PRIVACY AND ITS PROTECTION IN INFORMATIVE TECHNOLOGICAL COMPASS IN INDIA

*Sougata Talukdar**

Privacy as a concept is going through a metamorphosis in this era of technology. The discussion relating to privacy generally involves what it entails and how it is to be valued. Discourse on privacy as a right involves the extent to which it is or should be legally protected. However, nowadays, it is generally accepted that everybody has a need for privacy, although the way it is appreciated differs from culture to culture, and person to person. In the case of information technology, the concern for privacy is increasing day by day, as development in this field always brings misuse along with the betterment for human society. In India, privacy is an unenumerated fundamental right under the Constitution. The issue relating to privacy in the informational field is addressed by the Information Technology Act, 2000. However, even after that, a large number of disputes are coming to the fore. This article is primarily concerned with the concept of privacy, its recognition under the Constitution of India, and protection of informational privacy under the Information Technology Act, 2000.

Table of Contents

* Teacher in Charge and Assistant Professor, Sureswar Dutta Law College, Affiliated to University of Calcutta.

I. INTRODUCTION

Privacy is a "distinctly contemporary" concept.[1] Its violation always threatens the existence of a human being with social dignity. The rights based conceptualisation of privacy is widely acknowledged and well-supported across the world. Many familiar legal and ethical arguments have been developed on the concept of the right to privacy. Nowadays, however, the protection of privacy rights cannot be separated from developmental activities. With the development of science and technology, the potential to intrude into someone's privacy has increased tremendously. Every legal system has a duty to react to these changes by ensuring the legal protection tothe privacy of any individual, except in certain exceptional circumstances. Thus, information privacy law is a relatively nascent area of law. New developments are still shaping to conceptualise it with its wide range of possibilities and by considering the variations through which it is goingwith the change of time and social structure.[2] Due to issues relating to state surveillance, collection of data for government-sponsored programs, outsourcing, handling of data, including personal and financial information and press freedom, privacy issues have received attention in recent years.[3]

India is a signatory to the Universal Declaration on Human Rights and the International Convention on Civil and Political Rights. Both of these documents recognise privacy as a fundamental right.[4] However, India does not have any specific law or statute to guarantee the right to privacy to its citizens. In order to fill this lacuna, courts in India have tried to enforce a right to privacy in favour of its citizens through two main routes – firstly, by recognising a constitutional right to privacy, which has been read as part of the rights to life and personal liberty, and a common law right to privacy which is available under law of tort. In reality, the right to privacy is not a very strongly enforced right in India and there are a number of exceptions to the right to privacy which have been carved out by the Courts over a period of time. In the sphere of technology and communication relating to information, privacy has been secured through the Information Technology Act, 2000. Though this Act has already travelled a long way, it fails to secure privacy in the cyberspace in a strict fashion. The misuse of technology and invasion of the privacy of the individual are of major concern in this era. Thus, there is a requirement to understand the term 'privacy' and its protection under the Constitution. Along with that, there is a growing need to comprehend how far

---

1 Glenn Negley, *Philosophical Views on the Value of Privacy*, 31 Law and Contemporary Problems 319 (1966).

2 Daniel J. Solve & Paul M. Schwartz, An Overview of Privacy Law 39 (2015).

3 Sachin Chaturvedi, Krishna Ravi Srinivas & Vasantha Muthuswamy, *Biobanking and Privacy in India*, 44 Journal of Law, Med. and Ethics 45, 50 (2016).

4 *See also* Universal Declaration on Human Rights, G.A. Res. 217A, U.N. Doc. A/810 (December 12, 1948) Article 12; International Covenant on Civil and Political Rights, December 16, 1966, UN Doc. A/6316 (1966), Article 17.

privacy in the field of information technology is protected. This article is majorly concerned with these spheres of the law.

The article is divided into seven parts. In Part II, I discuss the concept of privacy and its legal and philosophical foundations. In Part III, I elaborate the application of right based approach to privacy and its impact on human rights jurisprudence. In Part IV, I deliberate upon the origin of the concept of privacy and its legal recognition in nineteenth and twentieth century. Further, in Part V, I have made an effort to elaborate the Constitutional validity of right to privacy in India by referring various judicial pronouncements from time to time. Finally, in Part VI, the protection of privacy and its extent has been discussed with reference to the various provisions of the Information Technology Act, 2000. Part VII includes some concluding remarks from the discussion.

II. PRIVACY AS A CONCEPT

Privacy as a concept is a volatile one and as a phenomenon, it is as old as the existence of mankind. Throughout history, it has been related to one's house, to one's family life, and to one's personal correspondence. As the concept itself includes a lot of dimensions, it is very hard to define the concept with crystal clear clarity.[5] Further, the volatile nature of privacy exists as it is very hard to put strict limitation to its ambit and its always perspective in nature with regard to other rights, such as right to know, right to cohabit *etc*.[6] The Black's Law Dictionary defines privacy as (i) the right to be let alone, (ii) the right of a person to be free from unwarranted publicity, and (iii) the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.[7] Thus, the nature, extent and scope of privacy depends upon the subject to which it is related. For example, the conception of privacy in the context of love, friendship, and trust depends on a complex account of these concepts, and they, in turn, depend on the more general notions of morality, respect, and personality.[8] The view of morality, upon which privacy rests, is one which recognises basic rights in persons, rights to which all are entitled equally, by virtue of their status as persons. All of these rights are subject to qualification only to ensure equal protection of

---

5 For understanding various attempts to define privacy see Griffin, *The Human Right to Privacy*, 44 San Diego Law Review 697 (2007); Solove, *A Taxonomy of Privacy*, 154 University Of Pennsylvania Law Review 477 (2006); Whitman, *The Two Western Concepts of Privacy: Dignity versus Liberty*, 113 Yale Law Journal1 153 (2004); Solove, *Conceptualizing Privacy*, 90 California Law Review 1087 (2002); Post, *Three Concepts of Privacy*, 89 Georgetown Law Journal 2087 (2001); Mindle, *Liberalism, Privacy and Autonomy*, 51 Journal Of Politics 575 (1989); M.R. Konvitz, *Privacy and the Law: A Philosophical Prelude*, 31(2) Law And Contemporary Problems 272 (1966).

6 *See* Myriam Dunn Cavelty & Matthias Leese, *Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity*, 5(3) European Review Of International Studies 49, 62 (2018).

7 *See also* Black's Law Dictionary 1358 (4th ed., 1988).

8 Charles Fried, *Privacy,* 77(3) Yale Law Journal 475, 478 (1968); *See also* W.A. Parent, *A New Definition of Privacy for the Law,* 2(3) Law and Philosophy 305 (1983) (for understanding the difficulty in defining 'privacy').

the same rights in the sphere of other's rights. Therefore, the concept of privacy is a widely accepted legal and moral notion. However, it's legal and philosophical foundations are uncertain as various people chosen different way to describe its core concept.[9] Many scholars have argued for privacy on the basis of relativity aspects. Many scholars have found that privacy as a right cannot stand alone, and is dependent on the violation of some other interestsuch as right to know, access to public information, *etc*.[10] As per them, privacy can be demonstrate as an opposite phenomena of right to know and right to information.[11] However, in the early days, independent discussions on privacy demonstrated privacy either as indications of hypersensitivity,[12] or an unjustified wish to manipulate and defraud.[13] Among the reviewers engaging in such discussions, Professor Richard A. Posner's version could be termed asthe most extreme one. He denied the utility of all 'intermediate' values, and assessed Acts and Rules by the single, ultimate principle of wealth maximisation.[14] However, although these reviewers disagree on many points, they were united in denying the utility of thinking and talking about privacy as a legal right. From the early sociological point of view, Barrington Moore defined privacy as something that cannot be the dominant value in any society. Man has to live in society, and social concerns have to take precedence.[15] Thus, there cannot be any static philosophy to define the concept of privacy. It changes with time, society and need of the hour.

However, what is considered to be private differs according to the era, the social structure, and the norms individuals follow. Moreover, what is considered to be private and what is legally protected as private can also differ. In the broad sense, with regard to the concept of privacy, there are two dimensions, a relational one and an informational one. The first deals with the relationship one has with other people, for example, determining who may enter the domestic environment or who is allowed to touch one's body.[16] These aspects sometimes are described as territorial privacy and bodily privacy. The informational dimension is related to the collection, storing, processing, and disclosing of personal

---

9 *See also* James H. Moor, *The Ethics of Privacy Protection*, Library Trends 69 (1990).

10 *See also* Philip Leith, *The Socio-legal Context of Privacy*, 2(2) International Journal of Law in Context 105, 128 (2006) (for understanding the relative discussion on privacy); Raymond Wacks, Law, Morality and The Private Domain (2000); David J. Garrow, Liberty and Sexuality: The Right to Privacy and the Making of Roe v. Wade (1998); William L. Prosser, *Privacy*, 48 California Law Review 383 (1960); Frederick Davis, *What Do We Mean by "Right to Privacy"?*, 4 South Dakota Law Review 1 (1959).

11 See for discussion, Fred H. Cate, D. Annette Fields, & James K. McBain, *The Right to Privacy and the Public's Right to Know: The "Central Purpose" of the Freedom of Information Act*, 46 Administrative Law Review 41 (1994).

12 Harry Kalven, *Privacy in Tort Law-Were Warren and Brandeis Wrong?*, 31 Law and Contemporary Problems 326, 329 (1966).

13 Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 Buffalo Law Review 1 (1979); Epstein, *Privacy, Property Rights, and Misrepresentations*, 12(3) Georgia Law Review 455 (1978).

14 Richard A. Posner, *The Right to Privacy*, 12(3) Georgia Law Review 393, 394 (1978).

15 Barrington Moore, Privacy: Studies in Social and Cultural History 274 (1984).

16 Jan Holvast, *History of Privacy*, in The Future of Identity in the Information Society 13, 16 (2008).

data. Apart from these two dimensions, other questions related to the privacy in the legal periphery can be raised with regard to its control and access, which is very much clear from the arguments of Professor Ruth Gavison. In a broader way, sheraised two types of questions in the process of describing privacy. The first one relates to the status of the term: Is privacy a situation, a right, a claim, a form of control, or a value? The second question is one related to the characteristics of privacy: Is it related to information, autonomy, personal identity, or to physical access?[17] Professor Gavison argued that in the context of legal protection, privacy should indicate certain values such as dignity, autonomy or personhood. The coherence and usefulness of privacy as a value is due to a similarity one finds in the reasons advanced for its protection,[18] a similarity that enables us to draw principles of liability for invasions.[19] The question related to physical access to an individual as a characteristic of privacy is always a concern for the conceptualisation of privacy. Usually, individuals lose privacy when others gain physical access to them. Physical access here means physical proximity – that A is close enough to touch or observe B through normal use of his senses. Observance ofan individual can also be done from a distance. But the physical sense of A allows him to know when B has physical access to him than when B observes him. The following situations will clearly elaborate when physical access can cause loss of privacy: (a) a stranger who gains entrance to awoman's home on false pretences in order to watch her giving birth; (b) Peeping Toms; (c) a stranger who chooses to sit on "our" bench,even though the park is full of empty benches; and (d) a move from asingle-person office to a much larger one that must be shared with a colleague *etc*.[20] In each of these cases, the spirit of the complaint is notthat more information about him has been acquired, nor that more attention has been drawn to him, but that his spatial aloneness has been diminished.[21] Therefore, the discussion relating to the physical access of privacy is surrounded by the facets of loss of privacy. The essence of the complaint is not that more information about one has been acquired, nor that more attention has been drawn to one's privacy, but it is more concerned with diminution of spatial aloneness. Thus, Alan F. Westin rightly stated that privacy is nothing but 'the claim of an individual to determine what information about himself or herself should be known to others'.[22] Hence, it is a negative concept with an expectation that something should not be done which affects one's intimate sphere.[23]

---

17 *See also* Ruth Gavison, *Privacy and the Limits of Law*, 89(3) Yale Law Journal 421, 424 (1980).

18 Generally, privacy is required to be protected to put a limit on the power of interference, to build and secure respect for individuals, to maintain appropriate social boundaries, to keep trust, and to reduce the power to control one's life. For discussion, *see* Will Thomas De Vries, *Protecting Privacy in the Digital Age*, 18 Berkeley Technology Law Journal 283 (2003).

19 Gavison, *supra* note 17, 425.

20 *Id*., 433.

21 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4(5) Harvard Law Review 193 (1890); For understanding spacing and its importance *see* Edward T. Hall, The Hidden Dimension 41 (1966).

22 Alan F. Westin, *Privacy and Freedom*, 25 Washington And Lee Law Review 166 (1968).

23 Giovanni Buttarelli, *Privacy Matters: Updating Human Rights for the Digital Society*, 17(4) Health And Technology 325, 326 (2017).

On the same line, the U.S. Supreme Court in *Griswold* v. *Connecticut*,[24] stated that a ban on using contraception is contrary to the 'right to marital privacy', in effect, the right of couples to be 'left alone' by the State in the privacy of their bedrooms.

In the twenty-first century, there is a clear shift of thinking regarding the concept of privacy. Scholars have tried to expand the scope of privacy by adding the right based approach to it. Professor Robert C. Post described privacy by attaching it (i) to the creation of knowledge, (ii) to dignity, and (iii) to freedom.[25] Regarding the creation of knowledge, privacy is always the opposite phenomena to it. Under the general terms, knowledge has a cordial relation with the information and information always has a tendency to flow against the privacy requirement of an individual. Interruption to the flow of information is the sole way to short circuit the formation of knowledge. Therefore, privacy should not set up an opposition between information and "true knowledge". True knowledge of other people, in all their complexity, can be achieved with only a handful of intimate persons or family members. To flourish, the intimate relationships on which true knowledge of others depends need time and private space, thus, in other words, it requires sanctuary from the gaze of the crowd, where mutual self-disclosure is possible. Thus, privacy more or less can be demonstrated as a pre-condition for the formation of true knowledge rather as an opposition to form true knowledge.[26] Moreover, privacy should not stand in the path of the general knowledge-building procedure. Privacy prevents the disclosure of the specific kind of information that cannot be adequately understood in the absence of special circumstances, like intimacy.[27]

More fully, the social aspect of privacy depends upon its relationship with the dignity of an individual and its protection under a given society. Thus, the description of privacy with regard to dignity always puts it in the ground of social forms of respect that we owe each other as members of a common community. Thus, it presupposes a particular kind of social structure in which persons are joined by common norms that govern the forms of their social interactions. These norms constitute the decencies of civilisation.[28] Thus, privacy stands on the point of balance between the social information and social information causing harm to the dignity of the individual. Further, privacy as freedom contemplates a space in which social norms are suspended, rather than enforced. Hence, in a negative way, an invasion of private life would emasculate individual freedom and independence. It portrays individuals as autonomous and self-defining, rather than as socially embedded and tied together through common socialisation into shared norms. In other words, privacy is about creating distance between oneself and society, about

---

[24] Griswold v. Connecticut, 381 U.S. 479 (1965).

[25] Robert C. Post, *Three Concepts of Privacy*, 89 Georgetown Law Journal 2087 (2000).

[26] Jeffrey Rosen, *Why Privacy Matters*, Wilson Quarterly 32, 34 (2000).

[27] *See also* Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America (2000) (for understanding the importance of privacy in the light of knowledge building).

[28] Post, *supra* note 25, 2093.

being left alone, which is the basic proponent of defining privacy as freedom from society. However, privacy as dignity seeks to eliminate differences by bringing all persons within the bounds of a single normalised community, whereas privacy as freedom protects individual autonomy by nullifying the reach of that community.[29] Hence under the conceptualisation of privacy as dignity, there is always an effort to define it in terms of protecting elemental community norms concerning, for example, intimate relationships or public reputation *etc*.[30]

III. THE RIGHT TO PRIVACY: A SUMMARY

The concept of the right to privacy is a much more modern concept than that of the privacy itself. In *Olmstead* v. *United States*,[31] Justice Louise Brandeis categorically argued that the right to privacy is the right most valued by civilised men. In similar terms, Winfield has denoted the right to privacy as the absence of unauthorised interference with a person's seclusion of himself or his property from the public. This definition on the basis of unauthorised interference also manifests the legal appreciation of the individual personality.[32] Given the importance laid on the role of privacy in moral and legal argumentation, one might expect that assertions on the right to privacy are emblazoned in a prominent position in the earliest philosophical and legal documents of any nation or international arena. Under the modern legal structure, privacy is a combination of an individual's psychological needs and the individual's fundamental right. However, in India, the right to privacy is not explicitly mentioned or clearly discussed under any specific legal statute.The judiciary has played a pivotal role in this respect.[33] In conformity with the international protocols, under the constitutional framework, the right to privacy is recognised as a fundamental right and its protection is mandatory in India. It is noteworthy that like all other fundamental rights, the right to privacy is also not an absolute right. Thus, under exceptional situations, the appropriate authority has the power to give overriding effect to public concern upon privacy of the individual.By upholding the present situation in *Bhabani Prasad Jena* v. *Convenor Secretary, Orissa State Commission for Women*,[34] the Supreme Court held that when there is an apparent clear cut conflict between the right to privacy of a person to not submit themselves to forcible medical examination, and a duty of the Court to reach the truth on the basis of that medical examination, the Court must exercise its discretion only after balancing the interests of the parties.

---

29 *Id*., 2096.

30 Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14(3) Human Rights Law Review 441, 442 (2014).

31 Olmstead v. United States, 277 US 438 (1928).

32 P. Ishwara Bhat, Fundamental Rights – A Study of Their Interrelationship 324 (2004).

33 *See also* A.M. Bhattacharjee, Equality, Liberty and Property under the Constitution of India 104, 105 (1997) (for discussion).

34 Bhabani Prasad Jena v. Orissa State Commission for Women, (2010) 8 SCC 633: : AIR 2010 SC 2851. *See also* Thalappalam Service CooperativeCoop. Bank Ltd. v. State of Kerala, (2013) 16 SCC 82 : (2014) 1 Comp LJ 319 Not Found.

There must be due consideration of what is just for arriving at a just decision in the matter at hand.

IV. THE ORIGIN OF PRIVACY

Privacy as a concept is not new. It got its recognition in the Ancient Ages. The Greek philosopher Aristotle spoke about the division between the public sphere of political affairs '*the polis'* and the personal sphere of human life '*the oikos*'. This dichotomy provided an early recognition of 'a confidential zone'for the citizenand also provided a basis to restrict governmental activities within the public realm.[35] In India, privacy is also an age old phenomenon. From the age of the Mahabharata, we can see that privacy was noted in literature. Among the Pandu Brothers, there was a rule that when any of them were to spend time with Draupadi, their wife, the others will not enter the room during that period. Thus, privacy among the family is a known culture. However, the Holy Bible already contained some passages where the violation of privacy appeared in its early form, where shame and anger followed the intrusion into someone's private sphere. The ancient Code of Hammurabi also contained a paragraph against intrusion into someone's home to preserve the privacy of that person, and Roman law also regulated the same question with specific attention.[36] Thus, once a civilisation has made a distinction between the "outer" and the "inner" man, between the life of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between rights inherent and inalienable and rights that are in the power of government to give and take away, between solitude and society, between private and public, it becomes impossible to avoid the idea of privacy.[37] However, during the ancient period and medieval age, there was very little recognition of privacy as a right.

Under the modern legal system, the notion of privacy first appeared in the famous study by the name 'The Right to Privacy' written by two famous advocates of America Louis Brandeis and Samuel Warren in 1890. In this study, the authors conceptualised the term "right to privacy" as "the right to be let alone". Since then, the idea of the right to privacy has been identified as a basic right and acknowledged widely, and through evolution, it becomes a fundamental human right in every society.[38]For instance, privacy is a fundamental human right recognised in the UN Declaration of Human Rights,[39] the International Covenant on

---

[35] Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29(2) Connecticut Journal of International Law 257, 261 (2014).

[36] D.J. Solove, Nothing to Hide: The False Trade-Off Between Privacy and Security 4 (2011) ('Solove').

[37] *Id*., 273.

[38] *See also* Adrienn Lukacs, *What is Privacy? The History and Definition of Privacy*, available at http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (Last visited on January 2, 2019).

[39] *See* Universal Declaration on Human Rights, G.A. Res. 217A, U.N. Doc. A/810 (December 12, 1948), Article 12 ("No one shall be subjected to arbitrary interference with his privacy, family,

Civil and Political Rights[40] and in many other international and regional treaties.[41] However, since the end of the nineteenth century, the emphasis shifted to personal information, with an emphasis on the ability to control one's own information.

During 1967, another new milestone was reached with regards to the recognition of privacy as a right. Alan Westinin his article 'Privacy and Freedom' defined privacy in terms of self-determination. He said, "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[42] This tendency to define privacy in the light of self-determination is a common phenomenon of the twentieth century. Many authors preferred to define privacy through a comparative study with freedom and control.[43] They defined privacy as a right to be left alone and a right of each individual to determine, under ordinary circumstances, what his or her thoughts, sentiments, and emotions shall be when in communication with others. Recently, in *Zulfiqar Ahman Khan* v. *Quintillion Business Media Pvt. Ltd.*,[44] the Delhi High Court on similar terms held that the 'right to be forgotten' and the 'right to be left alone' are inherent aspects of the right to privacy. However, with the development of technology and its assimilation with information, privacy becomes an ever growing concern for our society.

---

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.")

40 *See* International Covenant on Civil and Political Rights, December 16, 1966, UN Doc. A/6316 (1966), 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 or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.)

41 For discussion under treaties see International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, July 1, 2003, UN Doc. A/45/49 (1990), Article 14; Convention on the Rights of the Child, September 2, 1990, 1577 U.N.T.S. 3, Article 16; African Charter on the Rights and Welfare of the Child, November 29, 1999, CAB/LEG/24.9/49 (1990), Article 10; Declaration of Principles on Freedom of Expression in Africa, Article IV, (the right of access to information); American Convention on Human Rights, July 18, 1978, 1144 U.N.T.S. 123, Article 11; Article 5 of the American Declaration of the Rights and Duties of Man, May 2, 1948, 43 A.J.I.L. Supp. 133 (1949), Article 5; September 15, 1994, Article 16 & 21; ASEAN Human Rights Declaration, November 18, 2012, Article 21; European Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, ETS 5, Article 8.

42 *See also* Jan Holvast, *History of Privacy* in The Future of Identity in the Information Society 13 (2008). *See also* A. F. Westin, Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part I The Current Impact of Surveillance on Privacy, Disclosure, and Surveillance, 66 Columbia Law Review 1003 (1966); A. F. Westin, Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II - Balancing the Conflicting demands of Privacy, Disclosure, and Surveillance, 66 Columbia Law Review 1205 (1966).

43 *See also* H. Kalven Jr., *The Problem of Privacy in the Year 2000*, 93 Daedalus 876 (1967); S. M. Jourard, *Some Psychological Aspects of Privacy*, 31 Law and Contemporary Problems 307 (1966); M. R. Konvitz, *Privacy and the Law: A Philosophical Prelude*, 31 Law and Contemporary Problems 272 (1966); A. Bates, *Privacy - A Useful Concept?*, 42 Social Forces 429 (1964).

44 Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd., 2019 SCC OnLine Del 8494 : (2019) 175 DRJ 660.

V. CONSTITUTIONAL PROTECTION TO PRIVACY IN INDIA

Constitutional protection to any right is the basis of validating that right under the Indian legal scenario. The case of the right to privacy is of no difference. However, the right to privacy as an independent and distinctive concept originated from the field of Law of Tort. Under Tort, a cause of action for damages resulting from an unlawful invasion of privacy was recognised. In recent timesthis right has acquired a constitutional status. The Supreme Court of India has, in a number of decisions recognised the right to privacy as a subset of the larger right to life and personal liberty under Article 21 of the Constitution of India.[45] Article 21 states, "no person shall be deprived of his life or personal liberty except according to the procedure established by law". The Supreme Court of India has asserted that Article 21 of the Indian Constitution is the core of Fundamental Rights. The extension of the scope and ambit of Article 21 has been made possible by elaborating the words 'life' and 'liberty'. The scope of this right came up for consideration in *M.P. Sharma* v. *Satish Chandra* ('M. P. Sharma').,[46]and *Kharak Singh* v. *State of U.P.*('Kharak Singh').[47] In both these cases, the Apex Court observed that the Constitution of India does not specifically protect the right to privacy. Thus, in early days privacy was not considered as a Fundamental Right protected under Part III of the Constitution. In M.P. Sharma,[48] the Supreme Court observed that:

> "Power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law.When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction."

Further, it is interesting to note that in the Kharak Singh,[49] Rajagopala Ayyangar, J. and K. Subba Rao, J., differed in their opinions with regard to the constitutional validity of the right to privacy. Rajagopala Ayyangar, J. held that "the right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movements of an individual which is merely a

---

45 *See also* Rahmath Nisha v. Director General of Prison, 2019 SCC OnLine Mad 1693 : (2019) 3 Mad LJ (Cri) 1; Ramlila Maidan Incident , In re, (2012) 5 SCC 1; Bhavesh Jayanti Lakhani v. State of Maharashtra, (2009) 9 SCC 551; Sudhansu Sekhar Sahoo v. State of Orissa, (2002) 10 SCC 743 : AIR 2003 SC 2136; PUCL v. Union of India, (1997) 1 SCC 301 : AIR 1997 SC 568; R. Rajagopal v. State of T.N., (1994) 6 SCC 632 : AIR 1995 SC 264; Gobind v. State of M.P., (1975) 2 SCC 148 : AIR 1975 SC 1378.

46 M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 : 1954 SCR 1077.

47 Kharak Singh v. State of U.P., AIR 1963 SC 1295.

48 *See also* M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 : 1954 SCR 1077.

49 *See also* Kharak Singh v. State of U.P., AIR 1963 SC 1295.

manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III." Whereas K. Subba Rao, J. categorically supported the fundamentality of right to privacy and held that "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty." In the process of upholding privacy as a Fundamental Right, K. Subba Rao, J. cited the famous observation of Justice Frankfurter of the American Supreme Court in *Wolf* v. *Colorado*,[50] and quoted "Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his 'castle': it is his rampart against encroachment on his personal liberty."

The right to privacy was again considered by the Supreme Court in 1975 while deciding the case of *Gobind* v. *State of M.P.* ('Gobind'),[51]which laid down that "a number of fundamental rights of citizens can be described as contributing to the right to privacy." However, the Supreme Court also stated that the right to privacy would have to go through a process of case-by-case development and observed that:

> "Any right to privacy must encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation, and child rearing. This catalogue approach to the question is obviously not as instructive as it does not give analytical picture of those distinctive characteristics of the right of privacy. Perhaps, the only suggestion that can be offered as unifying principle underlying the concept has been the assertion that a claimed right must be a fundamental right implicit in the concept of ordered liberty."

In this regard, it is interesting to note that the Supreme Court considered the application of Article 21 in the case of actions of private persons in *Shrimathi Vidya Verma* v. *Shiv Narain Verma*.[52] The Court observed that Article 21 is not enforceable against private persons. Therefore, even if it is assumed that the right to privacy existed under Article 21, it is not enforceable against private persons. Hence, the only remedy available in cases of invasions of privacy by private persons is a tort action for damages.[53] In *Malak Singh* v. *State of P&H*,[54]

---

50 Wolf v. Colorado, (1949) 338 U.S. 25.

51 Gobind v. State of M.P., (1975) 2 SCC 148 : AIR 1975 SC 1378 (In this case, Mathew, J., Krishna Iyer, J., and Goswami, J., traced the origins of right to privacy and also pointed out how the said right has been dealt with by the United States Supreme Court in two of its well-known decisions – Griswold v. Connecticut [1965] 385 U.S. 479 and Roe v. Wade [1973] 410 U.S. 113).

52 Vidya Verma v. Shiv Narain Verma, AIR 1956 SC 108.

53 Sandeep Challa, *The Fundamental Right to Privacy: A Case-by-Case Development Sans Stare Decisis*, 1(1) Indian Journal of Constitutional Law 224, 229 (2007).

54 Malak Singh v. State of P&H, (1981) 1 SCC 420 : AIR 1981 SC 760. *See also* LIC Life Insurance CorporaLIC tion of India and Union of India v. Prof. Manubhai D. Shah, (1992) 3 SCC 637 : AIR

the Supreme Court indirectly addressed the issue relating to privacy. It was held that an encroachment on privacy infringes personal liberty under Article 21, and the right to the freedom of movement under Article 19(1)(d). Without specifically holding that privacy is a protected constitutional value under Article 19 or Article 21, the judgment indicated that serious encroachments on privacy impinge upon personal liberty and the freedom of movement.

The jurisprudential distinction between a right as emanating from a named right or right mentioned in the text of the Constitution, and a right or right not mentioned in the text of the Constitution as a facet of a named right is highlighted in the opinion expressed by Bhagwati, J. in the Maneka Gandhi case.[55] Bhagwati, J. held that it was not enough that a right merely flowed from or emanated from a named right. For an unnamed right to be a part of the named right, it must be "integral to the named right or must partake of the same basic nature or character of the named right." So, as the right to privacy does not exist as a named right under the constitutional framework, in order for it to become a part of the named right to "personal liberty", ithas to be shown that theabovementioned unnamed right is integral to one's personal liberty or is "partaking of the same basic character" as personal liberty.[56] Thus, in 1994 for the first time the Supreme Court in *R. Rajagopal* v. *State of T.N.* ('Rajagopal'),[57] directly linked the right to privacy to Article 21 of the Constitution and held that:

> "The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing, and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned."

Again in 1997, the Supreme Court in *PUCL* v. *Union of India* ('PUCL'),[58] observed that telephone tapping would be a serious invasion of an individual's privacy. The Apex Court further held that the right to privacy is a part of the right to 'life' and 'personal liberty' enshrined under Article 21. Once the facts in a given case constitute the frame of right to privacy, Article 21 is attracted.That

1993 SC 171; State of Maharashtra v. Madhukar Narayan Mardikar, (1991) 1 SCC 57 : AIR 1991 SC 207.

55 Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

56 Namit Obero, *The Right to Privacy: Tracing the Judicial Approach Following the Kharak Singh Case*, 1(1) Indian Journal of Constitutional Law 216, 221 (2007).

57 R. Rajagopal v. State of T.N., (1994) 6 SCC 632 : AIR 1995 SC 264.

58 PUCL v. Union of India, (1997) 1 SCC 301: AIR 1997 SC 568.

right cannot be curtailed except according to the procedure established by law.[59]By explaining the position of the right to privacy, the Apex Court observed that:

> "The right to privacy-by itself-has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as 'right to privacy'".

Thereafter in *'X'* v. *Hospital 'Z'*,[60] the Supreme Court called out the provisions of Article 21 and other provisions of the Constitution relating to the Fundamental Rights read with the Directive Principles of State Policy in defining the right to privacy. The Court observed that sometimes disclosure of even true private facts has the tendency to disturb a person's tranquillity. It may generate many complexes and may even lead to psychological problems. Thus, the right to privacy is an essential component of the right to life envisaged by Article 21.This rightis not absolute, and may be lawfully restricted for the prevention of crime and disorder, protection of health, morals, and protection of rights and freedom of others.

Further, in *Distt. Registrar and Collector* v. *Canara Bank* ('Canara Bank'),[61] the Supreme Court, at time of declaring certain provisions of the A.P. Stamps Act as unconstitutional, observed that the concept of privacy is solely related to the citizen and not the place. The implication of such a statement was that it did not matter that the financial records were stored in a citizen's home, or in a bank, or in some other place. Irrespective of the place of keeping records, personal records should be protected under the citizen's right to privacy. Further, by citing Canara Bank, in *Directorate of Revenue* v. *Mohd. Nisar Holia*,[62] the Supreme Court held that the right to privacy is crucial and imposes a requirement of a written recording of reasons before a search and seizure could be carried out. Even the issue relating to the choice of food has been upheld as one's personal affair and as a part of his right to privacy which is included in Article 21 of our Constitution.[63]

---

[59] The State is entitled to impose restrictions on the basis of social, moral and compelling public interest in accordance with law. Sometimes Article 19 also acts as a limiting factor to the right to privacy. Thus, under the Indian scenario following can be considered as a limiting factor to the right to privacy: (i) other fundamental rights,(ii) legitimate national security interest, (iii) public interest include scientific, historical or statistical purposes, (iv) criminal offences, (v) anonymised data, and (vi) taxes.

[60] 'X' v. Hospital 'Z' , (1998) 8 SCC 296 : AIR 1999 SC 495.

[61] Distt. Registrar and Collector v. Canara Bank, (2005) 1 SCC 496. *See also* P.R. Metrani v. CIT, (2007) 1 SCC 786 : AIR 2007 SC 386.

[62] Directorate of Revenue v. Mohd. Nisar Holia, (2008) 2 SCC 370.

[63] *See also* Hinsa Virodhak Sangh v. Mirzapur Moti Kuresh Jamat, (2008) 5 SCC 33 : AIR 2008 SC 1892.

Likewise, a woman's right to make reproductive choices is also recognised as a dimension of personal liberty under Article 21 of the Constitution of India. In the process of doing so, the Supreme Court upheld that a woman's right to privacy, dignity and bodily integrity should be respected.[64] Again in *Selvi* v. *State of Karnataka* ('Selvi'),[65] the Supreme Court observed that "an involuntary subjection of a person to narcoanalysis, polygraph examination, and BEAP tests violates the right to privacy."Thus, in the twenty-first century, the concept of the right to privacy has evolved from negative recognition to its positive attribute within the Indian legal framework.

In *Amar Singh* v. *Union of India*,[66] the Supreme Court dealt with a petition under Article 32 alleging that the Fundamental Right to privacy of the petitioner was breached, by intercepting his conversations on telephone services provided by a service provider. Considering the importance of privacy, the Court was of the opinion that the service provider has to act as a responsible agency, and cannot act on any communicationwith regard to tapping of calls. Here communication means any direction from any influential person, private company or any communication which is not made under the governmental official capacity. Only on the basis of governmental official communicationtelephonic conversations can beintercepted. Moreover, there isalways a requirement to maintain sanctity and regularity in official communication, especially when the service provider is taking the serious step of intercepting the telephone conversation of a person. Further, in *Ram Jethmalani* v. *Union of India*,[67] the Supreme Court held that the right to privacy is an integral part of the right to life. The right to privacy is a cherished constitutional value, and every human being should be allowed forms of freedom which are free of public scrutiny, unless they act in an unlawful manner or violate the limit of that right. The Court further observed that, "The notion of fundamental rights, such as a right to privacy as part of right to life, is not merely that the State is enjoined from derogating from them. It also includes the responsibility of the State to uphold them against the actions of others in the society."

Moreover, discussing the importance of right to privacy as an opposite phenomenon of disclosure of information in public interest, the Supreme Court in *Bihar Public Service Commission* v. *Saiyed Hussain Abbas Rizwi*,[68] held that the public interest has to be understood by keeping in mind the balance between the

---

64 *See also* XYZ v. Union of India, 2019 SCC OnLine Bom 560 : (2019) 3 Bom CR 400; Suchita Srivastava v. Chandigarh Admn., (2009) 9 SCC 1 : AIR 2010 SC 235.

65 Selvi v. State of Karnataka, (2010) 7 SCC 263 : AIR 2010 SC 1974.

66 Amar Singh v. Union of India, (2011) 7 SCC 69.

67 Ram Jethmalani v. Union of India, (2011) 8 SCC 1. *See also* Sanjoy Narayan v. High Court of Allahabad, (2011) 13 SCC 155 : (2012) 1 RCR (Civil) 525 NOT FOUND (in this case, the Supreme Court observed that the role of the media is to provide to the readers and the public in general with information and views tested and found as true and correct. This power must be carefully regulated and must reconcile with a person's fundamental right to privacy).

68 Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi, (2012) 13 SCC 61 : (2013) 1 MLJ 747.

right to privacy and right to information. This must be done keeping in mind the purpose sought to be achieved and the purpose that would be served in the larger public interest, particularly as both these rights emerge from the values under the Constitution. Thereafter, the Supreme Court in *National Legal Services Authority* v. *Union of India* ('NALSA'),[69] interpreted Article 21 as the heart and soul of the Constitution of India, which speaks of the rights to life and personal liberty. Right to life is the most basic Fundamental Right, and not even the State has the authority to violate or take away that right. Article 21 includes all the relevant aspects of life which go to make a person's life meaningful and thus, protects the dignity of human life, one's personal autonomy, one's right to privacy. The right to dignity has been recognised to be an essential part of the right to life and must be extended to all persons on account of being humans.Thus, NALSA indicates the rationale for the grounding the right to privacy in the protection of gender identity within the ambit of Article 15. The intersection between Article 15 and Article 21 detectsthe constitutional right to privacy as an expression of individual autonomy, identity, and dignity. The judgment in NALSA indicates that the right to privacy does not necessarily have to fall within the ambit of any one provision in the chapter on Fundamental Rights. Intersecting rights recognise the right to privacy. Though primarily, it is in the guarantee of life and personal liberty under Article 21 that a constitutional right to privacy exists, it is also enriched by the values incorporated in other rights which are enumerated in Part III of the Constitution.

Thereafter in *ABC* v. *State (NCT of Delhi)*,[70] the Supreme Court dealt with the question of whether it is imperative for an unwed mother to specifically notify the putative father of the child of her petition for appointment as guardian of her child. The woman contended that if she is compelled to disclose the name and particulars of the father of her child, her own Fundamental Right to privacy will be violated. Looking into the interest of the child, the Court directed that,

> "if a single parent/unwed mother applies for the issuance of a birth certificate for a child born from her womb, the Authorities concerned may only require her to furnish an affidavit to this effect, and must thereupon issue the birth certificate, unless there is a Court direction to the contrary."

Further, by emphasising on the balance between the right to know and the right to privacy the Supreme Court in *Supreme Court Advocates-on-Record Assn*. v. *Union of India*,[71] observed that the balance between transparency and confidentiality is very delicate. However, the right to know is not anexplicit-fundamental right but at best is an implicit fundamental right, and it is hedged in with the implicit fundamental right to privacy that all people enjoy.

---

[69] National Legal Services Authority NLSA v. Union of India, (2014) 5 SCC 438 : AIR 2014 SC 1863.
[70] ABC v. State (NCT of Delhi), (2015) 10 SCC 1 : AIR 2015 SC 2569.
[71] Supreme Court Advocates-on-Record Assn. v. Union of India, (2016) 5 SCC 1.

Thus, the concept of the right to privacy has progressed drastically and got its recognition under the constitutional framework. The content of the constitutional right to privacy and its limitations has proceeded on a case to case basis, each precedent seeking to build upon and follow the previous formulations. However, it is clear that the doctrinal foundation essentially rests upon the trilogy of M.P. Sharma, Kharak Singh and Govind, upon which subsequent decisions including those in Rajagopal, PUCL, Canara Bank, Selvi, and NALSA, *etc.* have contributed.Famously, in 2017, the Supreme Court in *K.S. Puttaswamy* v. *Union of India*,[72] after considering the origin of privacy, growth of privacy as a right, privacy concerns against the State, inalienable nature of the right to privacy, privacy as a part of human dignity, upheld that right of privacy is a fundamental right. It is a right that protects the inner sphere of the individual from interference from both the State and the non-State actors and also allows the individuals to make autonomous life choices. The Court further observed that right to privacy is not an absolute right, but it is subject to the various restrictions such as: (i) other Fundamental Rights, (ii) legitimate national security interest, (iii) public interest including scientific or historical research purposes or statistical purposes, (iv) criminal offences, (v) the information does not relate to an identified or identifiable natural person but remains anonymous, and (vi) the regulatory framework of tax and working of financial institutions, markets which require disclosure of private information.A similar restriction clause was highlighted by the Supreme Court in *Sharda* v. *Dharmpal*,[73] and it was held that when there is no right to privacy specifically conferred by Article 21 of the Constitution of India and only with the extensive interpretation of the phrase "personal liberty" this right has been incorporated into Article 21, it cannot be treated as absolute right available to individual. Thus, some limitations on this right have to be imposed and particularly where two competing interests clash. Recently, in *Arun kumar* v. *Inspector General of Registration*,[74] the Madras High Court observed that the gender identity of any person falls within the domain of one's personal autonomy and involves the right to privacy and dignity. Thus, the State authorities have no power to question this self-determination. Now, it is clear that the right to privacy has achieved a strong footing under the Indian constitutional framework and constantly getting its recognition under various statutes.

VI. THE INFORMATION TECHNOLOGY ACT, 2000, AND PRIVACY CONCERNS

With the development of science, Information and Communication Technologies through the computer and other electronic instruments have greatly

[72] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 : AIR 2017 SC 4161. *See also* G.K. Mani v. New Generation Media Corpn. (P) Ltd., 2019 SCC OnLine Mad 8332 : (2019) 5 Mad LJ 56; Kanimozhi Karunanidhi v. P. Varadarajan, 2018 SCC OnLine Mad 1637 : (2018) 5 Mad LJ 423.

[73] Sharda v. Dharmpal, (2003) 4 SCC 493 : AIR 2003 SC 3450.

[74] Arun kumar v. Inspector General of Registration, 2019 SCC OnLine Mad 8776 : (2019) 3 CTC 576.

enhanced our capacities to collect, store, process and communicate information. At the same time, it makes us vulnerable to intrusions of our privacy on a larger scale. This privacy invasion may happen from the personal sphere also. It may happen through any of the following ways:(i) data on our own personal computers can compromise us in unpleasant ways with consequences ranging from personal embarrassment to financial loss, (ii) transmission of data over the Internet and mobile networks is equally fraught with the risk of interception, (iii) in this age of cloud computing when much of our data, e.g. our emails, chat logs, personal profiles, bank statements *etc*., reside on distant servers of the companies whose services we use, our privacy becomes dependent on the internal electronic security systems of these companies, (iv) the privacy of children, women, old persons, and minorities tend to be especially fragile in this digital age as they have become frequent targets of exploitation, and (v)online data handling has procreated new kinds of annoyances such as electronic voyeurism, spam or offensive email, 'phishing' *etc*., and each of these can affect the privacy of any individual. In India, to address all these issues, the only available statute is the Information Technology Act, 2000 ('the IT Act'). This Act, enacted in 2000, has already been amended various times. However, as will be evidenced by the subsequent sections, it fails to provide complete security with respect to the abovementioned issues.[75] The available scheme for the protection of privacy under the IT Act, requires a detaileddiscussion for understanding the available protection, and its eventual efficacy.

A. CONSEQUENCES FOR FAILURE IN DATA PROTECTION

§43 of the IT Act, provides that if any person commits accesses or secures access to any computer, downloads, copies or extracts any data, introduces any computer contaminant or computer virus, damages any computer, disrupts any computer *etc*., without the permission of the owner or person in-charge of a Computer, Computer System or Computer Network, then that person is liable to pay damages to the person affected. It provides a remedy in the form of compensation to the victim. But for the application of this Section, the act of the accused person must have caused some damage or loss to the person so affected. None of the abovementioned acts would attract penal consequences.[76] However, that is not the only remedy under the IT Act for the victim. §66 of the Act provides that "if any person dishonestly or fraudulently, does any act referred to in §43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both". §66 of the Act was inserted by an amendment made to the original Act in 2009. The major difference between §43 and §66 is that (i) the prerequisite of §66 is the existence of *mens-rea*, which is reflected by the words "dishonestly or fraudulently". This prerequisite is not the condition for the application of §43. The only prerequisite required for

[75] *See also* Pavan Duggal, Electronic Commerce and Intellectual Property Rights in Cyber Space 34-36 (2014).

[76] *See also* Manubhai Murjibhai Varsani v. State of Gujarat, 2014 SCC OnLine Guj 15999 : (2015) 56 (1) GLR 530.

the application of§43 is that the actcommitted by the person must be without permission of the owner or person who is the in-charge of the Computer, Computer System, Computer Network, and (ii) §43 provides for the remedy of the victim in the form of damages to be paid to the person affected by way of compensation by the person committing such contravention, whereas, §66 provides for punishment of the person committing the act, which may extend to three years imprisonment, or to fine which may extend to Rs. 5,00,000.Thus, while discussing both these Sections in *Amit Kumar Jadaun* v. *State of U.P.*,[77] the High Court of Allahabad observed that most important facet about this provision of IT Act is that, no single provision of the Act provides for the alternative application of §43 and §66 of the Act, that means it is not asserted that Simultaneous actions under §43 and §66 of the Act may be initiated by the victim against the person who commits any contravention under §43 of the Act. Thus, the violation of §43 would constitute a civil as well as criminal liability.[78]

Further, the Act provides that where a body corporate is negligent in implementing or maintaining reasonable security practices, and thus causes wrongful gain or wrongful loss to any person, such body corporate shall always be liable to pay damages by way of compensation to the person so affected.[79] The pre-condition for application of this provision is that such body corporate must own, control or operate a computer resource through which it possesses, deals or handles sensitive personal data or information.[80]Therefore, the offences punishable under §43A of the Act lead to civil consequences only and there is no criminal liability to it.[81]As a result, there is always a tendency on the part of body corporate to avoid these practices and get release from the charge only by paying fine.

B. TAMPERING WITH COMPUTER SOURCE DOCUMENTS

The offence of tampering with computer source documents is made out when a person (i) intentionally conceals, destroys or alters a computer source code used for a computer, computer programme, computer system or computer network, (ii) intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network. However, the offence is made out only when computer source code is required to be kept orwhen computer source code is maintained by law for the time being in force.The Act provides imprisonment up to three years or

---

77 Amit Kumar Jadaun v. State of U.P., (2018) 105 ACC 443. not found

78 Sajai Singh, *The Security of Data Export to India*, 13(5) Journal of Internet Law 9, 10 (2009).

79 The Information Technology Act, 2000, §43A.

80 Sensitive personal data or information includes information relating to passwords, credit or debit cards information, biometric information (such as DNA, fingerprints, voice patterns, *etc*. that are used for authentication purposes), physical, physiological and mental health condition, *etc*. Further, any information, which is freely available or accessible in the public domain, is not considered to be sensitive personal data. *See* Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3.

81 *See also* B. Riaz Ahmed v. State of Karnataka, 2016 SCC OnLine Kar 5493.3 : 1 not found plz chk

a fine of Rs. 2,00,000 or both as punishment for the abovementioned offence.[82]The term'computer source code' is also defined in the Explanation to §65 of the IT Act. As per the explanation a) list of programmes, b) computer commands, (c) design and layout, and d) programme analysis of computer resource in any form, is a 'computer source code' for the purpose of §65 of the IT Act.[83] Therefore, §65 requires concealment, destruction or alteration of the "computer source code", which under the Explanation to §65 means the listing of programmes, computer commands, design and layout and programme analysis of computer resources in any form. The deletion of information in a computer can thus not amount to an offence under §65 of the IT Act.[84] This always tends to give a way to the offenders to escape the punishment.

C. BLOCKING FOR ACCESS OF INFORMATION

§69A of the IT Act deals with the power to issue directions for blocking a website to prevent the public from accessing any information through computer resource. From a study of §69A, it can be noticed that it is a narrowly drawn provision with several safeguards. First and foremost, blocking can only be resorted to where the Central Government is satisfied that it is necessary so to dofor any of the following six reasons, such as (i) sovereignty and integrity of India, (ii) defense of India, (iii) security of the State, (iv) friendly relations with foreign states, (v) public order, and (vi) preventing incitement to the commission of any cognisable offence relating to above. Secondly, such necessity is relatable only to the subjects set out in Article 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a writ petition under Article 226 of the Constitution. However, under §69A, any type of blocking to the access of information can take place by a reasoned order after complying with several procedural safeguards, including the hearing of the originator and intermediary. By studying §69A with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, (the '2009 Rules') it can be concluded that there are only two ways in which a blocking order can be passed: (i) by the Designated Officer after complying with the 2009 Rules and (ii) by the Designated Officer when he is bound to do so under the order passed by any competent Court. Any duty regarding the application of mind by the intermediary to judge whether information should or should not be blocked is noticeably absent in §69A read with 2009 Rules.[85] Thus, situation based judgement by following due process is not possible under §69A of the IT Act.

---

82 The Information Technology Act, 2000, §65.

83 *See also* Syed Asifuddin v. State of A.P., 2005 SCC OnLine AP 1100 : (2006) 1 ALD (Cri) 96.

84 *See also* Ramesh Rajagopal v. Devi Polymers (P) Ltd., (2016)_6 SCC 310 : AIR 2016 SC 1920.

85 *See also* Christian Louboutin SAS v. Nakul Bajaj, 2018 SCC OnLine Del 12215 : (2018) 253 DLT 728; Sharat Babu Digumarti v. State (NCT of Delhi), (2017) 2 SCC 18 : AIR 2017 SC 150.

D. PROCEDURAL SAFEGUARDS FOR BLOCKING FOR ACCESS OF INFORMATION

The 2009 Rules have been framed under §69A(2) of the IT Act. The 2009 Rules providea detailed scheme for the application of §69A of the Act. Under the 2009 Rules, the Central Government shall designate by notification in the official gazette an officer of the Central Government not below the rank of a Joint Secretary as the Designated Officer, to issue direction for blocking for access by the public any information referable to §69A of the Act.[86] Further, every organisation[87] has to designate one of its officers as the "Nodal Officer".[88] Any person may send his complaint to the "Nodal Officer" for blocking of access by the public any information generated, received, transmitted, stored or hosted in any computer resource. After receiving such complaint, the concerned organisation will examinethe same and after being so satisfied, shall transmit such complaint through its Nodal Officer to the Designated Officer in a format specified by the Rules.[89] Thus, the Designated Officer is not to entertain any complaint or request for blocking directly from any person. On receiving any such request or complaint from the Nodal Officer of an organisation or from a competent Court, the Designated Officer may by order direct any intermediary or agency of the Government to block any information or part thereof.[90]

The request or complaint shall then be examined by a Committee of Government Personnel[91] who will make all reasonable efforts to identify the originator or intermediary who has hosted the information.[92] If so identified, a notice will be issued to them to appear and submit their reply at a specified date and time, which shall not be less than forty-eight hours from the date and time of receipt of notice by such person or intermediary. The Committee then examines the request and has to consider whether the request is covered by §69A(1) and then has the duty to give a specific recommendation in writing to the Nodal Officer of the concerned organisation. It is only thereafter that the Designated Officer is to submit

---

86 *See also* Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 3.

87 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 2(g). (It defines "organisation", which includes (i) Ministries or Departments of the Government of India, (ii) State Governments and Union territories, (iii) Any agency of the Central Government, as may be notified in the Official Gazette, by the Central Government).

88 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 4.

89 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 6.

90 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 5.

91 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 7.

92 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 8.

the Committee's recommendation to the Secretary, Department of Information Technology, who is to approve such requests or complaints. Upon such approval, the Designated Officer shall then direct any agency of Government or intermediary to block the offending information. Thus, it is also clear from an examination of this provision that it is not merely the intermediary who may be heard. If the originator is identified, the Designated Officer has a duty to hear that originator before passing a blocking order. Thus, it is clear that only after these procedural safeguards are met, that blocking orders can be passed.Apart from this, in the case where there is a certified copy of a Court order, then also such a blocking order can be made.[93]

In cases of emergency where delay caused would be fatal, blocking may take place without any opportunity of hearing. The Designated Officer shall then, not later than forty-eight hours of the issue of the interim direction, bring the request before the Committee, and only on the recommendation of the Committee, the Secretary Department of Information Technology willpass the final order.[94] In the case of an order of a competent Court in India, the Designated Officer shall, on receipt of a certified copy of the Court order, submit it to the Secretary, Department of Information Technology, and then initiate action as directed by the Court.[95] In addition to the above safeguards, a Review Committee shall meet at least once in two months and record its findings as to whether directions issued are in accordance with §69A(1) and if it is of the contrary opinion, the Review Committee may set aside such directions and issue orders to unblock the said information.[96] The Rule further requires that strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof.[97] Thus, except in cases of emergency, the doctrine of natural justice should be complied with. Apart from this, the role of the Review Committee as inspecting authority is very important. If the Review Committee fails to maintain an unbiased attitude at the time of considering the applications, then there is a high chance of giving decisions tilted in favour of the Central Government. As a result, this Review Committee can be called "custodian of fundamental rights to privacy" in cases of website blocking.

---

93 *See also* Shreya Singhal v. Union of India, (2015) 5 SCC 1 : AIR 2015 SC 1523.

94 *See also* Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 9.

95 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 10.

96 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 14.

97 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 16.

E. BREACH OF CONFIDENTIALITY AND PRIVACY AND DISCLOSURE OF INFORMATION

The IT Act provides specific provisions for penalty for breach of confidentiality and privacy. §72 of the Act forbids access to any electronic record, book, register, correspondence,*etc.* without the permission of the person concerned and this offence is punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs. 1,00,000 or with both. By applying the principle of this Section along with §§43, 65, and 66 of the IT Act, the Himachal Pradesh High Court in *Vipul Kumar Kapadi* v. *State of H.P.*,[98] held that the petitioner, who in order to make profit, sent data shade through his e-mail ID to other concerns, as such committed offences under §§43, 65, 66 and 72 of the IT Act. Similarly, by applying the fundamental principle of the right to privacy, the Madhya Pradesh High Court in *Anurima* v. *Sunil Mehta*,[99] observed that when a conversation was recorded without the knowledge of the wife, behind her back, thenit is definitely an infringement of her right to privacy. Besides that, there is also a penalty under §72 of the IT Act for such recording and it could not be used as an instrument to create evidence of such nature.

The newly inserted §72A provides a way to punish in cases of disclosure of information in breach of a lawful contract. It states that,

> "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 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".[100]

Hence, it is clear that the liability under §72A only arises out of contractual obligation. If the complainant fails to prove the existence of the contract, there is no scope to apply the provisions of §72A. Mere apprehension of misuse of data does not constitute any offence.[101] Further, under this Section not only the public officials, but also the private individuals are subject to penalty. In addition to that, there are occasions when without having any contract, access to personal information is provided.In those cases,though there is sharing of information, but §72A has no role to play.However, India has cyber police who have the capacity to

[98] Vipul Kumar Kapadi v. State of H.P., ILR 2017 HP 21. Not found plz chk

[99] Anurima v. Sunil Mehta, 2015 SCC OnLine MP 7340 : AIR 2016 MP 112.

[100] Inserted by the Information Technology (*Amendment*) Act, 2008, §37.

[101] *See also* Aaron Softech (P) Ltd. v. State of Assam, 2019 SCC OnLine Gau 5636.6 :() Not found plz chk

prosecute people for violations of this Act, which highlights the potential of this Section in cases of abuse.

F. NATIONAL PRIVACY PRINCIPLES

In the discussion of privacy and more particularly the right to privacy in India, the Justice *Ajit Prakash* Shah Committee report is a path breaking event. In 2012, the Planning Commission and the Group of Experts on Privacy Issues met several times on the question of the Right to Privacy. In its report, the Committee prescribed protection of privacy regarding information through nine principles, such as: (i) the **principle of notice**, (ii) the **principle of choice and consent**, (iii) the **principle of collection limitation**, (iv) the **principle of purpose limitation**, (v) the **principle of access and correction**, (vi) the **principle of disclosure of information**, (vii) the **principle of security**, (viii) the **principle of openness**, and (ix) the **principle of accountability.**[102]**The principle of notice** provides that the data controller has a duty to givenotice of its information practices to all individualsbefore any personal information is collected from them. This notice of information should be in clear and concise language. The **principle of choice and consent** articulates that a data controller shall give individuals the choice when providing their personal information, and take individual consent. Only after consent has been taken, the data controller will collect, process, use, or disclose such information to third parties, except in the case of authorised agencies. Further,**the principle of collection limitation** and **principle of purpose limitation** require the collection of only such personal information from data subjects as is necessary for the purposes identified for such collection and that should be adequate and relevant to the purposes for which they are processed. Moreover, individuals have the right to access and correct data after collection of them. The data controller shall not disclose personal information to third parties in general circumstances. The data controller can disclose information only after providing notice and seeking informed consent from the individual for such disclosure. **The principle of security**stresseson the duty ofthe data controller to secure personal information by reasonable security safeguards against loss, unauthorised access, use, destruction, storage, modification, processing, deanonymisation, unauthorised disclosure or other reasonably foreseeable risks. The data controller shall take all necessary steps to implement practices, procedures, policies regarding privacy principles and he or she will be also accountable for the same. It also recommends setting up privacy commissioners, both at the Central and State levels. Thus, these parameters provide a detailed scheme of privacy principles for the first time. They further provide guidelines for the future statutes or regulatory frameworks regarding the right to privacy.

[102] *See* Planning Commission, *Report of the Group of Experts on Privacy*, October 16, 2012, ¶3.2 (2012).

VII. CONCLUSION

Informational privacy is a facet of the right to privacy. In an age of information, the threats to privacy can originate not only from the State but from non-State actors as well. This right to privacy has also been spelled out and based on the inherent human right to be left alone.[103] A common premise is that the available technical safeguards protect individual privacy in accordance with legal and social norms. Privacy technologies are viewed through this lens because privacy is inherently a normative concept, with foundations in philosophical, legal, sociological, political, and economic traditions.[104] Various privacy regulations and policies attempt to capture and codify these norms and values as enforceable constraints on behaviour. In India, though privacy has been recognised as an integral part of personal liberty, like most other Fundamental Rights, the right to privacy is not an "absolute right" and in certain circumstances, it can be overridden by competing State interests. Therefore, the balance between personal needs and social welfare should be maintained. In this technological era, information privacy can be seen as a social goal. To achieve information privacy goals,there isthe requirement of social innovation, including the formation of new standards and legal rules to establish demarcation lines between acceptable and unacceptable uses of personal data.[105] Thus, the Union Government must examine and put into place a robust regime for data protection with a far more detailed scheme than the one that exists under the Information Technology Act. That prospective detailed schemesshould maintain a careful and sensitive balance between individual interests and legitimate concerns of the State. However, the Personal Data Protection Bill, 2018, recognises the right to privacy to be a Fundamental Right and demonstrates the need to protect personal data as an essential facet of informational privacy. It also demonstratesthe right to privacy as a pre-requisite for the creation of a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress, and innovation. ThisPersonal Data Protection Billis currently pending before the Parliament. The Union Legislature should proceed with the same as early as possible. Moreover, there should be continuous effort from the end of the government to train all citizens about data handling and to provide basic knowledge about the process of protecting personal information. Awareness building among the general masses along with the strict implementation of a specific statute relating to informational privacy, is the way forward to combat the misuse of technological development.

---

[103] Soli J. Sorabjee, *Creative Role of Indian Judiciary in Enlarging and Protecting Human Rights*, 17 Journal of the National Human Rights Commission 21, 22 (2018).

[104] J.M. Cohen. *What Privacy Is for*, 126 Harvard Law Review 7, 1904 (2013); D. J. Solove. *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 San Diego Law Review 4, 745 (2007).

[105] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stanford Law Review 1125, 1169 (2000).