Chapter - 4

Right to privacy and data protection Indian perspective
CHAPTER – 4

Right to Privacy and Data Protection
Indian Perspective

An Overview

Today in many fields of human activity information technology has been employed as substitute for some or all of the functions performed by human beings and as consequence, these technically performed functions have the potential to conflict with the fundamental human right of privacy and thus raises a legal concern in an era in which the technology has made all data equally accessible, regardless of the jurisdiction in cyberspace.

In this context, the computer world and The Internet (world wide wave, www) are perfect examples for both of the sides i.e. positive effect as well as negative effect globally and its activities in a comprehensive manner such as communications, administration, governance, relationships, financial Services (Banking & Non Banking), medical records and individual information.

With the advancement in technological development, there took place a transition in the standard of crimes. In the
present era, most of the crimes are being done by the single click; the criminals are able to get the secured information. The lust of information is acting as a catalyst in the growth of cyber crimes.

Maintaining of data bases is not as much difficult task as maintaining its integrity, so in this era the most concerned debate is going on to discover a perfect method of data protection. Therefore, it is the very big challenge for the business houses, financial institutions and the governmental bodies so as to give adequate protection to their huge databases. In the absence of any particular stringent law relating to data protection, the miscreants are gaining expertise in their work day by day.

Though this world has simplified our life style but it left certain anomalies in procurement of its object which resulted in involuntary disclosure of data. Many countries other than India have their data protection laws as a separate discipline. They have well framed and established laws, exclusively for the data protection.
Data Protection and Indian Legal Perspective

The Constitution of India has implicitly provided the law relating to privacy under the scope and ambit of Article 21. Its interpretation is found insufficient to provide adequate protection to the data. In the year 2000, effort has been made by the Indian legislatures to embrace privacy issues relating to computer system under the purview of the Information Technology Act, 2000. This Act contains certain provisions which provide protection of stored data.

Moreover, in the year 2006, Indian legislature has also introduced a bill known as ‘The Personal Data Protection Bill, 2006’ so as to provide protection to the personal information of the persons.

The Personal Data Protection Bill, 2006

Upon the footprints of the foreign laws, this bill has been introduced in the Upper House of Indian Parliament Rajya Sabha on December 08, 2006. The purpose of this bill is to provide protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for

---

1 http://rajyasabha.nic.in/bills-ls-rs/2006/XCI_2006.pdf
2 Ibid.
commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. Provisions contained in this Act are relating to nature of data to be obtained for the specific purpose and the quantum of data to be obtained for the purpose\(^3\). Data controllers have been proposed to be appointed to look upon the matters relating to violation of the proposed Act.

On comparing the Indian law with the law of developed countries the proper requirement for the Indian law can be analyzed. Data are not of same utility and importance; it varies from one another on the basis of utility. So, we require framing separate categories of data having different utility values, as the U.S. have. Moreover, the provisions of Information Technology Act, 2000 deals basically with extraction of data, destruction of data.

Organizations cannot get full protection of data through that which ultimately forced them to enter into separate agreements to keep their data secured. These agreements have the same enforceability as the general contract.

\(^3\) Ibid.
Despite the effort being made for having a data protection law as a separate discipline, the Indian legislatures have left some lacuna in framing the bill of 2006. The bill has been drafted wholly on the structure of the UK Data Protection Law⁴ whereas today’s requirement is of a comprehensive Act. Thus it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favourable to current legal requirements.

Being one of the most concerned topics of discussion in the modern era, legislatures are required to frame more stringent and comprehensive law for the protection of data which requires a qualitative effort rather than quantitative in modern context of developing technologies.

**Information Technology Act, 2000: Some Reflections**

Regarding the protection, the Act has various provisions and it also provides certain penalties for violation of the prescribed standard.

The Act provides protection against unauthorized access of the computer system by imposing heavy penalty up to one

---

⁴ The U. K. Data Protection Act, 1998
The unauthorized downloading, extraction and copying of data are also covered under the same penalty. It also imposes penalty for unauthorized introduction of computer viruses or contaminants. It also provides penalties for assisting the unauthorized access.

The section 65 provides provisions for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer a penalty of imprisonment of fine up to 2 lakh rupees. Thus protection has been provided against tampering of computer source documents.

Protection against hacking has been provided under this Act. As per the provision hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss or damage will be caused to any person and information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This Act imposes the penalty of imprisonment of three years or fine up to two lakh rupees or both on the hacker.

---

5 Section 43
6 Cl. (c)
7 Cl. (g)
8 Section 66
The Act also provides protection to the data stored in the protected system.\(^9\) Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

The section 72 provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act, 2000 and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both.

**Issue of Privacy & Data Protection**

In the context of digital or cyber privacy, the privacy concern exists wherever personally identifiable information is collected and stored in digital form or otherwise. Improper or

\(^9\) See, Section 70.
non-existent disclosure control can be the root cause for privacy issue and breach of confidentiality. Since, Data privacy is the relationship between collection and dissemination of data. The challenge in data privacy is to share data while protecting personally identifiable information. The various types of personal information often come under privacy concerns.

Thus, privacy may be\textsuperscript{10}:

- **Life Style**
- **Financial**
- **Data/Internet**
- **Medical**
- **Political**
- **Genetic**

**Life style**

For various reasons individuals may not wish for personal information such as their religion, sexual orientation, political affiliations, or personal activities to be revealed. This may be to avoid personal embarrassment or damage to one’s professional reputation.

\textsuperscript{10} See, Dhruv Jain, “The Right to Privacy in India: An Overview”, AIR-June 2009-Journal Section, P.91
Financial Privacy

Information about a person’s financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases can be sensitive. If criminals gain access to information such as a person’s account or credit card numbers that person could become the victim of fraud or identify theft. Information about a person’s purchases can reveal a great deal about that person’s history, such as places he has visited, whom they have had contact with, products they use, their activities and habits, or medications they have used. In some cases corporations might wish to use this information to target individual with marketing customized towards those individual’s personal preferences, something which that person may or may not agree.

Internet Privacy

The ability to control what information one reveals about oneself over the Internet, and to control who can access that information, has become a growing concern include whether e-mail can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited
collect, store, and possibly share personally identifiable information about users.

Medical Privacy

A person may not wish for their medical records to be revealed to others. This may be because they have concern that it might affect their insurance coverage or employment, or it may be because they would not wish for others to know about medical or psychological conditions or treatment which would be embarrassing. Revealing medical data could also reveal other details about one's personal life.

Physician and Psychiatrists in many cultures and countries have standards for doctor-patient relationships which include maintaining confidentiality. In some cases the physician-patient privilege is legally protected. These practices are in place to protect the dignity of patients, and to ensure that patients will feel free to reveal complete and accurate information required for them to receive the correct treatment.

Political Privacy

Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot is the simplest and most widespread measure to ensure that political views are not
known to anyone other than the voter themselves, it is nearly universal in modern democracy, and considered a basic right of citizenship. In fact even where other rights of privacy do not exist, this type of privacy very much exists.

Genetic Privacy

The concept of genetic privacy has only recently entered in our vocabulary. It is necessary in order to prevent genetic discrimination on the basis of apparent or perceived genetic abnormalities. A person may have some serious repercussions on the revelation of a particular genetic disorder, thus genetic privacy is very important.

Generally, Data privacy issues can arise in response to information from a wide range of sources such as financial transactions, biological information, such as genetic records etc., residential and geographic records, administrative records and policy matters, scientific information and records, security and strategic information.

Technological Means of Privacy Protection

With the recent development of commercially available technology based systems, privacy protection has also moved into the hands of individual users. Users of the Internet and of
some physical applications can employ a range to programs and system that provide varying degrees of privacy and security of communications. On the one hand technology is widely being misused for violation of privacy on the other hand the same technology provides means to protect one’s privacy. One of these technologies is digital signature.

All electronic documents can be signed digitally and once signed their secured communication on the Internet is guaranteed as the message gets encrypted. It can not be read in transit by any third party and only the addressee will be able to decipher it. Firewall, another network based technology, is frequently used by computer networks towards the attempts to breach the privacy of a network. A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

A firewall is a hardware and software combination used to create security checkpoints at the boundaries of private networks. Suppose, there is network of 50 computers, it must have one point from which the information comes in and goes out. At that point a firewall is the form of a checkpoint. It can block traffic to and from suspicious destinations.
The Right to Privacy, Encryption and Cryptography

The use of Internet has provided a new forum to express the views and concerns on a worldwide platform. The freedom to speak and communicate is the fact which demands state interference in public as well as national interest which immediately raises the debatable issue of right to privacy.

At the same time, it is common concern that liberty cannot thrive without certain restrictions put on them so that each individual in society can be best protected from intrusion by the others as well as state also.

It would therefore seen that a technology is required to legitimate utilization of the right to freedom of speech and expression and the right to have a private conversation without intrusion. For this, encryption may provide a practice tool. Since, the practice of encryption and its study that is known as ‘cryptography’ provides individuals with means of communication that no third party can understand unless specifically permitted by the communicators themselves.\textsuperscript{11}

The technique ‘Encryption’ is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. Therefore, this has the effect of ensuring total privacy even in open networks like the Internet. In process, encryption involves the use of secret codes and cipher to communicate information electronically from one person to another in such a way that the only person so communicating would know to use the codes and ciphers.\textsuperscript{12}

On the other side, the field of cryptography deals with the study of secret codes and cipher and the innovations that occur in the field. Cryptography is also defined as the art and the science of keeping messages secure.\textsuperscript{13}

In concern to the right to privacy, it is usually agreed upon that in most democratic countries there is existence of private and public spheres in every citizen’s life and that these two spheres are distinct and to be treated as separately.

Although, the line of demarcation is sometimes blurred and continues to be the subject of private as well as public importance such as pornography, public and personal security,

\textsuperscript{12} See, \textit{Daniel Bernstein v. United States}(Dept. of State), 922 F. Supp.1426( N. D. Cal.1996)

\textsuperscript{13} Jonathan Rosenoer, “Cryptography and Speech” at http://cyberlaw.com/1095.html
national security etc. In contrast the liberal democratic state has no power to interfere with the private aspect of its citizen’s lives.

There is also a common misconception that the right to privacy is merely a weapon to ensure confidentiality in human affairs. However, this does not reflect the correct and complete picture in the subject matter.

It is important to note that the right to confidentiality arises only after information regarding human transaction or affairs have reached to third parties.

It may be stated that privacy involves the right to control one’s personal information and how that information should be used and obtained which is sometimes to be referred as the right to “informational self determination”.¹⁴

With the onset of the Internet and e-commerce and the varying nature of the transaction carried out on the Internet are such that the right to privacy must extend at least to a limited extent.

At the same time, volume and the nature of transactions also raises the issue of various types of computer related crimes

e.g. distribution of sensitive information, e-mail scams, password attacks, I.P. Spoofing hacking, credit card frauds, alteration and destruction of digital information etc. which raises the issue of national security concerns as to the political, social and economic health of any country in the present scenario of global menace of terrorism and practice of on-line transactions.

**Techno-Legal Safeguards (Encryption)**

An encryption algorithm transforms a plaintext into an unreadable ciphered text (encryption) and vice versa decryption using a special key. The economics behind encryption is to transform the problem of keeping thousand of messages secret into the problem of keeping a single key secret.\(^\text{15}\) A useful distinction can be made between symmetric and asymmetric encryption algorithms. Symmetric algorithms use the same key for encryption and decryption and decryption. This means that communication parties have to agree on a secret key in advance the disadvantage is this they have to find a secure way to exchange this key. This is particularly cumbersome in an open environment with many participants that may not know each other beforehand. This disadvantage is avoided in asymmetric

\[\text{\textsuperscript{15} G. Aruna Kranthi, "Money in Electronic Age " Published in 'Cyber Space And The Law- Issues And Challenges' NALSAR University, Hyderabad Publication 2004, P.140}\]
encryption methods that use different keys for encryption and decryption. At present, encryption provides the most important tool to keep electronic communication and electronically stored documents confidential. Although new technologies will emerge sooner or later, it can be expected that encryption will remain the cornerstone for most confidentiality services on open network for the foreseeable future. Encryption has a long tradition in the defense area. However, encryption technologies are increasingly integrated into commercial systems and applications.

The above examples already show that the exclusive character of encryption belongs to the past. They also show that increasingly encryption technology is integrated into products primarily to protect, for example, intellectual property rights or to avoid fraud. Moreover, the fast growth of the Internet will create a fundamental change in the use of encryption, it will become an integral part of personal and business computing. Computer stores sell cryptography product and more and more people simply download encryption software from the Internet which can be easily installed on a normal computer system. The integration of complete cipher machines on smart cards is a

16 Ibid.
17 Digital Mobile Telephones enjoy stronger protection, uses encryption. Pay-TV & DVD also uses encryption.
reality. Computer System could be delivered with standardized smart card readers and fast crypto-chips. Various universities in the world teach cryptology and hundreds of companies in Europe and even more worldwide develop, produce and sell products and systems to be used for encryption.

Electronic commerce and many other applications of the information society will only expand and unfold their economic and social benefits if confidentiality can be assured in a user-friendly and cost-efficient way. Cryptographic technologies are flexible, support a wide range of applications and minimize transaction costs on open networks. Continuous progress in digital technologies will make computing crypto-algorithms even more cost-efficient. European companies have developed substantial capabilities to integrate high-quality cryptographic features into their products and services. As demand for products with encryption is now growing very fast worldwide, it provides substantial opportunities for the industry and job

---

18 When using services such as tele-shopping or tele-banking, the consumer needs to be ensured that personal data such as credit card numbers are kept confidential.

- Data protection laws require safeguards like encryption to ensure privacy.
- In storing select secret data and in carrying out sensitive business communication (project details, bidding information, research results, etc.) over open networks, companies wise to be protected against industrial espionage.
- Health care tele-matic applications must not allow for disclosure of medical histories of patients to unauthorized persons.
creation in Europe. Furthermore, the application of cryptographic products and services will have an enabling effect in all sectors of economic and social activity. Without this wide scale deployment, the ability to create new, more competitive forms of business and new forms of social interaction will be substantially inhibited.

International treaties, Constitutions and laws guarantee the fundamental right to privacy including secrecy of communications. Consequently in the current shift from offline to on-line information flows, the public needs to have access to technical tools allowing effective protection of the confidentiality of data and communication against arbitrary intrusions. Encryption of data is very often the only effective and cost-efficient way of meeting these requirements. Therefore, the discussion about the prohibition or limitation of the use of encryption directly affects the right to privacy, its effective exercise and the harmonization of data protection laws in the effective implementation.

---

Regulation of Encryption: Some Comparative Positions

Concerns over foreign threats to national security have been the primary motive for regulation and control. Whilst countries want to protect their own military and diplomatic communication through encryption, the objective of control is precisely to deny similar benefits of cryptography to foreign opponents, in particular if they do not have equivalent technical means. Therefore, regulation and control mechanisms are in general designed to prevent international proliferation of certain encryption technologies.

Law enforcement authorities and national security agencies are concerned that wide-spread use of encrypted communication will diminish their capacity to fight against crime or prevent criminal and terrorist activities. For this reason, in several member states consideration is being given to how their encryption policy could develop in the future. This has led to national and international discussions about the need, technical possibilities, effectiveness proportionality and privacy implications of such a regulation.\(^{20}\)

---

\(^{20}\) Existing regulation within the European Union and the OECD, Whist export control measures are internationally widely applied, up to now, domestic control of encryption is quite exceptional. In fact, currently only one Member State of The European Union (France), applies a comprehensive cryptographic regulation (Loi N° 90-1170 of 29.12.90, JORF 30.12.90; Decret N° 92-1358, 28.12.92, JORF 30.12.92;
Regulation of use would mean to rule the use of encryption without an authorization as illegal. Alternatively or additionally, supply and control of encryption products and services could be brought under an authorization scheme. Authorization would either be denied or granted under certain conditions, for instance to use only weak encryption or to sell approved software. These conditions are scaleable to satisfy any perceived needs of law enforcement and national security agencies. Such regulations could limit the use of encryption. In addition, divergence between regulatory schemes might result in obstacles to the functioning of the regulatory mechanism in particular for the free circulation of encryption. Today, nobody can be totally prevented from encrypting data.

Delivery, exportation and use of cryptography are subject to previous declaration if the cryptography can have no other object than authenticating communications or assuring the integrity or transmitted messages, and previous authorization by the prime minister in all other cases. This law is currently being modified. Although there have been discussions in other Member States, only the United Kingdom has so far launched a Public Consulation on regulation of TTPs for the provision of encryption services (but not for use of encryption) [ Licensing of TTPs for the provision of encryption services-DTI Public Consultation Paper on detailed proposals for legislation. 3.1997]

21 If any encryption software company which can freely develop its products in its home country, must comply with specific technical or legal requirements in other Member States, this company has to produce at least two, if not more, different versions of its encryption software. The same situation occurs if enterprises want to offer cross-border encryption services.

22 Criminals or terrorists can also use encryption for their activities. Most of the criminal cases involving encryption that are quoted as examples for the need of regulation concern “professional” use of encryption. It seems unlikely that in such
Firstly, because the access to encryption software is relatively easy, for instance by simply downloading it from the Internet.

Secondly, it is difficult to prove that a specific person has sent an unauthorized encrypted message. Electronic communication on open network is not like an end-to-end telephone conversation where people can be identified for instance by their voice.

Thirdly, encryption is also possible using steganographic methods. These methods allow one to hide a message in other data (e.g. images) in such a way that even the existence of a secret message and thus the use of encryption cannot be detected. As a result, restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies.

The Legal Accession to Encryption Keys underlying principle of this approach is to require that products and service incorporating encryption allow access to the respective keys. In cases the use of encryption could be effectively controlled by regulation; see also “Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism” by DE Denning and W.E Baugh,Jr.
This would permit regulating agencies to decrypt a ciphered text otherwise difficult or impossible to crack. Different technical and institutional ways to provide key access are being discussed. The two most know concepts are *key escrow* and *key recovery*. Broadly speaking, these concept imply that copies (*escrow concept*) or information (*recovery concept*) about relevant keys are give either directly to regulating agencies or to Trusted Third Parties (TTPs).

(1) Key access schemes are considered by law enforcement agencies as a possible solution, to cope with issues like encrypted messages. However these schemes and associated TTPs raise a number of critical question that would need to be carefully addressed before introducing them.23

---

23 The ongoing discussion of different legislative initiatives in the US is an illustrative example of the implied controversy. The most critical points are vulnerability, privacy, costs and effectiveness:

- Inevitably, any key access scheme introduces additional ways to break into a cryptographic system (See for a comprehensive analysis the recently published study “The Risks of Key Recovery, Key: escrow, and Trusted Third Party Encryption”). More people will know about “secret keys” and “system designs” leading to higher risks of insider abuse and the TTPs itself can become target for attacks.
- These new vulnerabilities are complex and need to be understood as substantial liability and privacy questions are implied. The costs associated with key access schemes can be very high. Up to now, questions on costs and who would bear them have not been addressed by policymakers. Important cost factors would be the specific requirements put on TTPs, e.g. response time to deliver keys, storage time for session keys, authenticate...
Furthermore substantial and unknown costs would occur through the need for scaleability of key access schemes i.e. making it work in a multi million user environment. Up to now, such systems have at best been developed for small scale use.\footnote{The costs to make them work on an economy of even global wide scale need to be looked at carefully.}

(2) Any involvement of a third party in confidential communication increases its vulnerability. The main reason for involving a third party in the management of keys for confidentiality is to allow that party to make the keys available to other than the two communicating parties, for example, to law enforcement. Users may therefore not see many advantages requesting government agency, secure transfer of recovered keys, internal security safeguards, etc.

- Key access schemes can be easily circumvented—even if, hypothetically speaking, everyone would be forced to pass through these systems.
- Users could first encrypt the data with an unrecoverable key and later use a licensed escrowed encryption system. Unless encryption as such is forbidden, this would even be legal. Anyhow, such an operation could only be detected when an agency actually tries to decrypt the data. It is impossible to “scan” the network to detect the use of non-escrowed encryption. Therefore, use of non-escrowed encryption would not even be able to act as a general indicator for possible illegal activities.
- Users could encrypt a relatively large number of session keys in a way that the previous key encrypts the next one, always using one or several official escrow/recovery systems. Only the last key would be used to encrypt the message. An agency would need to reverse this process and to obtain all keys in order to read the message; although technically feasible, this task would be extremely difficult to manage. To be noted, the uses would have fully complied to a key recovery scheme.
in using TTPs for confidential communication, and probably not even for stored information. Regulators would thus need to offer incentives to convince user to use licensed TTPs for confidentiality purposes, for instance through a "public security label" or even by introducing a "mandatory scheme".25

Privacy considerations suggested not limiting the use of cryptography as a means to ensure data security and confidentiality. The fundamental right of privacy has to be ensured, but may be restricted for other legitimate reasons, such as safeguarding national security or combating crime, if these restrictions are appropriate, effective, necessary and proportionate in order to achieve these other objectives. The EU Data Protection directive harmonizes the conditions under which access to personal data, their processing and transfer to third countries is lawful.26

Cryptography is one important technical means by which data integrity and their confidentiality can be ensured. To ensure also the secured flow of personal data throughout the regulation,

---

25 Supra, note 15, P.145
26 As regards data security the Directive requires Member States to provide that a data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
such technical means must be able to “travel” with the personal information they are securing. Any regulation hindering the use of encryption products and services throughout the regulation and control system thus hinders the secure and free flow of personal information and the provision of related goods and services.

Encryption and Cryptography: A Comparative View

Proposals for regulation of encryption have generated considerable controversy. Industries express major concerns about encryption regulation, including key escrow and key recovery schemes. Although there is a lack of experience, as electronic communication and society, a preliminary examination and assessment can be made in order to build a common understanding of the subject, in particular as member states may have different views on security issues implied. Such an understanding could be founded on the following points:

Problems caused by encryption to crime investigation and the finding of evidence are currently limited, but they may increase in the future. As with any new technology, there will be abuse of encryption and criminal investigations will be hindered

---

because data was encrypted. However, widespread availability of encryption can also prevent crime. At present, the damage caused by electronic crime (e-crime) is estimated in the order of billions of dollars industrial espionage, credit card fraud, toll fraud on cellular telephone, piracy on pay-television encryption. Criminal cannot be entirely prevented from having access to strong encryption and from bypassing escrowed encryption. Benefits of regulation for crime fighting are therefore not easy to assess and often expressed in a fairly general language. However, control measures could make use of encryption for criminal activities more difficult and cumbersome.

In the information society, citizens and companies will increasingly carry out more aspects of their lives and business on-line through tele-conferencing, tele-shopping, tele-working, electronic payment, e-mail, etc. A huge amount of information will be available electronically, in a way never experienced before. Therefore, if citizen and companies have to fear that their communication and transaction are monitored with the help of key access or similar schemes unduly enlarging the general surveillance possibility of regulating agencies, they may
prefer remaining in the anonymous offline world and electronic commerce will just not happen.²⁸

Key escrow-or key recovery raises a number of practical and complex questions that policy makers would need to solve in particular issues of privacy vulnerability, effectiveness and expenses if at all required, regulation should be limited to what is absolutely necessary. Regulation would also need to distinguish between a multitude of possible key types (storage keys, session keys, authentication keys etc.) as there are important differences in their use.

Cryptography in India: The Information Technology Act, 2000

The use of cryptography and encryption in India is a relatively new phenomenon. The use of technology in itself, for the purposes of communication, has begun only over the last few years in India. The use of the Internet is a phenomenon of the mid-90s.

According to a recent report²⁹, in India, there are very few companies involved in the development of tools for

cryptography. Further, cryptography remains, by and large, within the domain of the defence sector. It was only as late as 1995 that India introduced a list of items that required licensing before export. The list only included encryption software for telemetry systems in specific and did not relate to encryption software in general.

Under a recent agreement between India and US, the former has agreed to facilitate the import of items listed on the US Munitions List (USML)\textsuperscript{30}. This, as we have seen earlier, might require specific licensing both for exports and imports.

The Information Technology Act, 2000 introduced some form of control over the use of encryption for communication in India.\textsuperscript{31}

The Act takes into consideration the system of ‘key-pair encryption’ for the recording and authentication of digital signatures. The Act provides specifically, that the public key is to be deposited with a certifying authority.

\textsuperscript{30} The List reads as “Cryptographic systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems” 22 U. S. C. 2278 (a) (1).
\textsuperscript{31} See, Chapter III, IV and V of The I T Act, 2000
Section 69 of the Information Technology Act, 2000 deals with this problem. This Section provides the Controller of Certifying Authorities with the power to intercept any transmission if certain criteria are satisfied. One such criterion provided for is the security of the state and concerns about the sovereignty and integrity of the nation. In such a case, the subscriber is under an obligation to decrypt the information for the authority. The viability of this provision however, remains questionable. The section provides that the controller can call upon any subscriber to decrypt a message in the event of requirement. Thus, in the absence of any non co-operation from the subscriber, even the controller cannot directly intercept and decrypt a message, since he is only a repository of the public keys and not of the authority is made punishable under the

Section 69 of the Information Technology Act, 2000 reads as under:

Directions of Controller to a subscriber to extend facilities to decrypt information.-

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section(1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.
section. Thus, it is only for encrypted messages. Since, the controller cannot directly decrypt messages the right to privacy is still protected to a large extent.

It will be seen that complete discretion is vested with the controller to determine whether a condition has arisen where a transmission may be intercepted in the interest of national security. The right to an encrypted transmission may be viewed as integral to the right to privacy flowing from article 21 of the Constitution. In such a case, the right can only be curbed by a "procedure established by law." It is now well settled that such a procedure must be right, just fair and reasonable to be valid.

One cannot deny that there arise exceptional circumstances when transmissions need to be intercepted to prevent anti-national activities. But such circumstances cannot be abused to further political vendetta. On a plain reading of section 69, it may be concluded that the procedure is not adequate as it leaves complete discretion in the hands of the controller. The wording, it may be pointed out, is similar to that of the Telegraph Act, 1885, that came up for discussion in the P.U.C.L. Case\textsuperscript{33}. If one follows the ruling in that case, it may be

\textsuperscript{33} P.U.C.L. V. Union of India (1997) 1 SCC 318
said that inadequate procedural safeguards would render the section inapplicable.

Further, considering the fact that the section also provides for punishment in the event of non-compliance, it is imperative that stronger safeguards be built into the system. Thus, the question as to what constitutes a security threat or when the friendly relations are being threatened should not be left to the sole discretion of the controller, but must emanate from the legislature. In the alternative, the controller should frame specific regulations under Section 89, laying down specific criteria as to when the security of the nation is being threatened and the like. In the absence of such measures, the provision in Section 69 can be said to be an infringement of the right to privacy in view of Article 21 and, consequently, unconstitutional and void *ab initio*.\(^{34}\)

As in the case of any issue affecting constitutional rights, the validity, or alternatively, the invalidity, of restrictions on the practice of cryptography and encryption remains mere speculation. True, the right to privacy is recognized as inherent in the right to life with dignity in Article 21 and the right to freedom of speech and expression in Article 19. Neither of these

---

can and should be allowed to stand as an impediment in curbing activities prejudicial to national security and interests. Not surprisingly, both these rights contain express conditions when they may be deprived.\(^{35}\)

At the same time, the balance cannot be allowed to till completely to one side, so as to negate the basic liberties, even when not absolutely essential. The only way out is a compromise between the two extremes. While the restrictions on cryptography and encryption may be abused for several illegitimate purposes, so also the freedom is liable to be misused for anti-national activities. The solution lies neither in absolute freedom nor unwarranted state control.\(^{36}\)

A possible solution to the problem may lie in the technology that encryption uses. The problem has to be looked at, at a two-fold level. At one level, the issue is of encryption and cryptography as a mode of free speech and at the other, is the more important issue of cryptography as an integral part of the right to privacy. While the former may be subject to reasonable restrictions, the second may be restricted only by a procedure established by law.

\(^{35}\) Ibid.
\(^{36}\) Ibid.
With regard to the issue of free speech, it would be only reasonable to adopt the standard applied by the courts in permitting restrictions on other modes of expression. Cryptographic studies should therefore be dealt with as any ordinary publication and restraints on the same should be allowed only in so far as Article 19(2) of the Constitution of India permits them. With regard to the issue of privacy and the deprivation of the same by a procedure established by law, the answer lies in a strong and comprehensive set of safeguards to ensure that state interference is permitted only when absolutely essential.\textsuperscript{37}

It may not be unreasonable to build procedural safeguards into the existing IT Act, 2000. Such safeguards would have to include procedures for declaring when an issue involving national security concerns has arisen and on what concerned authority should be allowed to intercept encrypted information and be permitted to decrypt the same. Such a proclamation is not to be invoked at the absolute discretion of the authority; it will have to be made by the concerned legislature.

Further, by making such a proclamation, a provision could also be made to provide that for the period of the emergency or

\textsuperscript{37} Id. p.392
security concern, encryption should be avoided. In spite of this, if encryption is carried on, the government should have the authority to intercept the same. This would have the dual effect of avoiding unnecessary breaches of privacy and also reduce the task of the government in intercepting and maintaining records substantially.\textsuperscript{38}

Moreover, in addition to a general invasion of privacy possible through the process set forth above, it may also be necessary, as mentioned earlier, to intercept the messages of specific individuals, even when an actual emergency is not proclaimed. In such a scenario, it would be both unreasonable and impractical to require a proclamation by the legislature. However, here too, the circumstances necessitating the invasion will have to be clearly set forth by the relevant authority and the procedural guidelines as to maintenance and destruction of intercepted message will have to be adhered to. While this would give the authority concerned the power to single out an individual, it nevertheless will still be subject to review by an advisory board, as laid down in the \textit{P.U.C.L.} Case\textsuperscript{39} and later, if necessary, by the judiciary, arbitrary action would be reduced. Another alternative might be the process of prior judicial

\textsuperscript{38} \textit{Ibid.} \\
\textsuperscript{39} \textit{Supra}, note 33
permission, before the actual passing of the order. However, this approach has several practical problems and may not be appropriate, when action needs to be taken immediately.

When an interception is to take place, the same will have to be done with certain specific guidelines. Detailed records and copies of the intercepted messages should be kept and destroyed once the proclamation is no longer in force. The cryptographic keys obtained should be similarly deleted from government resources to ensure that authorities can no longer use them to intercept messages, in the absence of any emergency.

It is true that no procedure is completely foolproof and without loopholes, the procedure outline above gives individuals the choice to avoid the usage of encryption for a specific period and, thereby, avoid any breach of their privacy. While the executive should work out the exact nature of the guidelines and procedures, the aforesaid scheme may provide a starting point to develop the mechanism of control and regulation to protect the privacy and confidentiality.

However, it has to be contemplated in a true democratic set up where liberties of individuals are supreme to function, mere legislative protections in the absence of a strong political will, would be futile. Therefore it is submitted that the legal
infrastructure should be developed and enlarged without any delay with the changes introduced by new technological innovations in the electronic transactions and the system of e-governance.