WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Information Technology Vis-À-Vis Right to Privacy: Legal And Judicial View

Dr. Anant D. Chinchure*

Central University of Karnataka,India

ABSTRACT:

Internet and privacy are two core components of human life. The right to privacy is an elementary human right and is a facet of human dignity. Privacy has become one of the pertinent human rights issues in the age of internet. Hence, there is a stern demand of legislation to protect digital privacy. The act of contravenes begin when the personal data and space of an individual by the use of internet. The adaptations of government policies like E-governance, the collection, storage, use and sharing of biometric data has increased. There is always a risk of data leakage from these gigantic databases. Cyber threats are also one of the major problems created by hackers which hampers with the data protection of individuals. The article provides an outline of the concerns and responses in protecting breach of privacy which is getting hampered in digital age. To protect and safeguard the data must be priority, prevention and investigation of breach of privacy should be the legitimate aims of the State. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Indian legislations by a large way primarily concerned with the security of the state however in the digital era time has changed and since law is ever evolving it is the time to make necessary amendments into the contemporary law of the country which will serve greater protection to the data and privacy.

Key Words: Privacy, Internet, Data, Security

Introduction

In many countries, the concept of privacy is connected with data protection. The facet of data protection includes privacy as a tool of a trustworthy relationship between entities associated with giving and collecting the data which includes wide personal information of individuals.

According to Black's Law Dictionary, right to privacy means *'*right to be let alone, the right of a person to be free from any unwarranted interference.' The predominant presence of state and non-state entities controls the aspects of social existence which stand upon the freedom of the individual. The rights came from the wake of a person's right to life and liberty and in some or other all are interconnected to the right to equality, liberty and freedoms. The concept can be seen in golden triangle in the Indian constitution which includes the articles 14, 19 and 21.

Justice Thomas Cooley has observed that the law of privacy has the same meaning as the right to be let alone.[1] Professor Edward Shils explained that 'privacy is zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose.'[2]

The right to privacy is an elementary human right which is mentioned under the United Nations Universal Declaration of Human Rights,[3] the International Covenant on Civil and Political Rights[4] and by many other international instruments. Right to privacy is a facet of human dignity and also relates to essential rights such as freedom of association and the freedom of speech. It has become one of the pertinent human rights issues of the modern age. Almost every country in the world recognizes the right of privacy implicitly or expressly in their respective constitutions.

Privacy is a state of the individual where a human being has full control over the disallowed intrusion by any person into his or her life. It is true that man is a social animal however he has complete command over his personal existence which cannot be disturbed by anyone without his permission. Right to privacy has justified the need of being left alone.[5]

In the countries like the United States, India, Ireland etc. the right to privacy is not expressly mentioned in their constitutions. However, because of the

* Assistant Professor, Department of Law, Central University of Karnataka, Kalaburagi (dranantdc@gmail.com)
[1] Cooley Thomas, A Treatise on the Law of Torts, Callaghan, pp. 29, (1888).
[2]Edward Shils, Privacy: Its Constitution and Vicissitudes, Law and Contemporary Problems, pp. 281306, (1966).
[3] Universal Declaration of Human Rights, Article 12, UN General Assembly, 217 A (III), (10 December 1948).
[4]International Covenant on Civil and Political Rights, Article 17, United Nations, Treaty Series, vol. 999, p. 171, (16 December 1966).
[5] Rana P.K., Right to Privacy in Indian Perspective, International Journal of Law, pp. 07, (2016).

ruling of their courts this right is recognized as a part of other provisions. The countries who are a signatory to the international instruments like the International Covenant on Civil and Political Rights or the European Convention on Human Rights have inculcated the right of privacy into their legislations. The laws concerning the protection of individual privacy started developing in early 1970's.[6]

With respect to India, there is a stern demand of legislation for the reason that the evolution of information technology has given entities new unrestricted powers by which they can easily gather, store and share private information of individuals. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the extent of knowledge generated by each individual. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any individual without the necessity for one central system. New technologies developed by the defense industry are spreading into enforcement, civilian agencies, and personal companies.

Digital privacy is another aspect of the right to privacy. It comes into picture when a person, organisation or a state contravenes with the personal data and space of an individual by the use of internet and the devices connected through it. The meaning and data shared willingly by person may differ from person to person in digital space.

There are two aspects of privacy. It can be defined in negative sense and can also be defined in positive sense. The negative aspect to privacy protects the intrinsic identity of a person such as sexual orientation, political and religious beliefs etc. However, the positive aspect puts an obligation on the part of the state to enact laws to protect the individual identity of a person and eradicating hindrances in their lives which would infringe their privacy.[7]

That the argument where it is said that privacy concerns more about the personal and social rights of an individual. However, one must also know that in this technology driven world the facets of digital privacy are also becoming a pertinent part to be addressed by the state. The discussions about privacy have become the need of the hour since with the digital growing world it is one of the most vulnerable rights guaranteed to the individual. There is no doubt about the fact that as we move technologically forward, protection of privacy will get hampered. Also, with the adaptations of new government policies like E-governance, the collection, storage, use and sharing of biometric data has increased. There is always a risk of data leakage from these gigantic databases. Cyber threats are also one of the major problems created by hackers which hampers with the data protection of individuals.

The right to Privacy is an interest with several proportions which also includes the privacy of personal data in internet dominion, known as the 'internet privacy' or 'online privacy'[8]. Internet privacy and anonymity are vital to users, especially in this modern tech era. Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen. Internet privacy is a subset of data privacy and is necessary to preserve and protect any personal information in the internet domain, collected by any organization, from being accessed by a third party. Further, it is a part of Information Technology that helps an individual or an organization determine what data within a system can be shared with others and which should be restricted. The essence of privacy of personal data is that the individuals can legitimately claim that data about themselves should not be automatically available to other individuals and organisations and that, where the data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. Such data must be within the controllable limits of the individual whose data is in question and that it shall be used with the consent of the person. Thus, every individual has the desire to control, or at least significantly influence, the handling of data about themselves. There are opposing interests too; but protection is a process of finding appropriate balance between privacy and these multiple competing interests. Internet privacy is perhaps one of the most important personal rights being violated in the realm of liberty without the person himself being aware of such violations.

Legal and Judicial perspective of Right to Privacy

Information Technology Act, 2000

The Information Technology Act, 2000 contains provisions regarding the safeguarding of the online privacy[9], online fraud and hacking,[10] data protection standards for the corporate bodies,[11] monitoring and collecting of online traffic data,[12] surveillance, monitoring and decryption of communications[13] etc. Going in detail into the provisions of the Information Technology Act, 2000 and the Information Technology (Amendment) Act, 2008, there are certain sections which are essential to be discussed in relation to the subject at hand.

[6] German Federal Data Protection Act of 1977, Federal Law Gazette.
[7] Anna Jonsson Cornell, Right to Privacy, Max Planck Encyclopaedia of Comparative Constitutional Law, (2015).
[8]Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term and refers to a variety of factors, techniques and technologies which are used to protect sensitive and private data, communications, and preferences.
[9] The Information Technology Act, 2000, No. 21, Parliament of India, pp. 67.
[10] The Information Technology Act, 2000, No. 21, Parliament of India, pp. 43
[11] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information Rules, (2011)
[12] Information Technology (Procedure and Safeguards for Monitoring and Collection Of Traffic Data Or Other Information) Rules, (2009).
[13] Information Technology (Procedure and Safeguards for Intercepting, Monitoring, And Decryption) rules, (2009).

The information technology act was enacted with an objective of providing recognition to the transactions that are carried out in online medium, e-commerce transactions and the businesses that arise through the technological medium. As we witness the expansion and growth in technology, the act underwent amendments and also published rules and regulations time to time to come up with the pace of the technology. In the hurried process, there still remained some gaps. From last decade itself, there was a need for the laws relating to the online privacy and data protection in the internet realm. Further, the collection, processing and usage of the data of individuals for the use of government through policies like Aadhar are not efficient at that point of time. There was a push for such laws from a very long time. We have a need to put in laws relating to the internet privacy concerning the freedom of speech and expression. Though the IT act is all about the technology, privacy and protection of data, it is important to discuss with special emphasis to the internet privacy and the freedom of speech and expression. In order to protect the individual privacy of citizens, the Information Technology Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules of 2011 were framed.

In general, the information that is disseminated in the internet is dealt by the intermediaries only who host the internet to the users and the content which users post go through the intermediaries. In the Information Technology act, 2000 there is a provision i.e. section 79 in which the intermediaries are held liable for the content for some extent which goes through them. This was amended in the 2008 amendment and the new provision provides a safe harbour to the intermediaries i.e. section 79 of the act exempted the intermediaries from the liability of hosting unlawful content in certain circumstances. The contents of the provisions of section 79 in both IT act, 2000 and IT (amendment) act, 2008 are as follows:

The IT act, 2000 in chapter XII states with a head note 'network service providers not to be liable in certain cases' and the provision[14] reads (section 79):

> "For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation – for the purposes of this section –

a) "network service provider" means an intermediary;
b) "Third party information" means any information dealt with by a network service provider in his capacity as an intermediary;"[15]

Section 79 of the amended Information Technology Act (2008) which was added in Chapter XII of the act titled 'Intermediaries not to be liable in certain cases'[16] and the section reads as

"Exemption from liability of intermediary in certain cases:

1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
2) The provisions of sub-section (1) shall apply if-
    a. the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
    b. the intermediary does not:
        i. initiate the transmission,
        ii. select the receiver of the transmission, and
        iii. select or modify the information contained in the transmission;
    c. the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
3) The provisions of sub-section (1) shall not apply if-
    a. the intermediary has conspired or abetted or aided or induced, whether by threats or promise or authorise in the commission of the unlawful act;
    b. upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation - For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his

[14] The Information Technology Act, 2000, No. 21, Parliament of India, pp. 79.
[15] Ibid
[16] The Information Technology (Amendment) Act, 2008, No. 10, Parliament of India, pp. 79.

capacity as an intermediary"[17]

Both the texts of the previous act and the amended act speak of the intermediary liability only but the terms are different from that of the IT act, 2000. This amended provision makes it a safe harbour as the intermediary is not made liable if it only facilitates the content but has no knowledge of the same, the intermediary can be directed by the court[18] to remove such content. In furtherance, there are rules framed subsequent to the act which the intermediary has to follow in order to avail the exemptions under section 79 of the principal act. The term intermediary is defined under section 2(w) of the principal act[19] which is also amended under the IT (amendment) Act, 2008 and is defined as:

> "'Intermediary' with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes."[20]

Data Protection Bill, 2019

The data protection law in India is still in developing phase. Data Protection Bill of 2019 was introduced in late 2019 in the legislature to protect the privacy of individuals and to protect their personal data from sharing and usage by unlawful means. The bill aims to create a mutual understanding and trustworthy relationship between the individual and data collecting entities so that the data of such individual could be processed in a cautious manner in return of the services provided to them by those entities. The bill also ensures that no unauthorised sharing will be done by these data collecting entities. The bill also aims to create an authority (Data Protection Authority) to protect the data of individuals.

The ambit of this bill is quite expansive as it covers majority of businesses in India such as real estate, healthcare services and pharmaceutical companies etc. The scope of this bill is also extended to protect digital processing of data in the sectors like Ecommerce, social media and information technology sector. However the small entities like business which collect information on manual basis are covered under the exception under this bill. But, they also have to act in compliance of the bill.

The financial services and telecommunication sector are governed under their own respective laws and their regulators have already set certain strict and cogent norms to protect the privacy of individuals and to provide confidentiality to their data.

The Data Protection Bill, 2019 gives directions to the data collecting and data storing entities to obtain consent by the individuals for such measure. The entities must also preserve such evidence where the consent of the individual was received. Under this bill, the individuals can also get access to their data[21] in one place. Further, they can also make corrections and can even delete their personal data. One of the most pertinent features of this bill is that the consumers can withdraw their consent to collect and store data by the businesses.

Another important feature of this bill is transfer of data. There are certain cases where a person wants to change his place of work or he wants to terminate a particular service provided by a respective business entity and switch to another entity whose service is better than the previous in the idea of the consumer. In such a case he can transfer his data to other business entity. The Data Protection Bill, 2019 makes it compulsory to business entities to make and include organisational changes into their framework to protect the privacy of the individual at each step. This is also called as privacy by design principle. The bill also specifies that the sensitive personal data shall be kept in Indian servers only and such sensitive data must not be transferred from India to any other country. This bill also creates a group, from many data fiduciaries called as significant data fiduciary where the duty of this group is to audit the personal data of individuals and to ensure that data is stored in a fair and responsible manner. The group of significant data fiduciary is also in charge of appointing data protection officers. With respect to the infringement under this bill, the Data Protection Authority has the power to impose fine any business entity who does not act in accordance with the bill. The maximum penalty which the bill specifies is either rupees fifteen crores or four percent of the global turnover of the business, whichever is higher.

In Chapter VIII of the PDP bill which deals with exemptions, sections 35 provides power to the central government to exempt any governmental agency from this act and section 36 also exempts certain provisions from application in processing of personal data. These provisions provide much power to the central government in excluding any government agency and exempting the provisions of the act. Certain provisions are also not applicable to the courts and other law enforcement officers under section 36 of the bill.

The significant changes made to the PDP bill, 2019 from that of the 2018 bill and the draft bill proposed by the committee is that a separate class of intermediaries is made which includes the social media intermediaries who enable the individuals to interact and pass information to one another in the

[17] The Information Technology (Amendment) Act, 2008, No. 10, Parliament of India, pp. 79.
[18] Shreya Singhal v. Union of India, AIR 2015 SC 1523; Supreme Court read down section 79 to mean the actual knowledge from the direction of a court order or from the appropriate government.
[19] The Information Technology (Amendment) Act, 2008, No. 10, Parliament of India, pp. 2.
[20] Ibid
[21] Sec. 17, Data Protection Bill, 2019, Parliament of India, pp. 11

internet realm. This is a welcome change as the data that is exchanged and disseminated under the social media and online media comes under the purview of the PDP bill, 2019. But another change is that the bill gives more power to the central government in exempting governmental agencies from the bill which may hamper the whole idea of bringing the legislation.

Judicial Viewpoint

The judicial evolution of the right to privacy started in the year 1950 with the infamous case of A.K. Gopalan v. State of Madras[22] where the court was of the opinion that Article 21 only guaranteed procedural due process and the preventive detention legislation under which the petitioner was detained was a valid law and in accordance with the constitution. Even though there are some fundamental rights of the petitioner have been infringed such as the freedom of movement and the right against arbitrary detention mentioned under articles 14 and 19. The rationale that came out of this decision was that Article 14, Article 19 and Article 21 are not in nexus with each other but are separate and independent rights because these rights are also different to one another.

In the case of MP Sharma v. Satish Chandra[23] the court has held that the search of property and seizure of articles does not violate the right against self-incrimination. The court also observed that if the framers of the constitution itself did not intend to inculcate the right guaranteeing privacy to individuals just like the fourth amendment of the US constitution, they have no justification to adjudge this as a fundamental right. Moreover, even the framers of the constitution were not of the view that the power of search and seizure by the state authorities violate the right to privacy. Therefore there is no question to include the right to privacy in our constitution.

In Kharak Singh v. State of Uttar Pradesh[24] court adjudged that

> "the Indian Constitution does not contain a guarantee similar to the Fourth Amendment of the US Constitution, it proceeded to hold 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 manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III."

However, if we refer to the dissenting judgment of Justice Subba Rao, we can observe of an idea that the right to privacy was being given importance. He held that:

> "Personal liberty must not exclude the right of a person to sleep which is very essential requirement to the existence of a human being. Every person has a right to get comfortable sleep. Further, if the policemen invade the home of any individual at this odd hour, it will amount the violation of the right to sleep. The essential human needs are a part of personal liberty of a person which helps in overall development of a person. The preamble of the Indian constitution also guarantees to assure the dignity of the individual."

Justice Subba Rao referred upon the judgment of Wolf v. Colorado[25] which held that,

> "The security of one's privacy against arbitrary intrusion by the police is basic to a free society. We have no hesitation in saying that a state was affirmatively to sanction such police incursion into privacy it would run counter to the guarantee of the Fourth Amendment."

The right to personal liberty includes not only a right to be free from hindrances placed on the movements of a person, but also free from intrusions on his private life. Article 21 grants the right to the individual to be free from restrictions or encroachments. In this view, though the Constitution does not expressly declare the right to privacy as a fundamental right, such a right is essential to personal liberty of a person. Subsequently, Justice Subba Rao mentioned that the right to privacy is a constitutional principle and an ingredient of personal liberty under Article 21 of the Constitution.

The next landmark case concerning the right to privacy is Govind v. State of Madhya Pradesh.[26] In this case the judgment of the Supreme Court is considered ambiguous because there was no clear cut rule or guideline was mentioned by the court concerning protection of privacy of an individual. However, the court was of the view that the right to privacy is an important right to an individual but the Indian constitution does not contain this right. The court held that:

> "There can be no doubt that privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that acclaimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling state interest test. Then the question would be whether a state interest is of such paramount importance as would justify an infringement of the right... Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right that fundamental right must be subject to restriction on the

[22] AIR 1950 SC 27
[23] (1954) SCR 1077
[24](1964) 1 SCR 332.
[25]338 U.S. 25.
[26] 1975 AIR 1378

basis of compelling public interest."

In another locus classicus case of Maneka Gandhi v. Union of India[27], it was established that the constitutional doctrine is that, the expression 'personal liberty' in Article 21 covers a variety of rights, some of which 'have been raised to the status of distinct fundamental rights' and given additional protection under Article 19. The decision in Maneka carried the constitutional principle of the over-lapping nature of fundamental rights to its logical conclusion. Non arbitrariness but reasonable principles are the key elements of the guarantee against arbitrary state acts under Article 14 with is also in nexus with Article 21. A law which provides for a compromise of life or personal liberty under Article 21 must lay down not just a procedure which is fair in nature but a procedure which is 'just, fair and reasonable.'

In the case of R. Rajagopal v. Union of India,[28] the Supreme Court recognized that the right to privacy can be both a tort, a civil wrong whose remedy can result in an actionable claim as well as it can be a fundamental right. The court further held that:

> "A citizen has a right to safeguard the privacy of his or her own family, marriage, procreation, motherhood, child-bearing and education among other matters and nobody can publish anything regarding the same unless
> (i) he or she consents or voluntarily thrusts himself into controversy,
> (ii) the publication is made using material which is in public records (except for cases of rape, kidnapping and abduction), or
> (iii) he or she is a public servant and the matter relates to his/her discharge of official duties."

In People's Union for Civil Liberties v. Union of India,[29] the Supreme Court extended the scope of life and personal liberty and mentioned that the communications of an individual comes under the purview of the right to privacy. The Court also laid down the guidelines that form an essential subject for the checks and balances in interception provisions in India, they are:

- Interception orders to be issued only by Home Secretaries at both the Central and State governments;
- Issues such as the necessity of the information and whether it can be acquired by other means to be considered while making the decision to approve interception;
- The addresses and the persons whose communication has to be intercepted should be specified in the order, which means that the interception order cannot be generic; and
- Putting a cap of two months on the life of an interception order.

In Selvi and others v. State of Karnataka and others,[30] The Supreme Court accepted the fact that there is a difference between physical privacy and mental privacy. The court held that:

> "Indian criminal and evidence law contends that interference with the right to physical and bodily privacy in certain circumstances, but the same cannot be used to compel a person to impart personal knowledge about a relevant fact. This case also establishes the intersection of the right to privacy with Article 20(3) (self-incrimination). An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy. Subjecting a person to techniques such as narcoanalysis, polygraph examination and the Brain Electrical Activation Profile (BEAP) test without his or her consent violates the subject's mental privacy."

Further, in the case of Suresh Kumar Koushal v NAZ foundation,[31] The Supreme Court held that Section 377 of IPC criminalises a consensual sexual act of adults in their personal space is in contravention to Articles 14, 15 and 21 of the Constitution. However the Delhi High Court in the same matter[32] held that:

> "…The sphere of privacy allows persons to develop human relations without interference from the outside community or from the State. The exercise of autonomy enables an individual to attain fulfilment, grow in self-esteem, build relationships of his or her choice and fulfil all legitimate goals that he or she may set. In the Indian Constitution, the right to live with dignity and the right of privacy both are recognised as dimensions of Article 21. The High Court adverted at length to global trends in the protection of privacy – dignity rights of homosexuals, including decisions emanating from the US Supreme Court, the South African Constitutional Court and the European Court of Human Rights. The view of the High Court was that a statutory provision targeting homosexuals as a class violates Article 14, and amounted to a hostile discrimination on the grounds of sexual orientation. However, the SC held that "In its anxiety to protect the so-called rights of LGBT persons and to declare that Section 377 IPC violates the right to privacy, autonomy and dignity, the High Court has extensively relied upon the judgments of other jurisdictions. Though these judgments shed considerable light on various aspects of this right and are informative in relation to the plight of sexual minorities, we feel that they cannot be applied blindfolded for deciding the constitutionality of the law

[27]AIR 1978 SC 597.
[28]AIR 1995 SC 264.
[29]AIR 1997 SC 568.
[30] 2010 (7) SCC 263
[31](2014) 1 SCC 1.
[32]Naz Foundation v Government of NCT, 2010 Cri.LJ 94.

enacted by the Indian Legislature."

In the case of Unique Identification Authority of India and another v. Central Bureau of Investigation,[33] for a reason to investigate a criminal offence, the Central Bureau of Investigation asked for an access to the database of the Unique Identity Authority of India. Conversely, the Supreme Court its interim order held that the data of any person must not be shared by the Unique Identity Authority of India specially the biometric data of persons which is a very essential form of information. If such information goes in the hands of any third party agency without the consent of the concerned person, it would be a gross violation of privacy of an individual.

The case that settled the privacy conundrum that whether this right is a part of life and personal liberty is K.S Puttaswamy v. Union of India,[34] the Supreme Court its landmark judgment held that:

> "the right to privacy and the protection of sexual orientation lie at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution. Every individual in society irrespective of social class or economic status is entitled to the intimacy and autonomy which privacy protects. It is privacy as an intrinsic and core feature of life and personal liberty which enables an individual to stand up against a programme of forced sterilization. Then again, it is privacy which is a powerful guarantee if the State were to introduce compulsory drug trials of nonconsenting men or women. The sanctity of marriage, the liberty of procreation, the choice of a family life and the dignity of being are matters which concern every individual irrespective of social strata or economic well being. The pursuit of happiness is founded upon autonomy and dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals."

The central theme is that privacy is an intrinsic part of life, personal liberty and of the freedoms guaranteed by Part III which entitles it to protection as a core of constitutional doctrine. The protection of privacy by the Constitution liberates it, as it were, from the uncertainties of statutory law which, as we have noted, is subject to the range of legislative annulments open to a majoritarian government. Any abridgment must meet the requirements prescribed by Article 21, Article 19 or the relevant freedom. Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III. Judicial recognition of the existence of a constitutional right of privacy is not an exercise in the nature of amending the Constitution nor is the Court embarking on a constitutional function of that nature which is entrusted to Parliament.

Conclusion

Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data serves together with the legitimate concerns of the State. One of the chief concerns which the formulation of a data protection regime has to take into account is that while the internet is a source of lawful activity, both personal and commercial and concerns of national security conundrums since the seamless structure of the internet can be exploited by non-law abiding instruments to wreak havoc and destruction in civilised societies. As long as intelligence personnel can be trusted to use the knowledge gained only for the defense of the nation, the public will be compensated for the costs of diminished privacy in increased security from terrorist attacks.

Apart from national security, the state may have justifiable reasons for the collection and storage of data. In a social welfare state, the government embarks upon programs which provide benefits to impoverished and marginalized sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilization of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. But, the data which the state has collected has to be utilized for legitimate purposes of the state and ought not to be utilized unauthorized for extraneous purposes. This will ensure that the legitimate concerns of the state are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information technology which is legitimately deployed is a powerful enabler in the spread of innovation and knowledge.

Privacy involves hiding information whereas anonymity involves hiding what makes it personal. An unauthorized parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy. On the other hand, the state may assert a legitimate interest in analyzing data borne from hospital records to understand and deal with a public health epidemic such as malaria or dengue to obviate a serious impact on the population. If the State preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it.[35]

[33] Special Leave Petition to Appeal (Crl) No(s).2524/2014.
[34] Writ Petition (Civil) No. 494 of 2012
[35] Jeffrey M. Skopek, Reasonable Expectations of Anonymity, Virginia Law Review, Vol. 101, pp. 691, (2015).

Pre-surveillance authorization from a judicial or quasi-judicial authority, which is not too proximate to the institutions carrying out the surveillance, and only where there is clear evidence of a sufficient threat and the surveillance proposed, is strictly necessary and proportionate. An effective and accessible remedy for people subjected to unlawful surveillance, including post notification and the possibility of civil compensation and criminal sanction for unlawful surveillance.

Indian legislations by a large way primarily concerned with the security of the state however in the digital era times have changed and since law is ever evolving it is the time to make necessary amendments into the contemporary law of the country which will serve greater protection to the data of individuals. The Indian Data Protection Bill, 2019 readily provides a system which will direct the parties and business organizations to be concerned about the personal data. The Bill provides a change in framework and organization in the businesses which also is beneficial for the ordinary person. However, the drawbacks of the draft legislation, which are mentioned in this study, must be appropriately addressed before it becomes a law.