over the dichotomy of "security vs. privacy," "interest vs. right," or "value vs. value" is based on the idea that some weighing rule must always be followed to balance one against the other. Data, Data Controller, Data Processer, Data Storage, and the proposed regulation are also presented here.[58]

## X. DATA PROTECTION AND INTELLECTUAL PROPERTY LAW

In relation to computer-related database work, the parity between "data protection" and "intellectual property law" must be examined using a right-based approach[59]. According to section 63B of the Indian Copyright Act, any person who knowingly makes use of an infringing copy of computer program on a computer shall be liable for infringement. The individual's intellectual property rights are based on "labor, skill, and judgment." The protection of the right of ownership of any literary, dramatic, musical, artistic, or cinematographic works that are recognized by law is essential. However, the Copyright Act[60] makes it difficult to distinguish between database protection and data protection.

Database protection serves a completely different purpose, namely to safeguard the creativity and investment made in the compilation, verification, and presentation of databases. Data protection aims to protect individuals' informational privacy.

Access, privacy, ownership, and evidence are universal legal concepts that apply to all relationships. However, these ideas can also be used to examine the rights and responsibilities of professional and business participants in recordkeeping. As right-duty things that demonstrate the legal relationship rather than as merely physical objects, records can be subject to property law. Examples of the various requirements that participants in recordkeeping have been access, intellectual rights, and obligations. In order to establish rights and responsibilities, identity information must be retained over time while privacy protection must be balanced.

[57] Law Enforcement, National Security, and Privacy, Accessed March 25, 2015, http://cis-india.org/internet-governance/blog/law-enforcement-nationalsecurity-privacy.pdf.
[58]The Hindu, Published in June 24, 2013,Accessed October 21, 2016, http://www.thehindu.com/news/international/world/edward-snowden-andthe-nsa-files-story-so-far/article4846529.ece?css=print.
[59] Daniel J. Solove & Paul M. Schwartz, "Privacy, Information and Technology," Wolter Kluwer Law & Business Publisher in New York, (2011), 79-256.
[60] Supra Note 27

 [ISSN 2581-5369]

Using the rights and obligations method assigns responsibility for the creation, documentation, and preservation of evidence to a variety of parties in a web of relationships, including the author and the recipient, data subjects, and third parties that are equally applicable to the online environment[61]. In a similar manner, "data protection" and "intellectual property right" are relevant terms for rights. It discusses four categories of privacy: information privacy, bodily privacy, communication privacy, and territorial privacy[62]. The core of the "right base approach" is the intellectual property right model, the moral right model, and the trade secrecy model. In order to generalize the idea of intellectual property, the author's right must be recognized as a legal right to control how personal data is used or disclosed. The author also mentioned "government" in this context. should accept property right-related solutions and take a flexible and responsive approach to protecting personal data.[63]

## XI. DATA PROTECTION AND CORPORATE AFFAIRS

The relationship between "data protection" and "corporate affairs" also forms the right base approach. The business is really affected in many different ways. The data's processing, access, disclosure, and sharing are crucial. The corporate sector has relied heavily on the custody of data processors or controllers. Occasionally, it is up to the private organization to decide whether or not to share. The conflict between the enforcement agency and the private and public organizations lies here. The online advertisement prompts users to submit information whenever they wish to access any information or place an order for any product. Now, the question of whether the data that was kept by the authority adheres to public policy or not arises following the submission of this information. In this context, in the banking industry, the banker is obligated not to disclose the information they possess, which would violate the client's confidentiality and secrecy obligation. Because it was incompatible with the right to information and public information[64], the scope of the banking customer's right to privacy was limited.

The Securities and Exchange Board of India Act of 1992[65] establishes the Securities and Exchange Board of India (SEBI) to govern and regulate the use of individual credit

[61] Stephen Wagner, Stopping Police in Their Tracks: Protecting Cellular Location Information Privacy In The Twenty-First Century, 12 Duke Law & Technology Review 200
[62] AIR 2005 SC 186
[63] VaishaliSharma,"YouHaveZeroPrivacy,Get OverIt:(DataProtectionLaw InIndia, Analyzed In A Comparative Framework)", Accessed October 21, 2016, http://thegiga.in/LinkClick.aspx?fileticket=4I_C-RPOQMg%3D&tabid=589
[64] Maria Grazia Porcedda"Data Protection and The Prevention Of Cybercrime: The Eu As An Area Of Security? European University Institute, Florence Department of Law," Accessed October 21, 2016, http://ssrn.com/abstract=2169340.
[65] Supra Note 10.

information.[66] According to the Act[67], the Security Exchange Board of India is granted broad access to private-sector data related to the securities market. SEBI can only conduct an inspection if it has good reason to believe that: The Act re-enforces reactive access to and disclosure of information by penalizing any person who fails to furnish the required information[68]. In another area of corporate affairs, the Credit Information Companies Regulation Act, 2005[69]("CICRA"), the credit information pertaining to individuals in India must be collected in accordance with privacy norms outlined in the CICRA regulation. If a company has been engaging in insider trading or fraudulent activity, unfair trading practices are being used, transactions in securities are being handled in a manner that is The data have been held accountable for any possible disclosure or alteration by those who collected and maintained them. The CICRA has established a stringent framework for information about a person or business's credit and finances in India, based on the Fair Credit Reporting Act and Graham Leach Bliley Act[70].

The Reserve Bank of India recently issued a notification regarding the CICRA Regulations, which establish stringent data privacy standards. Because of this, "data protection" and "corporate affairs" both follow the same path as the "right based approach".

## XII. DATA PROTECTION AND CONSUMER

The relationship that the company has with its customers is very important in articulating the "data protection" issue. The Calcutta High Court ruled in the case of Shakankarlal Agarrwalla v. State Bank of India[71] that a banker has a duty of secrecy. "It is implied term of the contract between a banker and his customer that the banker will not divulge to third person without the express and implied consent of the customer either the state of the customer's account, any of his transactions with the bank, or any information's relating to the customer acquired through the keeping of his account unless the banker is compelled to do so by order of a court or the circumstances give rise to a public duty of disclosure or the protection of the banker's own interest Therefore, the concept of establishing a relationship between the banker and customer

[66] THE COPYRIGHT(AMENDMENT)ACT,20l2, Accessed October 21, 2016 http://www.wipo.int/edocs/lexdocs/laws/en/in/in066en.pdf.

[67] Property, privacy, access and evidence as legal and social relationships, Accessed October 21, 2016, http://download.springer.com/static/pdf/977/chp%253A10.1007%252F1-4020-4714-2_5.pdf?auth66=1424433931_1c7e42dfa070decb666a36746471f322&ext=.pdf

[68] Available at, http://gilc.org/privacy/survey/intro.html (Accessed October 21, 2016).

[69] M M S Karki, "Personal Data Privacy & Intellectual Property,"Journal of Intellectual Property Rights, Vol 10. (2005): 59-63.

[70] Mr. K.J. Doraisamy v. The Assistant General Manager, State Bank of India and others, (2007) 136 Comp Cases 568 (Mad).

[71] SECURITIES AND EXCHANGE BOARD OF INDIA ACT 1992, Accessed October 21, 2016, http://www.sebi.gov.in/acts/act15ac.pdf

 [ISSN 2581-5369]

must be maintained.

In contrast, e-commerce poses a threat to data security and fuels an ever-increasing rate of misuse. The only problem is with how internet users' data is collected, stored, used, and accurate. The most concerning aspect of this is BPO fraud, which is covered by the IT Act's criminal provisions[72]. This phenomenon only arises from the relationship between the customer and the authority. This won't happen if the authority, or the service provider, has the right privacy policy in place. However, the unfavorable aspect is that the authorities have absolutely no concern for this kind of privacy policy. Additionally, the enforcement agencies are unaware of all rights violations. The well-equipped "right based approach" is the only way to address both the privacy issue and the data protection issue.

## XIII. CONCLUSION

Data protection has been viewed as a right from a variety of perspectives, as highlighted by the analysis of various themes. The acceptance of data protection as a right was emphasized in all subjects, including the right to privacy, the right to information, information technology, the Indian Penal Code, corporate affairs, and consumer. The issue aims to raise awareness of data protection as a fundamental human right in the age of technological liberalization. To keep up with the expanding scope of technology, it is necessary to strengthen the data protection system in order to safeguard individual liberty. The goal of this research is to make the right to privacy and data protection a fundamental right, and after conducting an analysis, to treat as right is justifiable. Individual liberty can only be protected from outside interference if the entire legal requirement of data protection is met. A standard approach to data protection can be provided by the institutional status of data protection. The elements of data protection—collection, processing, storage, security, and access—must collaborate in the legal framework to give data protection special status as a right. The correct foundational approach to data protection and privacy must be universally recognized.

*****

[72] Ibid.

 [ISSN 2581-5369]