First Analysis of the Personal Data protection Law in India

Final Report

PREPARED BY:

CRID – University of Namur

TABLE OF CONTENT

I. Introduction ........................................................................................................ 5

II. Methodology ...................................................................................................... 6
   1. General remarks ............................................................................................ 6
   2. Principal assessment criteria ....................................................................... 6
      2.1. Legal criteria .......................................................................................... 6
      2.2. Methodological criteria .......................................................................... 7

III. Overview of the Indian Outsourcing business .............................................. 7

IV. Context of India’s data protection regime ...................................................... 9
   1. Federal structure .......................................................................................... 9
   2. Constitution ................................................................................................. 11
      2.1. Background and structure .................................................................... 11
      2.2. The Preamble ......................................................................................... 11
      2.3. The Amendment and the Basic Structure doctrine .............................. 12
      2.4. The separation of powers ................................................................. 15
      2.5. Judicial Review in India ....................................................................... 16
   3. Judicial system ............................................................................................... 16
      3.1. The Supreme Court ............................................................................... 16
      3.2. The High Courts .................................................................................. 18
      3.3. The Lower Courts ................................................................................ 18
      3.4. The Judicial independence ................................................................. 18
   4. Administrative tribunals system .................................................................. 19
   5. Competence to legislate on data protection .................................................. 20
   6. Influence of international norms ................................................................. 21
   7. General legal protection for Human Rights ............................................... 23

V. Data Protection Legislation ............................................................................. 24
   1. Introduction ................................................................................................. 24
   2. The Right to Privacy in India ...................................................................... 25
      2.1 Before the Constitution .......................................................................... 25
      2.2. The Right to Privacy in the Constitution ............................................. 26
      2.3. Judicial developments ......................................................................... 26
   3. Statutory Safeguards of Privacy and data protection interest outside data
      protection legislation .................................................................................. 30
      3.1. The Information Technology Act, 2000 .............................................. 30
      3.1.1. Background .................................................................................... 30
      3.1.2. Principles and definitions ............................................................... 30
      3.1.2.1. No such concept of “personal data” .............................................. 30
      3.1.2.2. Provisions regarded as providing rules pertaining to data protection... 31
         a) Section 43. Penalty for damage to computer, computer system, etc ........ 31
         b) Section 65. Tampering with computer source documents ..................... 31
         c) Section 66. Hacking with Computer System ....................................... 32
         d) Section 72. Penalty for breach of confidentiality and privacy .............. 32
      3.1.3. The Amendments to the IT Act....................................................... 33
      3.1.3.1. Introduction ............................................................................... 33
3.1.3.2. The full text of aforesaid amendments

a) Section 43. Compensation for damage to computer, computer system, etc.
b) Section 66. Computer related offences
c) Section 72. Breach of confidentiality and privacy

3.1.4. Content Principles

3.1.4.1. Principle of purpose limitation
3.1.4.2. Principle of data quality and proportionality
   a) Definition
   b) Accurate and up-to-date data
3.1.4.3. Adequate, relevant and not excessive data
3.1.4.4. Principle of security
   a) Definition
   b) Security in the IT Act
3.1.4.5. The Rights of Access, Rectification and Opposition
3.1.4.6. The Principle of Restriction on Onward Transfers
3.1.4.7. Additional principles
   a) Direct marketing
   b) Sensitive data

3.1.5. Enforcement mechanisms

3.1.5.1. Introduction
3.1.5.2. The Adjudicating Officer
3.1.5.3. Presiding Officer of the Cyber Regulations Appellate Tribunal
3.1.5.4. The National Association of Software and Service companies (NASSCOM)

3.2. The Indian Contract Act, 1872

3.3. The Credit Information Companies (Regulation) Act, 2005

3.3.1. Scope of regulated “data processors”
3.3.2. Scope of regulated information
3.3.3. Provisions pertaining to data protection in this Act
3.3.4. Regulations made under Section 20(f)
3.3.5. Regulations made by the Reserve Bank in exercise of the powers conferred by Section 37(2) of the Credit Information Companies (Regulation) Act, 2005

3.3.5.1. Introduction – General concepts
3.3.5.2. Privacy Principles
   a) Principle 1. Care in Collection of Credit Information
   b) Principle 2. Data Security and secrecy
   c) Principle 3. Access and Modification
   d) Principle 4. Data Collection Limitation
   e) Principle 5. Data Use Limitation
   f) Principle 6. Data Accuracy
   g) Principle 7. Archiving/Length of Preservation
   h) Section 16 Solicitation of personal data from individual concerned
   i) Section 19. Remedies to individuals
   j) Section 18. Procedure to be adopted
3.3.5.3. Regulations made by the Government in exercise of the powers conferred by Section 36 of the Credit Information Companies (Regulation) Act, 2005
a) Chapter III. Steps and security safeguards to be taken by credit institution for ensuring accuracy, completeness and protection of data…………………………………………………………………………………………57
b) Chapter IV. Steps and security safeguards to be taken by credit information companies and, specified user for ensuring accuracy, completeness and protection of data……………………………………………………………………………………………….61
c) Chapter V. Prohibition from unauthorised access or use or disclosure……66
d) Chapter VI Fidelity and secrecy……………………………………………………67
3.4. The Public Financial Institutions Act of 1993……………………………………68
3.5. The Indian Telegraph Act…………………………………………………………68
3.6. Common Law……………………………………………………………………69
4. Procedural/ Enforcement Mechanisms…………………………………………………69
4.1. Absence of any Data Protection Authority in India……………………………..69
4.2. Specific Relief Act……………………………………………………………………70
5. Industry codes of practice…………………………………………………………70
Conclusion………………………………………………………………………………70
I. Introduction

This report was prepared upon request of the Commission of the European Communities, Directorate-General for Justice, Freedom and Security. It presents the views of the contractors who performed the analysis and does not necessarily represent the views of the Commission.

The basic aim of the report is to provide the Commission with information on the Personal Data Protection Law in India that will enable a proper determination of whether a second step – adequate protection analysis – has to be undertaken.

Article 25 of Directive 95/46/EC\(^1\) regulates the transfer of personal data from Member States of the European Union (EU) to “third countries” – i.e., countries outside the EU (and EEA). According to Art. 25(1), transfer of personal data “may take place only if ... the third country in question ensures an adequate level of protection”. The essential concern of the Directive on this point is to ensure that data relating to European citizens and residents\(^2\) remain subject to safeguards when transferred out of the EU (and EEA). The adequacy of protection “shall be assessed in the light of all the circumstances surrounding a data transfer or set of data transfer operations ...” (Art. 25(2)).

The European Commission has the power to make determinations of adequacy which are binding on EU (and EEA) Member States (Art 25(6))\(^3\). Positive determinations of adequacy have hitherto been made for Hungary\(^4\), Switzerland\(^5\), Canada\(^6\), Argentina\(^7\) and the United States' (US) “safe harbour” scheme\(^8\).

---


2 Note, though, that applicability of the provisions of the Directive does not turn on the nationality or official place of residence of a data subject

3 The Commission does not make such decisions on its own but with input from: (i) the Data Protection Working Party established pursuant to Art. 29 of the Directive (which may deliver a non-binding opinion on the proposed decision (Art. 30(1)(a) & (b))); (ii) the Committee of Member State representatives set up under Art. 31 of the Directive (which must approve the proposed decision and which may refer the matter to the Council for final determination (Art 31(2)); and (iii) the European Parliament (which is able to check whether the Commission has properly used its powers). The procedure follows the ground rules contained in Council Decision 1999/468/EC of 28.6.1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ L 184, 17.7.1999, p. 23 et seq.).


II. METHODOLOGY

1. General remarks

The Directive sets out criteria for assessing adequacy. Article 25(2) states that adequacy shall be assessed in the light of all circumstances surrounding a data transfer operation. Consideration must be given to the nature of the data, and the purpose and duration of the proposed processing operations. The rules of law in general and in specific sectors must be analysed. The content of the rules applicable and the means for ensuring their effective application must be also considered.

When assessing the content of applicable rules, account must not only be taken of formal legal rules and formal oversight mechanisms rooted in legislation. Indeed, other means can contribute to ensure an adequate level of data protection as for example professional rules and security measures which are complied with in India. The directive therefore requires that account be taken of non-legal rules that may be in force in the third country in question, provided that these rules are complied with.

Moreover, the way in which a regime functions (including, of course, the extent to which “law in books” equates with “law in practice”) will be tied not just to the rules found in both “hard” and “soft law” instruments but also to a myriad of relatively informal customs and attitudes which prevail in the country concerned – e.g., the extent to which the country’s administrative and corporate cultures are imbued with a respect for authority or respect for “fair information” principles.

At the same time, the customs, attitudes and other informal elements of the regulatory culture pertaining to data protection in India are difficult to ascertain accurately. Little academic analysis appears to have been conducted on these matters, and other empirical data are scarce.

2. Principal assessment criteria

2.1. Legal criteria

The principal legal criteria for assessing India's data protection regime are the rules in Directive 95/46/EC as construed and applied by the European Court of Justice (ECJ). There are as yet no decisions of the ECJ interpreting the concept of ‘adequacy’.

---

2.2. Methodological criteria

The principle methodological criteria for assessing India's data protection regime are set out by the Article 29 Data Protection Working Party in its document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12 5025/98)\(^\text{11}\). While the core criteria suggested by the Working Party do not have any legal standing, they are the considered view of Europe’s data protection authorities as to what constitutes ‘adequacy’, and are derived from the Working Party’s assessment of the most important requirements of Directive 95/46/EC and other international data protection texts.

The headings of the core criteria suggested by the Working Party are as follows:

1. Content Principles
   - Purpose limitation
   - Data quality and proportionality
   - Transparency
   - Security
   - Rights of access, rectification and opposition
   - Restrictions on onward transfers
   - Additional principles in appropriate types of processing, such as those concerning (i) sensitive data, (ii) direct marketing and (iii) automated decisions

2. Procedural/enforcement mechanisms
   - Delivery of a good level of compliance
   - Support to individual data subjects
   - Provision of appropriate redress to the injured parties

In this Report these criteria are used as a guide to the most important factors comprising the adequacy of any legislation or other scheme.

III. Overview of the Indian Outsourcing business

Those last years, India became a leading market in outsourcing, processing data from all over the world for companies which are most of the time established in Western countries (the United States are the first client of the Indian market followed by the European Community, particularly UK).
India played a key role in the management of the millennium bug where a large part of the work was outsourced in India. At that time, India began to appear as a leading country in the computer industry. In the late 1990s, as the software market boomed in the US, many companies outsourced their software needs to India.

---

\(^{11}\) See also European Commission, Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data (Luxembourg: Office for Official Publications of the EC, 1998).
Nowadays, the main concern of companies is to cut cost and a mere way to achieve this is to outsource part of their activities to third countries where the workforce is cheaper. India has a leading position in this industry.

According to NASSCOM\(^\text{12}\), the main reasons behind India’s success in the outsourcing industry are:

- Abundant, skilled, English-speaking manpower. India is one of the largest English speaking countries in the world, what is of first importance notably for the call centres. This advantages India that must face competition of other non English speaking emerging markets as China, Russia and Brazil.

- The high number of available graduates is also a big advantage, in 2001, India had 2.000.000 university graduates, China only had 950.000\(^\text{13}\). The educational system in India enhances this advantage : the educational system has a good general level and emphasizes on mathematics and science which contributes to a better understanding of the computer logic. Private schools offering specialisation in programming and computer language courses are encouraged by the Government. This leads to a large number of students ready to work in these blooming sectors with - as a prime example for them to follow- the tremendous success of the Indian programmers in the Silicon Valley acting as an incentive upon which these new vocations thrive.

- Improving telecom and other infrastructures in order to be up to par with global standards. Since India had no software legacy, investments in brand new technologies were made possible allowing for a better specialisation and the development of new technologies that were not yet company-owned. In this regard, outsourcing has been an efficient way to cut costs and to improve services in comparison with the prospects offered by their own enterprises.

- Strong quality orientation among players and their focus on measuring and monitoring quality targets.

- Fast turnaround times and the ability to offer 24x4 services based on the country’s unique geographic location that allows for leveraging time zone differences.

- Proactive and positive environment policy which encourages ITES/BPO investments and simplifies rules and procedures. A friendly tax structure, which places the ITES/BPO industry on par with IT services companies. Last, the government, aware of the opportunities offered by the outsourcing business, has fostered the companies by creating Software Technology Parks and allowing tax exemptions on all exports and duty free hardware imports\(^\text{14}\).

The outsourcing business is of first importance for the Indian economy: The ITES-BPO industry generated total revenues of US$ 3.9 billion in 2003-04, representing a growth of


\(^{14}\) B. NAMBIAR, IT outsourcing and India, p. 10
around 45.3 percent over the previous year. The sector was expected to reach revenues of around US$ 5.7 billion by the end of 2004-05, at a growth rate of 44.4 percent\textsuperscript{15}.

Regardless of these promising perspectives, India in its immediate surroundings has a problem to tackle: namely the bad reputation outsourcing has earned abroad. Consequently, under public pressure, foreign public authorities decided not to outsource their activities. Nevertheless, companies who are enticed by cost cuts will probably continue to outsource which leads to believe that this trend is far from over. India, on its side, will certainly continue to propose attractive incentives and protection against potential obstacles in order to favour the activity.

Therefore, the adoption of data protection legislation could be helpful in India.

Indeed, if people’s first preoccupation was the job losses, nowadays, the consumers – American and European- are concerned by the data security\textsuperscript{16}. Some cases of data thefts (credit cards numbers, etc.) have highlighted the risk of outsourcing in countries that are not yet equipped with comprehensive data protection legislation. In response to the consumers’ fears, some American States considered the possibility of banning the outsourcing of data concerning particular domains (such as medical, financial or personal information)\textsuperscript{17}.

The compliance with European standards would facilitate outsourcing from Europe and reassure Western consumers on the European market as well as other partners.

In the face of an ever stronger competition, notably with the emergence of the West Balkan countries and China as major players, India has shown relentless will in setting up the best legal and economic environment possible, coupled with quality infrastructures.

For the purpose of this report, the importance of the outsourcing business in India must certainly be taken in consideration given the quantity of processed data that can potentially increase the degree of risk that a transfer could pose for data-subjects.

**IV. Context of India’s data protection regime**

**1. Federal structure**

India is an Union of States subdivided in twenty-eight States\textsuperscript{18}, six Union Territories\textsuperscript{19} and the National Capital Territory of Delhi.

\textsuperscript{15} Indian ITES-BPO Trends (2003-04), available on http://www.nasscom.org/artdisplay.asp?cat_id=800


\textsuperscript{17} S. RAI, « Software Success Has India Worried », New York Times, February 13, 2003, available on http://64.233.179.104/search?q=cache:mAYkDBs0hd0J.leitl.org/tt/msg15197.html+%22software+success+has+india+worried%22+saritha+rai&hl=fr&gl=be&ct=clnk&cd=1

\textsuperscript{18} Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Goa, Gujarat, Haryana, Himachal Pradesh, Jammu and Kashmir, Jharkhand, Karnataka, Kerala, Madhya Pradesh, Maharashtra, Manipur, Meghalaya, Mizoram, Nagaland, Orissa, Punjab, Rajasthan, Sikkim, Tamil Nadu, Tripura, Uttarakhand, Uttar Pradesh, West Bengal
India has a federal structure: the Constitution assigns certain statutory powers to the States. Until the 1990s, the devolution of powers was only made to States without any further decentralization, which, given the importance of each State in terms of population, was more characteristic of a centralized State. In the 1990s, the devolution of powers was made to both States and sub-state government bodies although all residuary powers were still reserved to the Center.

At the federal level, the executive power is exercised by the President and the Council of Ministers charged to aid and advise the President. The President’s role is mainly ceremonial and the Council of Ministers, led by the Prime Minister, is in charge of the real national executive power, but must always act in the name of the President. The Council of Ministers is collectively responsible to the Lok Sabha.

India has a bicameral Parliament, which consists of the Rajya Sabha (Council of States) and the Lok Sabha (House of People). The legislative power in India is separated into three lists: the Union list containing subjects on which only the Union Parliament can legislate, the State list, containing all matters on which the States Legislatures have an exclusive competence and the Concurrent list which contains points on which both Union and State Legislatures can take laws. It is noteworthy to mention that Union laws take precedence over States laws.

The States have more or less the same organisation as the one existing within the Union: the governor is the head of the executive power and is helped in his task by the Council of Ministers.

---

19 Andaman and Nicobar Islands, Chandigarh, Dadra and Nagar Haveli, Daman and Diu, Lakshadweep and Pondicherry


22 Article 73 of the Constitution: “73. Extent of executive power of the Union.— (1) Subject to the provisions of this Constitution, the executive power of the Union shall extend—

(a) to the matters with respect to which Parliament has power to make laws; and

(b) to the exercise of such rights, authority and jurisdiction as are exercisable by the Government of India by virtue of any treaty or agreement:

Provided that the executive power referred to in sub-clause (a) shall not, save as expressly provided in this Constitution or in any law made by Parliament, extend in any State to matters with respect to which the Legislature of the State has also power to make laws.

(2) Until otherwise provided by Parliament, a State and any officer or authority of a State may, notwithstanding anything in this article, continue to exercise in matters with respect to which Parliament has power to make laws for that State such executive power or functions as the State or officer or authority thereof could exercise immediately before the commencement of this Constitution.

23 Article 77 of the Constitution

24 Its composition is the following one: 12 Members are nominated by the President and the other Members (238 maximum) are the representatives of the States and Union Territories.

25 Its composition is the following one: A maximum of 530 Members are directly elected and 20 other Members (this is a maximum) represent the Union Territories.”
Ministers. As for the President at the federal level, the governor has a minor political role at the State level. The Chief Minister, who exercises the effective executive power, leads the Council, and is responsible in front of the Legislative Assembly of the State. The number of Houses depends on each State, some have only one House (the Legislative Assembly), others may have a second House (the Legislative Council).

The States are divided into districts of various size and population. The district collector is the main officer of the district, he heads the district revenue department and coordinates the other departments. Districts are also divided into areas named *taluqs* or *teshils*. At that level, the prominent officer is the *taluqdar* or *teshildar*, whose role is similar to the district collector.

2. Constitution

2.1. Background and structure

The Constitution of the Republic of India was passed on November 26th, 1949. It was adopted after two and a half years of deliberation by the Constituent Assembly and was inspired by different Western Constitutions, mainly the British one. Evidently, the Indian government is rooted in the Westminster system, the lawmaking procedure and the idea of single citizenship has derived inspiration from the British model.

This written Constitution aims to establish - at both Union and State levels - the main organs of the Executive, Legislative and Judiciary powers. It defines the powers of each and acknowledges a separation of powers. The Constitution is divided into twenty-two parts. Several schedules have been added by amendment, notably the seventh schedule containing the three lists dividing legislative powers between the Union and the States.

2.2. The Preamble

In its preamble, the Constitution defines India as a Sovereign, Socialist, Secular, Democratic Republic.

For a long time, the Supreme Court considered the preamble as exterior to the Constitution but it is no longer the case.

In Berubari Union, delivering the unanimous opinion of the Court, Justice Gajendragadkar held that, although the preamble may be recognized as a useful lever in which one may find the original intent of the founders of the Constitution and may help explain even further the general purpose through which the various provisions were made, it is nonetheless to be considered as not being part of the Constitution. He further went on to observe that the preamble per se does not constitute a source of power nor can it impose any limitations or prohibitions. In Golak Nath v. State of Punjab, relying on the Berubari case, Justice

26 Part V consists of Articles on the Union: Chapter I: The Executive, Chapter II: Parliament and Chapter IV: The Union Judiciary. The Part VI consists of Articles on the States, the Chapter II refers to the Executive, the Chapter III to the State Legislature and the chapters V and VI to the High Courts end the Subordinate Courts.

27 AIR 1960 SC 845.

28 AIR 1967 SC 1643.
Wanchoo said that the Preamble cannot control the unambiguous language of the articles of the Constitution.

Both these cases overlook constitutional history because the motion adopted by the Constituent Assembly stated in so many words that the Preamble stands a part of the Constitution\(^29\).

In *Kesavananda Bharati v. State of Kerala*\(^30\), the view taken in both the aforesaid cases was rejected. The majority held that the Preamble of the Constitution was part of the Constitution. Even though the Preamble is not a source of power or limitations, the majority held that the preamble had a significant role to play in the interpretation of the provisions of the Constitution as well as other statutes. Seven out of the thirteen judges held that the objectives specified in the Preamble contain the Basic Structure of the Constitution which cannot be amended under Article 368 of the Constitution\(^31\).

### 2.3. The Amendment and the Basic structure doctrine

The Parliament, while exercising its constituent power can amend the Constitution in accordance with the procedure laid down in article 368. The procedure is quite complex but not rare: the Constitution is amended twice a year in average which makes the Indian Constitution one of the most amended constitutions in the world.

A Bill can be introduced in each House of the Parliament and requires a majority of the total of membership of that House and a majority of no less than two-thirds of the members of that House present and voting to be passed. The president must then assent to this Bill.

When amending certain matters\(^32\), a special procedure must be followed. Before presenting the Bill to the President for its assent, the Bill must be approved by 50% of the state legislatures. This procedure is applicable for every amendment made to the seventh schedule regulating the separation of legislative powers between the Union and the states.

A unique feature of judicial review in India is that the Courts, aside of non-constitutional amendments, have the power to strike down constitutional ones.

---


\(^{30}\) AIR 1973 SC 1461.

\(^{31}\) Ibid at 1535, 1603, 1648 and 1860.

\(^{32}\) Provided that if such amendment seeks to make any change in—
(a) article 54, article 55, article 73, article 162 or article 241, or
(b) Chapter IV of Part V, Chapter V of Part VI, or Chapter I of Part XI, or
(c) any of the Lists in the Seventh Schedule, or
(d) the representation of States in Parliament, or
(e) the provisions of this article,
the amendment shall also require to be ratified by the Legislatures of not less than one-half of the States by resolutions to that effect passed by those Legislatures before the Bill making provision for such amendment is presented to the President for assent.
The power to judicially review constitutional amendments was cemented in the case of Kesavananda Bharati v. State of Kerala\textsuperscript{33}, where the Supreme Court held that there were certain basic features of the Constitution that were beyond amending powers of the legislature. This has been popularly referred to as the ‘basic structure doctrine’\textsuperscript{34}.

The Court in the aforesaid case refused to entertain the view that the amendment to the Constitution would be covered by the term ‘law’ in Article 13. Instead it took a jurisprudential and philosophical route and decided that restrictions were to be taken into account on the amending power conferred under Article 368:

Article 13(2) of the Constitution states that \textit{The State shall not make any law which takes away or abridges the rights conferred by this Part – Part III Fundamental Rights- and any law made in contravention of this clause shall, to the extent of the contravention, be void.}

One may question whether the term “\textit{any law}” referred to in this article includes the amendments to the Constitution. In the \textit{Golaknath} verdict, the Supreme Court held that an amendment is a law as understood in article 13(2), which implies that the Parliament could not modify, restrict or impair fundamental freedoms, or only do so through the instituted procedure to amend the Constitution.

The procedure has brought many criticisms upon itself, and was notably questioned by the parliament. In the \textit{Kesavananda} case, the Supreme Court decided that an amendment an amendment was not a law but, nevertheless, the Court fixed limits to the Parliament’s amending powers: \textit{the Parliament could not use its amending powers under Article 368 to damage, emasculate, destroy, abrogate, change or alter the basic structure or framework of the Constitution.}

In this case, Chief Justice Sikri enumerated the following as the basic features of the Constitution:

- Supremacy of the Constitution.
- Republican and democratic form of Government.
- Secular character of the Constitution.
- Separation of powers between the legislature, the executive and the judiciary.
- Federal character of the Constitution.

He observed that these basic features are easily discernible not only from the Preamble but also from the whole canvas of the Constitution. He added that the structure was built upon the basic foundation of dignity and freedom of the individual which could not in any form of amendment be destroyed.

While 7 out of the 13 Judges in the aforesaid case, boldly declared that the basic structure or framework of the Constitution could not be altered by Parliament by amendment of the Constitution under Article 368, no consensus was reached among these Judges as to the precise content of the basic structure or framework of the Constitution. Therefore, "basic structure" remains a vague and undefined concept, at least as vague as most of the basic

\textsuperscript{33} AIR 1973 SC 1461.

\textsuperscript{34} For a detailed analysis of the doctrine see D Conrad, Constituent Power, Amendment and the Basic Structure of the Constitution: A Critical Reconsideration, 6-7 Delhi L Rev 1 (1978).
features illustrated by the seven Judges. While this vagueness constitutes the weakness of the doctrine, it also suggests limitless judicial power.

The doctrine, though propounded in Kesavananda Bharati v. State of Kerala, was kept on the shelves and did not come into use until later when the Supreme Court struck down a constitutional amendment in Indira Gandhi v. Raj Narain. Prime Minister Indira Gandhi successfully moved a constitutional amendment by which the jurisdiction of the courts to adjudicate over election disputes in relation to the Office of the Prime Minister was removed. This was challenged as a violation of the basic features of the Constitution.

Following the ratio of Kesavananda Bharati, the Court declared that the amendment violated the basic structure of the Constitution, but the Judges differed in their perception of the basic structure and its application to the case on hand. While some Judges including Ray, C.J. held that the 39th Amendment violated the rule of law, H.R. Khanna, J. held that it subverted the principle of free and fair election which is an essential postulate and basic structure of the Constitution. K.K. Mathew, J. held that it was outside the scope of the constituent power.

The difficulty in applying the law declared in Kesavananda Bharati to specific cases was once again noticed in Minerva Mills Ltd. v. Union of India. In Waman Rao v. Union of India the Supreme Court applied the doctrine of prospective overruling to the law declared in Kesavananda Bharati by holding that all amendments to the Constitution which were made before 24-4-1973 were valid and the amendments made on or after that date were open to challenge on the ground that all or any of them were beyond the constituent power of Parliament being violative of the basic structure of the Constitution.

In Shri Raguhnathrao Ganapatrao v. Union of India, the Supreme Court upheld the validity of the amendment that derecognized the former India rulers and abolished their privy purses. The Court held that though the provision relating to the privy purses were an integral part of

35 AIR 1975 SC 2299.
37 The validity of clauses (4) and (5) of Article 368 as inserted by the 42nd Amendment was challenged. Section 55 of the 42nd Amendment Act, 1976 insulated Constitution amendments made under Article 368 before or after the commencement of Section 55 from judicial review. Clause (5) clarified that there shall be no limitation whatever on the constituent power of Parliament to amend by way of addition, variation or repeal the provisions of the Constitution under Article 368. The Court declared that Parliament cannot in exercise of the limited power of amendment contained in Article 368 enlarge that very power into an absolute power. On the question of validity of Section 4 of the 42nd Amendment Act, which enlarged the scope of Article 31-C by substituting the clause “all or any of the principles laid down in Part IV” for the clause “the principles specified in clause (b) or (c) of Article 39” Bhagwati, J. disagreed with the majority. Article 31-C as inserted by the 25th Amendment saved laws giving effect to the directive principles contained in clauses (b) and (c) of Article 39 only on the ground of violation of Article 14 or Article 19. The 42nd Amendment enlarged the scope of Article 31-C to save laws giving effect to all or any of the directive principles of State policy. While the majority declared Section 4 of the Amendment Act unconstitutional on the ground that it circumvented Article 32 by withdrawing totally the protection of Articles 14 and 19 which confer rights essential for the proper and effective functioning of a democracy in respect of a large category of laws, P.N. Bhagwati, J., declared that Section 4 by giving primacy to the directive principles over fundamental rights in case of conflict between them, did not damage or destroy the basic structure of the Constitution and the amended Article 31-C was valid.
38 (1981) 1 SCC 147.
39 AIR 1993 SC 1267.
the Constitution, they were not basic features of the Constitution and therefore could be amended.

In *Kihoto Hollohan V. Zachillu*⁴⁰, the petitioners challenged the constitutional validity of the 52nd Amendment that disqualified a member of a legislature on defection from his original party. This amendment introduced the Tenth Schedule to the Constitution. The Court held that the amendment only strengthened democracy, which was a basic structure of the constitution and did not violative it. Therefore the amendment was held valid.

2.4. The separation of powers

The doctrine of **separation of powers** stated in its rigid form means that each of the powers of the government, that is, namely, executive or administrative, legislative and judicial should be confined exclusively to a separate department or organ of government. The principle of checks and balances further limits governmental power. The underlying idea is that, if one organ is allowed to act without any sort of control, only arbitrary action will result. This system ensures that one organ be under the constant vigil of the other two.

Under the Indian Constitution only executive power is ‘vested’ in the President, while provisions are simply made for a Parliament and judiciary without expressly vesting the legislative and judicial powers in any person or body. India has the same system of parliamentary executive as in England and the Council of Ministers drawn from among the members of the legislature, both at the State and Union levels.

Accordingly, the Indian Constitution has not recognized a strict separation of powers between the legislature and executive. But it must be noted that there is a differentiation and demarcation of powers and functions between the legislature and the executive, and, generally speaking, this Constitution does not contemplate that one organ should assume the functions belonging to the other⁴¹.

It must be emphasized here, that there is strict separation of powers between the judiciary and the other two organs, which constitutes an unusual exception in face of its general resemblance to the Commonwealth system. The Constitution provides for an independent judiciary with extensive powers to review the acts of the legislature and the executive. In the context of the independence of judiciary, the Supreme Court has held that separation of powers is a basic feature of the Constitution⁴².

It also must not be forgotten, that though, the Indian Constitution does not have a strict separation or powers, the principle of checks and balances are very well present in the same. The power to appoint the judges to the higher judiciary in India has been vested in the President and the power to impeach them with the Parliament.⁴³ As mentioned already the Council of Ministers are collectively responsible to the Parliament. The judiciary is vested

---

⁴⁰ AIR 1993 SC 412.

⁴¹ Ram Jawaya Kapoor v. State of Punjab, AIR 1955 SC 549, see also In re Delhi Laws Act, 1912, AIR 1951 SC 332.


⁴³ See Articles 124. See also Sarojini Ramaswamy v. Union of India, (1992) 4 SCC 506.
with the power to invalidate actions of the legislature and executive on the touchstone of the Constitution.

2.5. Judicial Review in India

Article 245 of the Constitution states that subject to the provisions of the Constitution, Parliament may make laws for the whole or any part of India and the State legislature can make laws for the whole or any part of the State. It is to this subjection clause in Article 245 that the power of judicial review has been attributed to.44

Another source of judicial review is Article 13 which provides that no law shall violate the Fundamental Rights enshrined in Part III of the Constitution. Under the present constitutional pattern, the courts (i.e. the Supreme Court of India and the various High Courts in the States) can strike down legislations and executive actions as unconstitutional.

Though these may be seen as the textual sources of judicial review, it has been argued that the power of judicial review is inherent to a constitutional framework and even if these specific provisions did not exist, the higher judiciary in India would have still continued to enjoy the power of judicial review45.

3. Judicial System

3.1. The Supreme Court

At the federal level, the Supreme Court of India has been established by Part V, Chapter IV of the Constitution and stands at the top of the judicial hierarchy.

This Court has both original and appellate jurisdiction. The original jurisdiction covers any dispute between the Government and one or more states or between states or between Government and state(s) on one side, and, on the other side, state(s). The Supreme Court has an Appellate jurisdiction over any judgment, decree or final order of a High Court46 in both civil and criminal matters.

Apart from these powers, the Supreme Court is entitled by article 32 of the Constitution to issue directions or orders or writs, including writs in the nature of habeas corpus, mandamus, prohibition, quo warranto and certiorari47 to ensure enforcement of fundamental rights.

In certain circumstances, cases can be transferred to the Supreme Court as established in article 139A48. This allows uniformity of the cases, given that the law declared by the Supreme Court shall be binding on all courts within the territory of India49.


46 See Articles 132-134 of the Indian Constitution.

47 Article 32 of the Constitution of India states that « 32. Remedies for enforcement of rights conferred by this Part.—(1) The right to move the Supreme Court by appropriate proceedings for the enforcement of the rights conferred by this Part is guaranteed.»
The Supreme Court also has the right to assess the constitutionality of laws passed by Parliament.

The President can also consult the Supreme Court on question of law or fact of such a nature and of such public importance that it is expedient to obtain the opinion of the Supreme Court upon it.\(^{50}\)

Article 129 of the Constitution states that “the Supreme Court shall be a Court of record, and shall have all the powers of such court including the power to punish for contempt of itself”. The summary jurisdiction exercised by superior courts in punishing for contempt of their authority exists for the purpose of preventing interference with the course of justice and ensure the rule of law\(^{51}\). This jurisdiction will be used only in extraordinary circumstances only when there is real prejudice which can be regarded as a substantial interference with the due course of justice as distinguished from a mere question of propriety\(^{52}\). The procedure for the exercise of this power will be subject to the Contempt of Courts Act, 1971 but the Act cannot curtail the substantive power of the Court given under this provision\(^{53}\).

The Parliament under Article 138 is authorized to invest the Supreme Court with additional jurisdiction with respect to the enforcement of any of the matters enumerated in the Union List. The enlargement of powers contemplated under this provision may be applied to the original or appellate jurisdiction of the Supreme Court. The jurisdiction of the Supreme Court could be further enlarged with respect to any matter as the Government of India and the States may by special agreement confer, provided that the Parliament by law provides for the same.

As it has been discussed before, the Supreme Court has gained a great power and is quite an activist Court: it managed to give a compulsory character to the Constitution preamble, holds a central role in limiting the Parliament’s powers when amending the Constitution and has created a standing for public interest in *S.P. Gupta v. Union of India* (1982) and in *People’s Union for Democratic Rights v. Union of India* (1982).

\(^{48}\) “(1) Where cases involving the same or substantially the same questions of law are pending before the Supreme Court and one or more High Courts or before two or more High Courts and the Supreme Court is satisfied on its own motion or on an application made by the Attorney-General of India or by a party to any such case that such questions are substantial questions of general importance, the Supreme Court may withdraw the case or cases pending before the High Court or the High Courts and dispose of all the cases itself:

Provided that the Supreme Court may after determining the said questions of law return any case so withdrawn together with a copy of its judgment on such questions to the High Court from which the case has been withdrawn, and the High Court shall on receipt thereof, proceed to dispose of the case in conformity with such judgment.

(2) The Supreme Court may, if it deems it expedient so to do for the ends of justice, transfer any case, appeal or other proceedings pending before any High Court to any other High Court.”.

\(^{49}\) Article 141 of the Constitution

\(^{50}\) Article 143 of the Constitution


\(^{53}\) Pritam Pal v. High Court of MP, AIR 1992 SC 904.
3.2 The High Courts

The High Courts operate at the state level and are just under the Supreme Court in the judicial hierarchy. There might be only one High Court for several states or union territory. The High Court is headed by a chief Justice appointed by the president in consultation with the Supreme Court’s Chief Justice and the governor. As for the federal level, the state’s Chief Justice may advise the Governor.

Only six High Courts have original jurisdiction, the other ones are appellate courts but all High Courts have additional jurisdiction under special statutes, such as the Banking Companies Act (1949) and the Companies Act (1956)\(^{54}\).

The High Courts are independent from the state’s legislature and executive. They have an original and appellate jurisdiction within their state or territory and may issue writs in cases involving Fundamental rights. They also supervise the action of the lower courts.

3.3. The Lower Courts

At the lower level, the district judges are competent for civil cases. Criminal cases are examined by session judges. Those judges are appointed by the governor after consulting the state’s High Court.

At sub district level, we find the same distinction between civil cases within the munsif courts competence and the lesser criminal cases led by a subordinate magistrate under the supervision of a district magistrate.

For mere disputes, the people’s courts or panchayats or lok adalats are competent at village level.

A transfer from lower courts to high courts is always possible in the field of fundamental rights.

3.4. The judicial independence

The independence of the higher judiciary in India is ensured through a variety of mechanisms. Though the power to appoint the judges of the Supreme Court and the High Courts has been conferred to the President, who reaches his decision in consultation with a variety of constitutional functionaries, the Supreme Court - through a series of decisions - has mandated that mere consultation with the Chief Justice and other judges of the Supreme Court will not suffice. Indeed, it is a collegium of judges that now nominates the candidates while the President appoints them\(^{55}\).

Judges are strictly appointed on the basis of seniority. Security of tenure is guaranteed to every judge. A judge of the Supreme Court or a High Court can be removed only on proved

---

\(^{54}\) B. DEBROY, “Some issues in law reform in India”, in Governance, Decentralization and Reform in China, India and Russia, Jean-Jacques Dethier (ed.), Kluwer Academic Publishers, p. 344

grounds of incapacity or misbehaviour\textsuperscript{56}. Salaries of the judges have been fixed and cannot be varied by the legislature except during financial emergency. Once appointed, their privileges and rights cannot be altered to their disadvantage\textsuperscript{57}. Expenditure in respect of salaries and allowances of the judges is not put to the vote of the legislatures.\textsuperscript{58}

No discussion shall take place in the any of the legislatures with respect to the conduct of any judge of the Supreme Court or the High Court in the discharge of her duties\textsuperscript{59}. The Supreme Court and the High Courts have been given the power to recruit their own staff and frame rules regarding conditions of service\textsuperscript{60}.

4. Administrative tribunal system

Establishment of the Central Administrative Tribunal under the Administrative Tribunals Act, 1985 (hereinafter also referred as the Act) is considered as one of the major steps taken in the direction of development of Administrative Law in India.

The Act has been passed by the Parliament in pursuance of Article 323-A of the Constitution. This article, empowers the Parliament to establish Administrative Tribunals for dealing exclusively with service matters of government servants, and also provides for exclusion of jurisdiction of all the courts excepting the Supreme Court.

Even before Article 323-A was enacted, tribunals existed in various areas and their existence was recognized by the Constitution, but they were not intended to be an exclusive forum, and therefore, they were subject to judicial review by the High Courts under Articles 226 and 227. Distinct from this existing tribunal system, a new experiment was introduced by Article 323-A which provides for exclusion of the jurisdiction of the High Courts under Articles 226 and 227, notwithstanding any other provisions in the Constitution. The object of this experiment was to lessen the backlog of cases pending before the High Courts and to provide an expert and expeditious forum for disposal of disputes of Government servants relating to service matters.

However, in \textit{L Chandra Kumar v. Union of India}\textsuperscript{61}, holding that judicial review is a basic feature of the Constitution, the Supreme Court declared clause 2(d) of Article 323A and clause 3(d) 323B to the extent they excluded the jurisdiction of the High Courts as unconstitutional. The remaining provisions of Articles 323A and 323B are operative and tribunals are functioning these.

\textsuperscript{56} Articles 124, 218 of the Constitution.

\textsuperscript{57} Articles 125, 221 and 360 of the Constitution.

\textsuperscript{58} Articles 146 and 229 of the Constitution.

\textsuperscript{59} Articles 121, 211 of the Constitution.

\textsuperscript{60} Articles 146, 229.

\textsuperscript{61} (1997) 3 SCC 261.
5. Competences to Legislate on Data Protection

As explained above, the legislative powers are separated into three lists, one enumerating the exclusive competences of the Union State, the second one for the matters within the competence of the States and the last one for concurrent matters.

Article 246 (1) of the Constitution of India grants the Parliament with the exclusive power to make laws with respect to any of the matters enumerated in List I of the Seventh Schedule (Union List).

Those competences encompass everything pertaining to national defence and military forces, macroeconomic stability, international trade as well as other matters of first importance or implying more than one State. For instance, the Trade and commerce with foreign countries, the inter-States trade and commerce, banking, patents, inventions and designs, copyright, trade-marks and merchandise marks, the constitution, organisation, jurisdiction and powers of the Supreme Court are within the Union competence.

The Union List gives exclusive competence to the Union to participate in international conferences; associations and other bodies and to implement the decisions made thereat, as well as entering treaties and agreements with foreign countries and implementing of treaties, agreements and conventions with foreign countries.

This power of Parliament is unfettered by Article 246(2) and (3).

Regarding the States, Article 246 (2) of the Constitution of India entitles State Legislatures to legislate in an exclusive way in matters enumerated in List II.

The State list pertains to matters which concern the States such as public order, police, prisons, public health, fisheries, land rights and every aspect of local government. It also concerns every aspect relating to agriculture, the trade and commerce within the state.

This power of the Legislature is subject to Article 246(1) and (2).

The concurrent list enumerates every matter in which both the Parliament and the State Legislature can legislate such as the criminal law, criminal procedure, the preventive detention, marriage and divorce, contracts, including partnership, agency, contract of carriage, and other special forms of contracts, but not including contracts relating to agricultural land.

This power, given by Article 246(2) of the Constitution, is unfettered by Article 246(3) for the Parliament while the State Legislature is subject to Article 246(1).

The entries in the lists contained in the Seventh Schedule can be amended through a constitutional amendment under Article 368. But in such cases apart from the normal procedure (the sanction of the Parliament through special majority) the amendment will have to be ratified by not less than one-half of the legislature of the States, by passing a resolution to that effect before the bill is presented to the President for his assent.

The Parliament has a residuary power, as it is stated in Article 248 of the Constitution:
(1) Parliament has exclusive power to make any law with respect to any matter not enumerated in the Concurrent List or State List.
(2) Such power shall include the power of making any law imposing a tax not mentioned in either of those Lists.

Entry 97 of List I also states that the Parliament will be competent in respect with any other matter not enumerated in List II or List III including any tax not mentioned in either of those Lists.

In Union of India v. H. S. Dhillon, AIR 1972 SC 1061, the Supreme Court decided whatever doubt there may be on the interpretation of Entry 97, List I is removed by the wide terms of Articles 248. It is framed in the widest possible terms. On its terms the only question to be asked is: Is the matter sought to be legislated included in List II or in List III or is the tax sought to be levied mentioned in List II or in List III; No question has to be asked about List I. If the answer is in negative then it follows that Parliament has power to make laws with respect to that matter or tax.

Thus, if the subject matter of a legislation does not fall under any entry in List II or III, then the Parliament can take recourse to the residuary power.

This was followed in cases like Att. Gen. For India v. Amratlal Prajivandas, AIR 1994 SC 2179 / (1994) 5 SCC 54.

It can thus be concluded from the above discussion that only national Parliament is competent to legislate on privacy issues since it can be interpreted as any other matter not enumerated in List II (State competence) nor in List III (Concurrent list) by virtue of Entry 97 List I read with Art. 248 of the Constitution.

6. Influence of International Norms

Regarding international law, India has opted for a dualist paradigm: international and domestic law are strictly separated. Hence, a treaty is not enforceable until it has been incorporated into a domestic law.

The Union is competent to reincarnate international provisions into domestic law, this is foreseen by the Constitution in its article 253, which provides that

Notwithstanding anything in the foregoing provisions of this Chapter, Parliament has power to make any law for the whole or any part of the territory of India for implementing any treaty, agreement or convention with any other country or countries or any decision made at any international conference, association or other body.

Thus, in the exercise of this competence, the Union is not bound by the distribution of legislative powers, the Indian Parliament remains then the central actor in making laws to implement international agreements.

---

62 The question involved in Dhillon’s case was whether the central government could levy wealth tax on the assets of a person including agricultural land. Wealth tax does not fall within the ambit of Entry 49 List II and thus states cannot levy it. Entry 86 List I has the words exclusively of agricultural land and the thus the part of the central law which refers to agricultural land cannot come within that entry. The main question therefore was whether the tax could be levied under centre’s residuary power.
Ratification/accession to these agreements does not make them enforceable in court of law, nor do they override municipal law. They are enforceable only if a municipal law to that effect is legislated by the Parliament.

That an international treaty has been ratified but not incorporated doesn’t mean the act is ineffective. Courts can take them into account while interpreting statutory law, constitutional provisions or in case of vacuum in domestic legislation, as is has been demonstrated by many decisions of the Supreme Court.

In *Jolly George Verghese v Bank of Cochin*, the Supreme Court held that *it is a principle generally recognised in national legal systems that, in the event of doubt, the national rule is to be interpreted in accordance with the State’s international obligations.*

In *Mackinnon Mackenzie and Co Ltd v Audrey D’Costa*, the Supreme Court interpreted a domestic law (the Equal Remuneration Act, 1976) in the light of a principle issued from an international Convention to which India was Party.

In *Sheela Barse v Secretary, Children’s Aid Society*, the Supreme Court held that the states have the obligation, as the Union has, to implement the principles contained in an international instrument. But the main innovation in this case is that the Court, for the first time, admitted the binding nature of international obligations, instead of recognising a mere influence.

Another step was made by the Supreme Court in *Vishaka v State of Rajasthan* (1997) 6 SCC 241, which concerns a case on sexual harassment of women at the workplace. India has ratified Convention on the Elimination of All forms of discrimination against Women (CEDAW). Article 24 of CEDAW states that State reports should include information about sexual harassment, and on measures to protect women from sexual harassment and other forms of violence or coercion at the workplace. The Court observed “In the absence of domestic law occupying the field … The international conventions and norms (not inconsistent with the fundamental rights) are significant for the purpose of interpretation of the guarantee of gender equality in the Constitution”.

Last, the Supreme Court even brushed aside the specific reservation made by the Government of India while ratifying the International Covenant on Civil and Political Rights.

In *D.K. Basu v State of West Bengal*, the Court established a right to compensation for victims of unlawful arrest or detention—which India didn’t recognise—on the basis that *that reservation, however, has now lost its relevance in view of the law laid down by this Court in a number of cases awarding compensation for the infringement of the fundamental right to life of a citizen.*

Concurrently, we may conclude that in absence of any law incorporating international obligations, the courts have regard to the intent and content of the international Human Rights convention and norms provided that there is no inconsistency with domestic law.

Nevertheless the influence of international laws remains undeniable for interpreting unclear or ambiguous legislation or whenever a void in the legislation is highlighted through practice.
India has signed some conventions pertaining to the Human Rights. Quite relevant for this study is the fact that India ratified the International Covenant on Civil and Political Rights on April 10, 1979 which enounces in its Article 17 the right to privacy, nevertheless, India is not Party to the Optional Protocol to the ICCPR.

India has not signed the OCDE guidelines but is part of the United Nations and as such is held by the guidelines promulgated by the United Nations.

7. General Legal Protection for Human Rights

It has been rightly pointed out that several international human rights receive protection in the form of constitutional/fundamental rights as enshrined in Part III of the Constitution of India, among which the right to life and personal liberty, the freedom of speech and expression, freedom of assembly, freedom to carry on trade, occupation etc, and right to equality. This part also provides constitutional safeguards against child labour and forced labour. More importantly, there are a set of minority rights which also find mention in Part III of the Constitution.

Apart from this, the Parliament has enacted the Human Rights Act, 1993 to provide for the constitution of a National Human Rights Commission, State Human Rights Commission in States and Human Rights Courts for better protection of Human Rights and for matters connected therewith or incidental thereto.

Human rights are defined in s.2 as the rights relating to life, liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in two international human rights instruments (ICCPR and ICESCR) and enforceable by courts in India.

VI. Data protection legislation

1. Introduction

Before engaging in the core analysis of the regulation in the field of data protection, it would be relevant to evaluate the perception of privacy in India. Since India has a different culture and landmarks than that of Western countries, one should pay considerable attention to their customs in order to fully grasp the way in which privacy matters are considered and dealt with.

The surveys that have addressed this topic are scarce for the least. The following analysis is based on the two main studies published by the School of Computer Science of the Carnegie Mellon University.

The first survey focuses on members of the Indian high tech workforce and gives us a global understanding of how privacy among people working in outsourcing is perceived.

The second survey - in which P. Kumaraguru and L. Cranor have led a comparison between India and the United States - is also quite revealing as it vividly underlines the great gap that separates the Western perception of privacy and the predominating perception in India.

The most striking difference appears from the very first question: when Indian subjects are questioned about the word “privacy”, the first thing that comes to their mind is privacy in terms of personal space and subjects, while the US subjects mention information privacy, financial information and identity theft.

While 89% of US subjects disagree with the statement that “Data security and privacy are not really a problem because I have nothing to hide”, only 21% of Indian disagree.

Regarding privacy issues in respect with technology, a minority of Indian subjects (21%) are concerned about keeping computerized information secure (79% of the American subjects are concerned). While responding to this question, a quarter of the US subjects mentioned their concern about identity theft while the topic remained unaddressed by Indian subjects. Later, when the question about identity theft was directly posed, Indian subjects were a minority to

---


65 The sample includes undergraduate students, graduate students, professors from top Indian technical universities and professionals. Ninety percent of the respondents were IT students or professionals.

66 “48% of the subjects in India related privacy to physical, home and living space, but only 18% of the subjects in the US related privacy to these concepts”, P. KUMARAGURU and L. CRANOR, Privacy Perceptions in India and the United States : An Interview Study, p. 6, available on http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf
worry (21%) for a staggering 82% of US subjects declaring themselves concerned by the matter\(^67\).
The average of people concerned by threats to privacy due to cell phones equipped with
_cameras is the same in both countries (25%). This can be explained by the recent incidents
related to these technologies both in India and the USA and the media coverage which
ensued\(^68\).
Only a minority of Indian subjects (7%) mentioned the opt-in/opt-out system when a large
majority of US subjects mentioned it (89%).

The Indian subjects didn’t mention any privacy law in response to questions of general order
(14% of the American subjects mentioned privacy laws). When confronted with several
scenarios\(^69\) in which the subjects were to say if a law existed that could regulate the situation,
the number of Indian subjects that believed that an adequate law existed was very low and
many didn’t find necessary that a corresponding law be called upon\(^70\).

Thus, one may conclude that conception of privacy in India is far different from the Western
conception and it will then be useful to keep this in mind while reading this report.

2. The Right to Privacy

2.1. Before the Constitution

Prior to the adoption of the Constitution of India in 1950 effective from 26\(^{th}\) January, there
was no guarantee of rights, any rights, for the citizens of India. In fact the position as citizen
of India as a legal status came with the arrival of the Constitution.

Prior to the Constitution, the zone of privacy around an individual was determined by the law.
The Criminal Law gave insulation for the person, property and dwelling house and made it
punishable to impute un-chastity to a female.
The law of Torts was reputed as providing an additional dimension of protection of individual
interests in reputation as also the person and property with an admonition that the least
touching of another in anger was assault actionable in damages.
The law of Libel and Slander gave protection for the individuals name and fame.

\(^67\) “The typical responses of the subjects in India were “No absolutely not. I have never felt a threat to [my]
identity” and “No, nothing, I don’t have concerns about my identity being stolen”. P. KUMARAGURU and L.

\(^68\) P. KUMARAGURU and L. CRANOR, Privacy Perceptions in India and the United States : An Interview

\(^69\) “To use computer records and other methods to determine shopping habits” “To determine reading habits” and
“To connect to people’ cell phones or computers and send them customized advertisements”

\(^70\) “A common response of the Indian subjects regarding privacy laws for shopping habits and reading habits was
“Why do you need laws for it?”: In particular, regarding sending customized advertisement to cell phones and
computers, one Indian subject said, “Oh that’s good. I am going through a shop they can give us information and
I can buy products”. In contrast, a common response if the US subjects was “they should send me customized
information only if I want””. P. KUMARAGURU and L. CRANOR, Privacy Perceptions in India and the United
2.2. The Right to Privacy in the Constitution

Even after the Constitution came into force, no fundamental right to privacy was explicitly guaranteed. However, the Constitution of India embodied Fundamental Rights in Part III, which are enumerated in Article 14-30. Judicial activism has then brought the Right to Privacy within the realm of Fundamental Rights.

Indeed, the Supreme Court deduced that right from the Right to Life and Personal Liberty enshrined in Article 21 of the Constitution through an extensive interpretation of the phrase Personal Liberty.

Article 21 states “no person shall be deprived of his life or personal liberty except according to procedures established by law”.

On the basis of this provision, the Supreme Court observed that “those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law”.

Hence, the court held that “personal liberty” means life free from encroachments unsustainable in law. Thus, any law is required to answer a triple test-(1) it must prescribe a procedure; (2) the procedure must withstand the test of one or more of the fundamental rights conferred under Article 19 which may be applicable in a given situation; and (3) it must also be liable to be tested with reference to Article 21 in that the procedure authorizing interference must be right and just and fair and not arbitrary, fanciful or oppressive.

The court stated that intrusions into privacy can be by legislative provisions, administrative/executive orders, and judicial orders. The court can verify reasonableness and proportionality of legislative intrusions vis-à-vis the purpose. It can scrutinize the administrative or executive actions for a reasonable basis or reasonable material to support it. For judicial warrants the court must have sufficient reason to believe that search or seizure is warranted and necessary for the protection of State interest. Warrant-less searches have been permitted if conducted in good faith to preserve evidence or prevent sudden danger to person or property.

2.3. Judicial developments

Some decisions of the Supreme Court address privacy matters. These decisions draw the contours of the right to privacy, where necessary, and balance it against other rights and interests. Examples of such decisions follow.

71 21. Protection of life and personal liberty. - No person shall be deprived of his life or personal liberty except according to procedure established by law.

72 For example: in M. P. Sharma v. Satish Chandra, District Magistrate, Delhi AIR 1954 SC 300 the court held that, Power of search and seizure does not violate the right to privacy because it is in the interest of the State
1. Kharak Singh v State of UP

In this case the appellant was being harassed by the police under Regulation 236(b) of UP Police Regulation, which permits domiciliary visits at night. The Supreme Court held that the Regulation 236 is unconstitutional and violative of Article 21.

It concluded that the Article 21 of the Constitution includes “right to privacy” as a part of the right to “protection of life and personal liberty". The Court equated ‘personal liberty’ with ‘privacy’, and observed, that “the concept of liberty in Article 21 was comprehensive enough to include privacy and that a person’s house, where he lives with his family is his ‘castle’ and that nothing is more deleterious to a man’s physical happiness and health than a calculated interference with his privacy”.

2. People’s Union for Civil Liberties (PUCL) v Union of India

The Supreme Court held that the telephone tapping by Government under S. 5(2) of Telegraph Act, 1885 amounts infraction of Article 21 of the Constitution of India. Right to privacy is a part of the right to “life” and “personal liberty” enshrined under Article 21 of the Constitution. The said right cannot be curtailed “except according to procedure established by law”. The court wanted the right to privacy to be under Article 21 to be expounded consistently with Article 17 of International Covenant on Civil and Political Rights, 1966.

3. Gobind v State of M.P.

This is another case on domiciliary visits. The Supreme Court laid down 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 a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest test”

The court however ruled in Malak singh v state of P & H, AIR 1981 SC760, that while exercising surveillance over reputed bad characters, habitual offenders, and potential offenders the police should not encroach upon the privacy of a citizen so as to offend his rights under Article 21 and Article 19 (1) (d)

4. Pooran Mal v. Director of Inspection (Investigation) of Income-tax, New Delhi

AIR 1974 SC 348

The court held that evidence collected by an illegal search can not be excluded on ground of invasion of privacy because there is no specific fundamental right to privacy. (This would tend to weaken the right to privacy by allowing a public authority to use evidence obtained illegally.)

---

73 (AIR 1963 SC 1295)
74 (1997) 1 SCC 301
75 (1975) 2 SCC 148
5. V.S. Kuttan Pillai v. Ramakrishnan AIR 1980 SC 185

The court held that general warrant for searching and seizing listed documents would not entail invasion of privacy even if the search did not yield any result because of counter availing state interests.


It has been held that for a search of a person the safeguards provided Sec. 50 of the Code of Criminal Procedure are mandatorily to be followed. The invasion of a person has been given a protection through insistence on a procedural safeguard but the court has not ruled that evidence obtained in breach of Sec. 50 safeguards would be impermissible evidence.

7. R. Rajagopal v State of Tamil Nadu76

The Court held that the petitioners have a right to publish what they allege to be the life-story/autobiography of Auto Shankar insofar as it appears from the public records, even without his consent or authorization. But if they go beyond that and publish his life story, they may be invading his right to privacy, then they will be liable for the consequences in accordance with law. Similarly, the State or its officials cannot prevent or restraint the said publication. It stated that “A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing 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 and would be liable in an action for damages”.

8. Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363

Right to privacy of an electoral candidate was held not violated by publications of details of his criminal antecedents and/or his assets and liabilities. The right to be informed of the electorate was held superior to candidate’s desire for secrecy.

9. X v. Hospital Z AIR 1999 SC 495

It has been held that a doctor’s disclosure of a person’s incurable physical ailment (HIV) to the relatives of the one to whom he was to get married was not violative of right to privacy. Doctor-patient relationship, though basically commercial, is professionally; a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the Right of Privacy which may sometimes lead to the clash of one person's "right to be let alone" with another person's right to be informed. Circumstances in which the public interest would override the duty of confidentiality could, for example, be the investigation and prosecution of serious crime or where there is an immediate or future (but not a past and remote) health risk to others. In "X v. Hospital Z"AIR 2003 SC 664 the court held that a healthy person can contract a valid marriage even after knowing the fact of ailment.

76 AIR 1995 SC 264
10. Sharda v. Dharmal, AIR 2003 SC 3450

It was held that in divorce proceedings an order to undergo medical examination on strong grounds of necessity to establish a contention was held not invasive of right to privacy. Public policy requirements was permitted to prevail over private interests.


The court struck down Sec. 73 of the Indian Stamp Act, 1899 as amended by the Andhra Pradesh Act (17 of 1986) as permitting an overbroad invasion of private premises or the homes of persons in possession of documents in a power of search as seizure without guidelines as to who and when and for what reasons can be empowered to search and seize, and impound the documents. The court, however held that no right to privacy could be available for any matter which is part of public records including court records.

If one follows the judgments given by the Supreme Court, three themes emerge

(1) that the individual’s right to privacy exists and any unlawful invasion of privacy would make the ‘offender’ liable for the consequences in accordance with law;

(2) that there is constitutional recognition given to the right of privacy which protects personal privacy against unlawful governmental invasion;

(3) that the person’s “right to be let alone” is not an absolute right and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others;

As those judgements show, a right to Privacy is recognized in India but it is rather limited since it covers only “first generation rights” as understood in Europe. Moreover, the Right to Privacy has also been invoked in the field of women’s right:

- in State of Karnataka v. Krishnappa AIR 2000 SC 1470 the court strengthened the protection of the right to privacy over the person by requiring stern punishment of rapists. The offence was held to be seriously violating the right to privacy.

- in State v. N. M. T. Joy Immaculate" AIR 2004 SC 2282 the Supreme court set aside the direction of the high court given to the government that women witnesses/accused should not be taken to a police station but should be examined only by women police officers at their places. This direction was on complaint of harassment and torture in the police station. The Supreme Court seems to have erred with reference to Article 15(3) and Article 235 of the Constitution. What was in promotion of right to privacy of women has been set at nought.

- in Saroj Rani v. Sudarshan Kumar Chadha, AIR 1984 SC 1562 the Supreme Court ruled that Restitution of Conjugal Rights was a savage remedy denying the freedom over her person to the female and unconstitutional as violating the right to privacy.


Generally speaking, the right to privacy as an independent and distinctive concept has been found to have originated in the field of Tort Law and was developed by the Court on a case by
case basis. The consequence is that a compendious code on what is the right to privacy has not been evolved yet.

3. Statutory safeguards of Privacy and data protection interest outside data protection legislation

No specific legislation pertaining to data protection has been enacted in India. However, one could claim that other statutes provide some safeguards to the lack of explicit legislation in that field. These statutes must be examined even if they cannot provide adequate protection on their own accord.

3.1. The Information Technology Act, 2000

3.1.1. Background

The Information Technology Act (hereafter IT Act) is often presented, in India, as the text regulating data protection under Indian Law. This Act has been enacted in the Fifty first Year of the Republic of India. It received the assent of the President on the 9th June, 2000 and is effective as of 17th October, 2000. This Act is based on the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30th January, 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its twenty-ninth session. The aim of the IT Act was to set up India’s first ever information technology legislation.

There were three reasons:

(a) to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions,

(b) to enable the use of digital signatures in authentication of electronic records; and

(c) to showcase India’s growing IT prowess and the role of Government in safeguarding and promoting IT sector.

Hence, the scope of the Act covers “Ecommerce” and “E-governance” by introducing rules pertaining to a wide set of themes such as digital signatures, information in electronic form, computer crime, hacking, damage to computer source, breach of confidentiality and viewing of pornography. However, the IT Act is regarded by some Indian scholars as a text providing a data protection regime for the ecommerce and e-governance sectors.

3.1.2. Principles and definitions

3.1.2.1. No such concept as “personal data”

In the IT Act, data is defined as “a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored in the memory of the computer”

30
The IT Act doesn’t provide for any definition of personal data. Furthermore, the definition of “data” would be more relevant in the field of cybercrime. Nevertheless, as already exposed above, some provisions are considered by Indian scholars as providing rules pertaining to personal data protection. We will examine them keeping in mind that a concept such as "personal data" in the IT Act is absent.

3.1.2.2. Provisions regarded as providing rules pertaining to data protection

Chapters IX and XI define cyber contraventions related to unauthorized access to computer, computer system, computer network or resources, unauthorised alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, computer database, etc.

Some sections of those Chapters are viewed in India as the “backbone” of the data protection regime.

A discussion on these provisions follows.

a) Section 43. Penalty for damage to computer, computer system, etc.

Section 43 states that:

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

This section foresees civil liability in case of data, computer database theft and may cover computer trespass, unauthorised digital copying, downloading and extraction of data, computer database or information, theft of data held or stored in media is covered, unauthorised transmission of data or programme residing within a computer, computer system or computer network, use of cookies, spyware, GUID or digital profiling are not legally permissible, unauthorised access to computer data/databases, etc…

b) Section 65. Tampering with computer source documents

This Section states that:

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is
required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, “computer source code” means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.
This section protects computer code source.

c) Section 66. Hacking with Computer System

This Section states that:

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

This Section deals with hacking and is quoted in India as a data protection provision. According to Mr Unni, the word diminished in value/utility has considerable impact upon the confidentiality of a document. E.g. if any sensitive personal e-mail is saved in a computer and if any person accesses the said document, then the value of the information is completely lost, this will make then party liable under this provision.

d) Section 72. Penalty for breach of confidentiality and privacy

This section states that:

Any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

This is the only Section requiring the consent of the concerned person but, given its limited scope, it would be difficult to consider that it could provide a sufficient level of personal data protection.

Indeed, this section confines itself to the acts and omissions of those persons, who have been conferred powers under the Act, rules or regulations made thereunder.

These authorities are:
Appellate Tribunal, (vii) Network Service Provider, and (viii) Police Officer (Deputy Superintendent of Police).

Since the Act has only conferred powers to these authorities, the number of ‘data controllers’ having duties is rather limited.

3.1.3. The Amendments to the IT Act

3.1.3.1. Introduction

The contractor is of the opinion that the current IT Act does not contain sufficient data protection provisions. The Indian government, aware of the lack of regulation in this field, appointed an Expert Committee on Cyber Laws whose role is to suggest amendments to the IT Act.

The Department of Information Technology, the Ministry of Communications and Information Technology and the Government of India decided to set up an Expert Committee on Information Technology Act, 2000 (notification no. 9(16)/2004 –EC dated January 7, 2005).

The recommendations of the Committee were submitted to the Government of India. The matter is presently under consideration with the Ministry of Law and Justice. It is difficult to precise timeline and it would be speculative to say which suggestions would be incorporated as amendments.

One of its terms of reference was “to consider and recommend suitable legislation for data protection (privacy) in the Information Technology Act, 2000”.

The Expert Committee submitted its report in August 2005 to the Department of Information Technology. It was of the view that Sections 43, 65, 66 and 72 should be amended from the point of “data protection and privacy”. It has recommended the following amendments on the issue of data protection (privacy) to the Government of India:

(a) In addition to contractual agreements between the parties, the existing Sections (viz. 43, 66 and 72) have been revisited and some amendments have been provided for. Notably amongst these are:

(i) Proposed a new Section 43(2) related to handling of sensitive personal data or information with reasonable security practices and procedures thereto

(ii) Gradation of severity of computer related offences under Section 66, committed dishonestly or fraudulently and punishment thereof

(iii) Proposed fine tuning of Section 72(1)

(iv) Proposed additional Section 72 (2) for breach of confidentiality with intent to cause injury to a subscriber.
(b) Language of Section 66 related to computer related offences has been revised to be in lines with Section 43 related to penalty for damage to computer resource. These have been graded with the degree of severity of offence when done by any person, dishonestly or fraudulently without the permission of the owner.

3.1.3.2. The full text of aforesaid amendments

a) Section 43. Compensation for damage to computer, computer system, etc.

**Section 43 (2)** *If any body corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, is found to have been negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore to the person so affected.*

**Section 43, Explanation (v)** “Reasonable security practices and procedures” means, in the absence of a contract between the parties or any special law for this purpose, such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

**Section 43, Explanation (vi)** “Sensitive personal data or information” means such personal information, which is prescribed as “sensitive” by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

Section 43(2) should be read with both Explanation (v) and Explanation (vi). The basis idea behind the proposed amendment is to grant statutory protection to sensitive personal data. The onus is on the body corporate to adopt and implement reasonable security practices and procedures. Proposed section 43(2) provides a basis for liability if a body corporate does not implement reasonable security measures to protect sensitive personal information that it owns or handles using its computer resources. This liability accrues with the suit of a person who is affected by the body corporate’s inadequate security practices and procedures.

Further, it is significant to note that the amendment has paved the role of self-regulation in terms of defining what constitute: “reasonable security practices and procedures” and “sensitive personal data or information”.

b) Section 66. Computer related offences

(a) *If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is in charge of a computer resource:*

(i) accesses or secures access to such computer resource
(ii) downloads, copies or extracts any data, computer data base or information from such computer resource including information or data held or stored in any removable storage medium;
(iii) denies or causes the denial of access to any person authorised to access any computer resource;

he shall be punishable with imprisonment upto one year or a fine which may extend up to two lacs or with both;

(b) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is in charge of a computer resource:

(i) introduces or causes to be introduced any computer contaminant or computer virus into any computer resource;
(ii) disrupts or causes disruption or impairment of electronic resource;
(iii) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer resource;
(iv) provides any assistance to any person to facilitate access to a computer resource in contravention of the provisions of this Act, rules or regulations made thereunder;
(v) damages or causes to be damaged any computer resource, date, computer database, or other programmes residing in such computer resource;

he shall be punishable with imprisonment upto two years or a fine which may extend up to five lacs or with both;

Explanation: For the purposes of this section-

‘Dishonestly’ – Whoever does anything with the intention of causing wrongful gain to one person, wrongful loss or harm to another person, is said to do this thing dishonestly”.

‘Fraudulently’ – A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

“Without the permission of the owner” shall include access to information that exceeds the level of authorized permission to access.

Section 66 is the heart of the criminal provisions, and sets up two categories of criminal conduct punishable by imprisonment from 1 to 2 years. To its credit, section 66 criminalizes a wide range of conducts. However, all two sub-sections (1) and (2) have the same main requirement: dishonestly or fraudulently.

It has been modelled after Section 43 of the Information Technology Act, 2000. The idea is to not only make section 66 consistent with the provisions of the Indian Penal Code, but also provide extent of criminal liabilities in case of data, computer database theft, privacy violation etc.

The proposed section 66 is an attempt to conform to the provisions of the European Convention on Cyber crime.

c) Section 72. Breach of confidentiality and privacy

(1) Save as otherwise provided in this Act or any other law for the time being in force, any
person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned intentionally discloses such material to any other person shall be punished with imprisonment for a term which may extend upto two years, or with fine which may extend to five lakh rupees, or with both.

(2) Save as otherwise provided under this Act, if any intermediary who by virtue of any subscriber availing his services has secured access to any material or other information relating to such subscriber, discloses such information or material to any other person, without the consent of such subscriber and with intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to the subscriber so affected.

The proposed amendments have made public authorities, who have been given powers under the Act, liable for data and privacy violations, should they intentionally disclose such information without the consent of the person concerned.

Further, the newly proposed sub-section (2) makes the intermediaries (network service providers) liable for data and privacy violations. Such intermediaries must compensate caused damages by means of (financial) remuneration to the subscriber so affected.

3.1.4. Content Principles

Basic principles with respect to the content of applicable regulations have been established in order to weigh the adequacy of the protection for personal data provided by a country's legislation. Compliance with these principles is considered a minimum condition for adequate protection.

It should be underlined that the Information Technology Act 2000 is not a privacy protection act nor a data protection legislation as understood in Europe. It does not establish any specific data protection or privacy principles, no such term as “personal data” is defined. Instead of that, the IT Act is a generic legislation which regulates various themes, like digital signatures, public key infrastructures, e-governance, cyber contraventions, etc. Therefore in the IT Act, express provisions covering the core principles suggested by the Working Paper are scarce.

3.1.4.1 Principle of Purpose Limitation

As summarized by the Article 29 Working Party, the purpose limitation principle requires that data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

The IT Act contains no equivalent provision to the Directive's Article 6(b).

3.1.4.2 Principle of Data Quality and Proportionality
a) Definition

As summarized by the Article 29 Working Party, the data quality and proportionality principles require that data should be accurate and where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

b) Accurate and up-to-date data

The research found no express provision in the IT Act requiring data to be kept accurate and up-to-date.

3.1.4.2. Adequate, relevant and not excessive data

The research haven't found any provision in the IT Act requiring processed and transferred data to be adequate, relevant and not excessive.

3.1.4.3. Principle of Transparency

As summarized by the Article 29 Working Party, the transparency principle requires that individuals should be provided with the information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with articles 11(2) and 13 of the directive. The Information Technology Act, 2000 has no equivalent provision to the Directive's Articles 10 and 11.

3.1.4.4. Principle of Security

a) Definition

As summarized by the Article 29 Working Party, the security principle requires that technical organisational measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

b) Security in the IT Act

The IT Act defines “secure system” under Section 2 as “computer hardware, software, and procedure that are (1) reasonably secure from unauthorized access and misuse; (ii) provides a reasonable level of reliability and correct operations; (iii) reasonably suited to performing the intended functions; and (iv) adhere to generally accepted security procedures.”

Section 16 further states:
The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including
(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications.

It should be noted that under Schedule V: Glossary, Information Technology (Certifying Authorities) Rules, 2000, the term “transaction” means a « computer based transfer of business information, which consists of specific processes to facilitate communication over global networks. »

Hence, and given the purpose of the IT Act, it seems that section 16 is more concerned about requiring security procedures for commercial transactions than for “personal data” processes; indeed, no specific provision requires particular security requirements that are appropriate to the risks presented by the processing of personal data. Moreover, the IT Act lacks a provision ensuring that personal data should only be processed on the instructions from the controller.

3.1.4.5. The Rights of Access, Rectification and Opposition

As summarized by the Article 29 Working Party, the data subjects should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.

The IT Act does not provide for any of the principles related to access, rectification and opposition by individual data subjects.

3.1.4.6. The principle of Restriction on Onward Transfers

As summarized by the Article 29 Working Party, further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive. The IT Act does not provide for such a principle.

3.1.4.7. Additional Principles

a) Direct Marketing

According to the Article 29 Working Party, where data are transferred for the purposes of direct marketing, the data subject should be able to “optout” from having his/her data used for such purposes at any stage.

The IT Act is silent on the issue of direct marketing. It provides no opportunity to the data subject to 'optout' from having his/her data transferred for the purposes of direct marketing. In fact, there is no other legislation in India dealing with direct marketing. Only recently, the Hon'ble Supreme Court of India has in its interim order directed the banks and other financial institutions to start maintaining 'donotcallregistry' for the benefit of data subject. Now, a data subject has a right to 'optout' from such online consumer databases.
b) Sensitive Data

According to the Article 29 Working Party, where “sensitive” categories of data are involved (those listed in article 8 of the directive\textsuperscript{77}), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

The IT Act is getting amended on this point. Sensitive personal data or information has not been defined so far, it is foreseen that the Central Government, in consultation with self regulatory bodies of the industry will prescribe which information/data can be designated as sensitive.

A particular regime will be applicable for these information/data: any body, corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, must implement and maintain reasonable security practices and procedures\textsuperscript{78}, unless, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore to the person affected.

However, given that this provisions has not been introduced yet, our research will not take it into account.

3.1.5. Enforcement mechanisms

3.1.5.1. Introduction

The Information Technology Act, 2000 has provided a set of three authorities to provide a mechanism of arbitration or adjudication for settlement of civil disputes under the Act. These are:

\begin{itemize}
  \item Controller of Certifying Authorities,
  \item Adjudicating Officer, and
  \item Presiding Officer of the Cyber Regulations Appellate Tribunal
\end{itemize}

We will only focus on the Adjudicating Officer and the Presiding Officer of the Cyber Regulations Appellate Tribunal

3.1.5.2. The Adjudicating Officer

An affected party under Section 43 (a) – (h) has a right to seek damages from the wrongdoer by compelling him to pay for the damage done upto rupees one crore. The remedy lies in approaching and filing the complaint before the Adjudicating Officer under Section 46 of the Act\textsuperscript{79}.

\begin{flushright}
\textsuperscript{77} Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures.
\textsuperscript{78} “Reasonable security practices and procedures” means that “in the absence of a contract between the parties or any special law for this purpose, such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self regulatory bodies of the industry, if any”.
\textsuperscript{79} 46. Power to adjudicate.
\end{flushright}
As one of the regulators under the Act, it is the statutory duty of Adjudicating Officers to provide relief to the affected party by way of compensation. Hence, it is important that the adjudicating officer [S.46] under the Act must follow the principles of law of torts while granting damages by way of compensation.

It is important that in order to understand the process of adjudication in the Act, the role of adjudicating officer must be taken into consideration. Importance of the Information Technology Act could be gauged from the fact that it has created a separate apparatus to dispense civil justice.

The Adjudicating Officer has to act as:

(a) A Quasi-judicial Body

The adjudicating officer under the Act is a quasi-judicial authority as it is required of him to hold an enquiry before arriving at a decision. It is important to note that the aforesaid Section 46 (1) starts with the words “For the purpose of adjudging under this Chapter………” indicates that the quasi-judicial authority of the adjudicating officer is limited to the determination of contraventions and imposition of penalties under Ss. 43, 44 and 45 of the Act only.

It is obligatory to note that the Central Government as per the Gazette Notification for Information Technology Rules, 2003 has notified ‘Scope and Manner of Holding Inquiry’ [Rule 4]. Some of its important provisions are:

- to exercise jurisdiction in respect of the contraventions in relation to Chapter IX of the Act;
- to receive complaint from the complainant;
- to issue notices together with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings;

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under sub-section (2) of section 58, and—
(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.
• to hold an enquiry or dismiss the matter or may get the matter investigated;

• to fix a date and time for production of documents (including electronic records) or evidence; and

• to hear and decide every application, as far as possible, in four months and the whole matter in six months.

Further, the adjudicating officer, when convinced that the scope of the case (under adjudication) extends to the Offences(s), under Chapter XI of the Act, requiring appropriate punishment instead of mere financial penalty, then as per the aforesaid rules, he should transfer the case to the Magistrate having jurisdiction to try the case, through the Presiding Officer.

(b) A Civil Court

Moreover, it has been provided under S.46 (5) that the adjudicating officer has the same powers as are vested in a Civil Court under the Code of Civil procedure, 1908 while trying a suit, in respect of the following matters, namely: —

• summoning and enforcing the attendance of any person and examining him on oath;

• requiring the discovery and production of documents or other electronic records;

• receiving evidence on affidavits;

• issuing commissions for the examination of witnesses or documents;

• reviewing its decisions;

• dismissing an application for default or deciding it ex parte; and

• any other matter, which may be prescribed.

It is necessary that the aforesaid sub-section (5) should also be read and understood along with the ‘Scope and Manner of Holding Inquiry’ [Rule 4] of the Gazette Notification as mentioned above.

It is thus very much clear from the reading of the Act that the adjudicating officer has not only the trappings of a quasi-judicial authority but also has the power of a court to give a decision or a definitive judgment which has finality and authoritativeness which are essential tests of a judicial pronouncement. The adjudicating officer, therefore, possesses all the attributes of a court.

3.1.5.3. Presiding Officer of the Cyber Regulations Appellate Tribunal

The Information Technology Act, 2000 has established the Cyber Regulations Appellate Tribunal (CRAT) having appellate jurisdiction. Being an appellate authority it is entitled to
exercise its appellate jurisdiction both on fact and law over a decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer.

Under S.48 of the Act, Central Government has been given a mandate to appoint one or more appellate tribunals but the language of the Rule 13 of the Cyber Regulations Tribunal (Procedure) Rules, 2000 makes it clear that there shall only be one tribunal and it shall ordinarily hold its sittings at New Delhi.

A Cyber Regulations Appellate Tribunal is to be headed by one person only (known as the Presiding Officer) to be appointed, by notification, by the Central Government. The Presiding Officer will hold office for a term of 5 years from the date on which he enters upon his office or until he attains the age of 65 years, whichever is earlier.

Cyber Regulations Appellate Tribunal being an appellate body has the power to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Information Technology Act, 2000 is absolute. This impliedly bars the jurisdiction of civil courts to hear such appeals.

It grants an unconditional right of appeal to any aggrieved party, who has been aggrieved by an order made by Controller or an adjudicating officer under this Act. Further, the appeal before the Tribunal shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the Adjudicating Officer is received by the person so aggrieved.

---

80 **48. Establishment of Cyber Appellate Tribunal.**

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in subsection (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

81 **49. Composition of Cyber Appellate Tribunal.**

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

82 **51. Term of office**

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

83 **57. Appeal to Cyber Appellate Tribunal.**

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.
It is the Cyber Regulations Appellate Tribunal’s judicial function to give the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

Under the Act, the emphasis is on employing all ‘judicial means’ to dispose off the appeal finally within six months from the date of receipt of the appeal [S.57 (6)].

The Act further provides a second forum of appeal in the form of the High Court (the first being the Cyber Regulations Appellate Tribunal) to any person aggrieved by any decision or order of the Cyber Regulations Appellate Tribunal. An appeal is to be filed within sixty days from the date of communication of the decision or order of the Cyber Regulations Appellate Tribunal to him on any question of fact or law arising out of such order [S.62]°4.

The Cyber Regulations Appellate Tribunal is a ‘one member body’. It has been given the statutory authority to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Act.

So far, no Presiding Officer of Cyber Regulations Appellate Tribunal has been appointed by the Central Government.

3.1.5.4. The National Association of Software and Service Companies (NASSCOM)

National Association of Software and Service Companies (NASSCOM), is the premier trade body and the chamber of commerce of the IT software and services industry in India. NASSCOM’s member companies are in the business of software development, software services, software products and IT-enabled/BPO services. NASSCOM acts as an advisor, consultant and coordinating body for the software and services industry in India.

In 2000, NASSCOM urged the government to pass a data protection law to ensure the privacy of information supplied over computer networks and to meet European data protection standards°5. This initiative led to the adoption of an “IT Action Plan” and to the adoption of the IT Act.

3.2. The Indian Contract Act, 1872

The Indian Contract Act offers an alternative solution to protect data. This Act is an “existing law”, which has been defined under Article 366(10) as “any law, Ordinance, order, bye-law, rule or regulation passed or made before the commencement of this Constitution by any

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

°4 62. Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

Legislature, authority or person having power to make such a law, Ordinance, order, bye-law, rule or regulation”.

The Indian Contract Act 1872 extends to the whole of India, except the State of Jammu and Kashmir86.

Contract as a subject matter is mentioned as Entry 7 (‘Contracts, including partnership, agency, contracts of carriage, and other special forms of contract, but not including contracts relating to agricultural land’) of the Concurrent List (List III).

Article 254 of the Constitution87 states that in case of inconsistency between laws made by Parliament and laws made by the Legislatures of States88, the law made by Parliament, whether passed before or after the law made by the Legislature of such State, or, as the case may be, the existing law, shall prevail and the law made by the Legislature of the State shall, to the extent of the repugnancy, be void.

Article 254(2) engrafts an exception: if the President assents to a State law, which has been reserved for his consideration, it shall prevail in that State, notwithstanding its repugnancy to an earlier law of the Union. The predominance of the State law may however be taken away if Parliament legislates under the proviso to Clause (2) of Article 254.

Thus, “Contract” being an entry in List III can be legislated by both Centre and State. The present law on contracts is an existing law. The States can legislate on it but the provisions of the State enactment should not be repugnant to the Indian Contract Act, 1872. If they are repugnant, they would be void to the extent of repugnancy. It is imperative to note here that as on date, there has not been even a single State amendment to Indian Contract Act, 1872.

According to this Act, when a party commits a breach of contract, the other party is entitled to receive compensation for any loss or damage caused to it, or, in exceptional cases, the court may direct the “specific performance” of the contract against the party in default.

86 the State of Jammu and Kashmir has been given a special status under Article 370 of the Constitution of India
87 254. Inconsistency between laws made by Parliament and laws made by the Legislatures of States.—
(1) If any provision of a law made by the Legislature of a State is repugnant to any provision of a law made by Parliament which Parliament is competent to enact, or to any provision of an existing law with respect to one of the matters enumerated in the Concurrent List, then, subject to the provisions of clause (2), the law made by Parliament, whether passed before or after the law made by the Legislature of such State, or, as the case may be, the existing law, shall prevail and the law made by the Legislature of the State shall, to the extent of the repugnancy, be void.

(2) Where a law made by the Legislature of a State with respect to one of the matters enumerated in the Concurrent List contains any provision repugnant to the provisions of an earlier law made by Parliament or an existing law with respect to that matter, then, the law so made by the Legislature of such State shall, if it has been reserved for the consideration of the President and has received his assent, prevail in that State:
Provided that nothing in this clause shall prevent Parliament from enacting at any time any law with respect to the same matter including a law adding to, amending, varying or repealing the law so made by the Legislature of the State.
88 A State law would be repugnant to the Union law when there is a direct conflict between the two laws. Such repugnancy may arise where both laws operate in the same field with respect to one of the matters enumerated in List III and the two cannot possibly stand together.
Hence, Indian companies acting as ‘data importers’ may enter into contracts with ‘data exporters’ to adhere to a high standard of data protection. These contracts are binding and may fulfil the requirements of overseas customer(s) national legislations.

For example, if the data exporter in the EU and the data importer in India use the standard contractual clauses of the Commission of 2001 (2001/497/EC) or 2004 (“alternative set” of standard contractual clauses), the data importer is expected to honour its undertakings under the contract and treat the data with the level of data protection and limitations reflected in the contract.

Moreover, increasingly, outsourcing/BPO contracts are also incorporating clause(s) on international arbitration for dispute resolution. For example, such contracts often provide choice of law provision, which may include arbitration rules of UNCITRAL, ICC (Paris), London Court of International Arbitration (LCIA) etc. Furthermore, Indian outsourcing/BPO companies are accepting that the governing law under the Agreement(s) and any action arising hereunder shall be construed in accordance with and be governed by the substantive and procedural laws of the customer’s national laws without regard to the conflict of laws provisions thereof. They are also submitting themselves to the exclusive jurisdiction of customer’s national courts and forums.

In some cases, Indian outsourcing/BPO companies are also accepting process of mediation to resolve the dispute. For example, companies are agreeing to dispute resolution by non-binding mediation under the International Mediation Rules of the International Centre for Dispute Resolution of the American Arbitration Association (“ICDR”).

Finally, some Indian IT companies like WIPRO, INFOSYS, TCS, active in the IT/ BPO sector presently have a very stringent policy dealing with protection of their client’s information and all the employees are contractually bound to protect the confidential information which may be processed. The employment contracts clearly specify that the employees have to maintain as secret and confidential all such information which the company specifies from time to time.89 From all these examples, one could claim, that on an informal basis, there are attempts being made by Indian companies to ensure privacy of data although in many cases it may not be dealing specifically personal data.

89 Following is the provisions dealing with confidentiality in the employment contract of a leading Indian IT company WIPRO

“In consideration of the opportunities training and access to new technologies and know how that will be made to you, you will be required to comply with the confidentiality policy of the company. Therefore please ensure that you maintain as secret and confidential all Confidential Information (as defined from time to time in the confidentiality policy of the company) and shall not use or divulge or disclose any such Confidential Information except as may be required under obligation of law or as may be required by WIPRO and in the course of your employment. The covenant shall endure during your employment and for a period of one year from the cessation of your employment with WIPRO (irrespective of the circumstances of, or the reasons for, the cessation)

In your work for WIPRO, you will be expected not to use or disclose any confidential information, including trade secrets, of any former employer or other person with whom you have an obligation of confidentiality and by signing below you affirm that you have no conflicting obligations or non-compete agreements that would prevent you from working without limitation for WIPRO Technologies”
3.3. Credit Information Companies (Regulation) Act, 2005

The Credit Information Companies (Regulation) Act, 2005 was passed in May 2005 and notified in the Gazette of India on June 23, 2005. The Act was passed with a view to regulate credit information companies and to facilitate efficient distribution of credit and for matters concerned or incidental to it.

It has laid down provisions vis-à-vis “information privacy principles and furnishing of credit information” (Chapter VI).

3.3.1. Scope of regulated “data processors”

The Act imposes duties on:
- *Credit information company* defined as “a company formed and registered under the Companies Act, 1956 (1 of 1956) and which has been granted a certificate of registration under sub-section (2) of Section 5”;
- *Credit Institution* defined as a banking company and including—
  (i) a corresponding new bank, the State Bank of India, a subsidiary bank, a co-operative bank, the National Bank and regional rural bank;
  (ii) a non-banking financial company;
  (iii) a public financial institution ;
  (iv) the financial corporation established by a State;
  (v) the housing finance institution;
  (vi) the companies engaged in the business of credit cards and other similar cards and companies dealing with distribution of credit in any other manner;
- *Specified user* defined as “any credit institution, credit information company being a member under subsection (3) of Section 15, and includes such other person or institution as may be specified by regulations made, from time to time, by the Reserve Bank for the purpose of obtaining credit information from a credit information company”;

3.3.2. Scope of regulated information

The Act focuses on *credit information* defined as “any information relating to

(i) the amounts and the nature of loans or advances, amounts outstanding under credit cards and other credit facilities granted or to be granted, by a credit institution to any borrower;

(ii) the nature of security taken or proposed to be taken by a credit institution from any borrower for credit facilities granted or proposed to be granted to him;

(iii) the guarantee furnished or any other non-fund based facility granted or proposed to be granted by a credit institution for any of its borrowers;

(iv) the creditworthiness of any borrower of a credit institution;

(iv) any other matter which the Reserve Bank may, consider necessary for inclusion in the credit information to be collected and maintained by credit information companies, and, specify, by notification, in this behalf;”
3.3.3. Provisions pertaining to data protection in this Act

- Section 19 Accuracy and security of credit information

A credit information company or credit institution or specified user, as the case may be, in possession or control of credit information, shall take such steps (including security safeguards) as may be prescribed, to ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

This section requires data to be accurate. If that principle seems to be similar to the one enshrined within the European directive, its scope remains rather limited since:

- Only the credit institution, the credit information company and the specified user must take measures to ensure the accuracy and the limited access and disclosure of the information maintained by them;
- Only credit information are concerned by this provision, there is no such obligation for other kind of information

- Section 20 Privacy principles.

Section 20(b) provides for a purpose principle. Every credit institution, credit information company and specified user must determine the purpose for which the information may be used and restrict use and disclosure on such use.

Section 20(c) imposes to every credit institution, credit information company and specified user to determine the extent of their obligation to check accuracy of credit information before furnishing these information to credit institution, credit information company and specified user. This Section imposes a duty of accuracy on these institutions.

90 Every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to collection, processing, collating, recording, reservation, secrecy, sharing and usage of credit information, namely:

(a) the principles

(i) which may be followed by every credit institution for collection of information from its borrowers and clients and by every credit information company, for collection of information from its member credit institutions or credit information companies, for processing, recording, protecting the data relating to credit information furnished by, or obtained from, their member credit institutions or credit information companies, as the case may be, and sharing of such data with specified users;

(ii) which may be adopted by every specified user for processing, recording, preserving and protecting the data relating to credit information furnished, or received, as the case may be, by it;

(iii) which may be adopted by every credit information company for allowing access to records containing credit information of borrowers and clients and alteration of such records in case of need to do so;

(b) the purpose for which the credit information may be used, restriction on such use and disclosure thereof;

(c) the extent of obligation to check accuracy of credit information before furnishing of such information to credit information companies or credit institutions or specified users, as the case may be;

(d) preservation of credit information maintained by every credit information company, credit institution, and specified user as the case may be (including the period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information);

(e) networking of credit information companies, credit institutions and specified users through electronic mode;

(f) any other principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations.
Section 20(d) lays down principles regarding the preservation of information maintained by every credit information company, credit institution, and specified user: the period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information.

Section 20(f) foresees that the Reserve Bank may take regulations containing principles and procedures relating to credit information.

- **Section 21 Alteration of credit information files and credit reports**
  
  This provision foresees two principles contained in the European directive:

  - **The right to access:** any person may, when applying for a grant or sanction of credit facility, request a copy of the credit information. The request must be done to the credit institution. The access right is limited to credit information obtained by the credit institution from the credit information company.
  
  - **The right of rectification:** Any client or borrower may request that the information detained by a credit information company, a specified user or a credit institution in possession or control of credit information, shall be updated. Updating the information can be done by making an appropriate correction or addition or by every other mean. Only the credit information detained by the sub above institutions are concerned, this limits the scope of this principle.

3.3.4. Regulations made under Section 20(f)

The Credit Information Companies (Regulation) Act, 2005 required Rules and Regulations to be notified under the Act. While the Central government was empowered to make the Rules,

---

91 Any person, who applies for grant or sanction of credit facility, from any credit institution, may request to such institution to furnish him a copy of the credit information obtained by such institution from the credit information company.

Every credit institution shall, on receipt of request under sub-section (1), furnish to the person referred to in that sub-section a copy of the credit information subject to payment of such charges.

If a credit information company or specified user or credit institution in possession or control of the credit information, has not updated the information maintained by it, a borrower or client may request all or any of them to update the information; whether by making an appropriate correction, or addition or otherwise.

92 **36. Power to make rules.**—

(1) The Central Government may, after consultation with the Reserve Bank, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing powers, such rules may provide for all or any of the following matters, namely:—

(a) the authority or tribunal which may be designated under sub-section (1) of Section 7;

(b) the steps to be taken by every credit information company or credit institution and specified user for ensuring accuracy, completeness of data and protection of data from any loss or unauthorised access or use or disclosure under Section 19;

(c) the form in which a declaration of fidelity and secrecy shall be made under sub-section (2) of Section 29;

(d) any other matter which is required to be, or may be, prescribed.

(3) Every rule made by the Central Government under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.
the Reserve Bank was powered to make the Regulations\textsuperscript{93} to carry out the purpose of the Act. Accordingly, the Reserve Bank has prepared the Regulation for implementation of the Credit Information Companies (Regulation) Act, 2005 and placed them on their website for a feedback from stakeholders. Those Regulations provide among others:

- The privacy principles which will guide the credit information companies, credit institutions and specified users. These encompass accuracy, security, secrecy, adequacy of data collected as also limitation on the use of data, that is, the purpose for which the Credit Information Report can be made available and the procedure to be followed by specified uses for getting reports.

- A procedure by which an individual can file a complain against a credit information company, a credit institution or a specified user for contravening any provisions of the Act.

Rules have also been established.

Neither the rules, nor the Regulations have been adopted so far.

3.3.5. Regulations made by the Reserve Bank in exercise of the powers conferred by Section 37(2) of the Credit Information Companies (Regulation) Act, 2005

3.3.5.1. Introduction – General concepts

On April 5, 2006, the Reserve Bank of India published on its website Regulations pertaining to data protection. In Chapter I, the Reserve Bank defines some concepts which are relevant for this study.

\textsuperscript{93} 37. Power of Reserve Bank to make regulations.—

(1) The Reserve Bank may make regulations consistent with the provisions of this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing powers, such regulations may provide for all or any of the following matters, namely:—

(a) the persons or institutions which may be specified as specified users under clause (1) of Section 2;

(b) the form in which application may be made under sub-section (1) of Section 4 and the manner of filing such application under that sub-section;

(c) any other form of business in which a credit information company may engage under clause (e) of subsection (1) of Section 14;

(d) the form of notice for collection and furnishing of information procedure relating thereto and purposes for which credit information may be provided under sub-sections (1) and (2) of Section 17;

(e) the principles and procedures relating to credit information which may be specified under clause (f) of Section 20;

(f) the amount which may be required to be paid for obtaining copy of credit information under sub-section (2) of Section 21;

(g) the maximum amount of charges payable under Section 27.

(3) Every regulation, as soon as may be after it is made by the Reserve Bank, shall be forwarded to the Central government and that Government shall cause a copy of the same to be laid before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation, or both Houses agree that the regulation should not be made, the regulation shall, thereafter, have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.
For the first time, the concept of personal data is defined as “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of the credit information company”.

This definition is quite similar to the European definition of personal data since it encompasses every information on an identifiable individual. The exclusion of some information pertaining to employees is comprehensible given the aim of the Act.

The concepts of “collector”\(^{94}\) and “subject of information”\(^ {95}\) are also defined. It is also noteworthy to precise that, according to Section 37(2)(a), the Reserve Bank has listed some companies which can be regarded as specified user\(^ {96}\).

3.3.5.2. Privacy Principles

Chapter VI provides for privacy principles which aim to guide every credit information companies, credit institutions and specified users.

a) Principle 1. Care in Collection of Credit Information\(^ {97}\)

Every credit information company must ensure that all the information it collects or receives are:
- properly and accurately recorded, collated and processed;

---

\(^{94}\) "collector" means a credit institution, or a credit information company, or a specified user, as the case may be, which collects data, information, or credit information in respect of a borrower;

\(^{95}\) "subject of information" means one to whom the data, information or credit information, relate to and includes a borrower, client and a person;

\(^{96}\) 3. In addition to what has been provided in the Section 2(l) and Section 15 (8) of the Act, each of the companies specified hereunder shall be regarded, for the purpose of the Act, as a specified user; namely:-
(a) an insurance company as defined under the Insurance Act 1938 and registered with Insurance Regulatory and Development Authority;
(b) a company providing cellular/phone services and registered with Telecom Regulatory Authority of India;
(c) a rating agency registered with Securities and Exchange Board of India.
(d) a broker registered with Securities and Exchange Board of India;
(e) a trading member registered with a recognized Commodity Exchange;
(f) Securities Exchange Board of India; and
(g) Insurance Regulatory and Development Authority.

\(^{97}\) Care in Collection of Credit Information
Credit Information Company’s obligations
9.1.1. The Credit Information Company shall ensure that all necessary precautions are taken that all information received or collected by the Credit Information Company is:
9.1.1.1 Properly and accurately recorded, collated and processed;
9.1.1.2 Protected against loss;
9.1.1.3 Protected against unauthorised access, use, modification or disclosure.

Credit Institution’s Obligation
9.1.2 Each Credit Institution shall supply to the Credit Information Company information and data relating to its borrowers / Clients in the format as specified in Form ‘D’.
9.1.3 Each Credit Institution shall regularly update information on a monthly basis and data supplied to the Credit Information Company and take necessary steps to ensure that the information supplied by it, including the updates, are accurate, complete, correct and current.
- protected against loss;
- protected against unauthorised access, use, modification or disclosure.

Each credit institution must update information on a monthly basis and take measures to supply update, accurate, complete, correct and current information to the Credit Information Companies.

As summarized by the Article 29 Working Party, the data quality and proportionality principles require that data should be accurate and where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

The principle enunciated here above ensures the updating as well as the accuracy while collecting credit information (by both Credit Information Companies and Credit Institution).

b) Principle 2. Data Security and secrecy

The credit information companies, the credit institutions and the specified users must establish security and other procedures in accordance with the rules under the Act.

Principles are also laid down with respect to the employees:
- The credit information companies employees must sign a suitable declaration of fidelity and secrecy;
- The credit institution and the specified users must establish procedures for authorizing their employees to handle credit information. They must also ensure that credit information will be transferred and received through a secure medium.

The principle of security, as it is summarized by the Article 29 Working Party, requires that technical organisational measures should be taken by the data controller that are appropriate to the risks presented by the processing. This could be fulfilled by the requirements of Principle 2: security procedures must be established —we will examine them later— and organisational measures regarding the employees are foreseen.

98 Data Security and secrecy

Credit Information Company’s Obligation
9.2.1 Credit Information Company shall apply security and other procedures in accordance with the Rules under the Act.
9.2.2 Credit Information Company shall arrange for all its employees to sign a suitable declaration of fidelity and secrecy.

Credit Institution’s Obligation
The Credit Institutions shall:
9.2.3 Establish and enforce clear procedures for authorizing its employees to handle credit information on a need to know basis.
9.2.4 Establish security and other procedures in accordance with the rules under the Act.
9.2.5 Credit information shall be transferred through a secure medium.

Specified User’s Obligations
9.2.6 Credit Information Company shall apply security and other procedures in accordance with the Rules under the Act.
9.2.7 Establish and enforce clear procedures for authorizing its employees to handle credit information on a need to know basis.
9.2.8 Establish security and other procedures in accordance with the rules under the Act.
9.2.9 Credit information shall be received through a secure medium.
c) Principle 3. Access and Modification

Credit information companies and credit institution must establish procedures to allow a person to access record or information pertaining to him. The person must make a request and prove its identity.

The Credit Institution has the obligation to set up a procedure for fees to be charged to any individual for making copies of his record.

A right to modification is also foreseen in this principle:
- The credit information company must make the correction or addition or otherwise and take appropriate steps to update the credit information within 15 days after being requested to do so by a Credit Institution or Specified User.
- The credit institution must establish procedures to examine a request from a person concerning an amendment to a record or an information pertaining to him. The credit institution must take a decision and notify it to the credit information company within 30 days of the receipt of the request.

This principle comes close to the principles of access and rectification as summarized by the Article 29 Working Party: the data subjects should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. Moreover, the credit information companies have a general obligation to update information.

d) Principle 4. Data Collection Limitation

---

99 Access and Modification Credit Information Company’s Obligation
9.3.1 The Credit Information Company shall establish procedures for the disclosure to a person upon his request of his record or information pertaining to him on proper identification.
9.3.2 The Credit Information Company shall indicate reasonable times, places and requirements for establishing identity of a person, who requests his record or information pertaining to him before it makes the record or information available to the person.
9.3.3 The Credit Information Company in possession or control of the credit information shall make the correction or addition or otherwise and take appropriate steps to update the credit information within 15 days after being requested to do so by a Credit Institution or Specified User.

Credit Institution’s Obligation
9.3.4 Establish procedures for the disclosure to a person of his record or information pertaining to him that has been furnished to a credit information company upon his request and proper identification.
9.3.5 Indicate reasonable times, places and requirements for identifying person who requests his record or information pertaining to him before the Credit Institution shall make the record or information available to the individual.
9.3.6 Establish procedures for reviewing a request from a person concerning the amendment of any record or information pertaining to him. The Credit Institution will take a decision in the matter and notify the Credit Information Company of such amendment within 30 days of the receipt of the request.
9.3.7 Establish procedure for fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

100 DATA COLLECTION LIMITATION
Credit Information Company’s Obligation
9.4.1 Nature of data collected
The data collected shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected. Given below is an illustrative (but not exhaustive) list of the items of data, which will normally be collected by the Credit Information Company:
This principle provides for a proportionality principle as it is foreseen in the European directive. It requires that the data collected by the credit information companies must be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected. The principle is defined using exactly the same terms as the European ones.

e) Principle 5. Data Use Limitation

9.4.1.1 In the case of individuals - name, father's name, address, gender, date of birth, contact telephone numbers, PAN, driving license, passport, voter identity card numbers etc. and or any other information for the purpose of identifying the individual.

9.4.1.2 In the case of non-individuals - name, address, contact numbers, line of activity, Balance Sheet and Profit & Loss Account and particulars in respect of the proprietor/ partners/ directors/ guarantors on the lines of those for individuals as stated above.

9.4.1.3 In case of both, the details of accounts of the borrower such as credit limit, outstanding balance, repayment history, amount and period of default, if any, as well as of primary/collateral security taken.

Credit Institution's Obligation

9.4.2 The credit institution shall not withhold any data as required to be submitted in the reporting format provided by credit information company.

Credit Information Company's Obligation

9.5.1 Supply of credit information reports (CIRS) – permissible purposes:
The Credit Information Company will make available CIRs for the following purposes only:

9.5.1.1 To a Specified User for purposes as indicated in Regulation 10.5.3 below and to another credit information company.

9.5.1.2 To comply with the order of any court, tribunal, law enforcement agency or statutory/regulatory authority under an applicable law and subject to due process of law.

9.5.1.3 To a borrower other than individual, upon its own request, credit information pertaining to itself against payment of fees.

9.5.1.4 To an individual against his/her request, credit information pertaining to himself/herself against payment of a nominal fee not exceeding Rs.100/- and on identifying himself/herself.

9.5.1.5 For such purpose as the Reserve Bank may specify in this regard, from time to time.

9.5.2 Review of usage by members:
Credit Information Company will have in place, policy and procedures to monitor and review on a regular and ongoing basis, access, collection and usage of a CIR by the Specified User, with a view to detecting and investigating any unusual or irregular patterns of use by them.

Specified User's obligation

9.5.3 Drawing of reports by Specified Users -
Specified Users will be entitled to request for, access and use Credit Information Reports for the following purposes:

9.5.3.1 To take a credit decision on a person who has made a written application to the specified user to avail of/extend/ renew/ review /enhance financial assistance or other products offered by it.

9.5.3.2 To take a credit decision on a person who accepts liability for payment on a bill of exchange drawn by a person who has applied to the specified user for an availment/ extension/ renewal/ enhancement/review of credit.

9.5.3.3 To take a credit decision on a person who draws a promissory note in favour of person who has applied to the Specified User for an availment / extension/ renewal/ enhancement/ review of credit.

9.5.3.4 To take a credit decision on a person who proposes to act as guarantor for a person who has applied to the Specified User for an availment / extension/ renewal/ enhancement/ review of credit.

9.5.3.5 To make informed and objective credit decisions.

9.5.3.6 To deter concurrent borrowers and serial defaulters.

9.5.3.7 To Keep adverse selection of customers to the minimum.

9.5.3.8 To review and evaluate risk of its customers.

9.5.3.9 To effectively discharge the statutory / regulatory functions. This has been included for Specified Users which are regulators like SEBI, IRDA, PFRDA etc.

9.5.3.10 To effectively discharge the functions as a credit rating agency.

9.5.3.11 For such purpose as the Reserve Bank may specify in this regard, from time to time

9.5.4 Credit Information Reports-- non-permissible purposes
The Specified Users shall not request for, access, collect or use Credit Information Reports for any purpose whatsoever other than those listed under Clause 5.3.
This principle lays down the permissible purposes for which credit information companies may make available credit information reports (CIRs). Some of these permissible purposes are:
- to comply with the order of a court, tribunal,…;
- upon the request of a borrower other than individual for credit information pertaining to itself against payment of fees;
- upon the request of an individual for credit information pertaining to himself against payment of a nominal fee (not exceeding Rs 100) and on identifying himself.

This principle also precises the purposes for which specified users may request access and use CIRs.

An obligation to disclose has also been foreseen when a borrower is denied credit or any other service on the basis of Credit Information Report. In this case, the specified user who has denied the credit should send the specific reasons for rejection along with a copy of the said credit information report. It must also give the borrower/client the name and address of any Credit Information Company that issued a report and if other information was used in making the decision, the borrower has right to learn about that information.

f) Principle 6. Data Accuracy

This principle imposes the duty on credit information companies to make all possible efforts to ensure accuracy and completeness of data.

The credit institution is responsible of the correctness and accuracy of the data submitted to the credit information company and has the an obligation of monthly updating (or shorter intervals if agreed so).

Specified users must establish procedures to ensure that they are using latest credit information relating to the person in respect of whom a credit decision is to be taken.

This completes the obligations laid down in Principle 1.

---

9.5.5 Obligation to disclose
When a borrower is denied credit or any other service on the basis of Credit Information Report, the Specified User who has denied the credit should send the borrower/client a written rejection notice within 30 days of the decision stating the specific reasons for rejection along with a copy of the said credit information report. It must also give the borrower/client the name and address of any Credit Information Company that issued a report and if other information was used in making the decision, the borrower has right to learn about that information.

102 Data Accuracy

Credit Information Company’s Obligation
9.6.1 The Credit Information Company shall make all possible efforts to ensure accuracy and completeness of data.

Credit Institution’s Obligation
9.6.2 Credit Institution shall be responsible for the correctness and accuracy of the data submitted to the Credit Information Company.
9.6.3 Credit institution shall ensure updates of the data given by them to credit information company on monthly intervals or on shorter intervals as may be mutually agreed upon.

Specified User’s Obligation
9.6.4 Specified Users will establish procedures to ensure that they are using latest credit information relating to the person in respect of whom a credit decision is to be taken.
g) Principle 7. Archiving/Length of Preservation

The credit information company and credit institution shall retain all information collected and disseminated for a minimum of 7 years.

There is a different regime for information relating to criminal offences (which shall be of permanent nature) and information relating to financial default or civil offences (which shall be removed from the history after 7 years from the date of first reporting).

It is important to note that all information regarding non-individuals shall be of permanent nature.

It is foreseen that personal information in respect of an individual that is no longer required in terms of sub-regulations 9.7.1 and 9.7.2 should be destroyed, erased or made anonymous. Credit information companies and credit institutions shall develop guidelines and implement procedures to govern the destruction of personal information.

h) Section 16 Solicitation of personal data from individual concerned

This Section provides for a transparency obligation when requiring that a credit institution must, when requiring personal data from an individual, for inclusion in a credit information report or in a generally available publication, inform the individual of:

---

103 Archiving/Length of Preservation

9.7.1 The Credit Information Company and Credit Institution shall retain all information collected and disseminated for a minimum of 7 years.

9.7.2 Information relating to criminal offences in respect of an individual shall be of permanent nature in the credit information pertaining to a person while information relating to financial default or civil offences shall be removed from the history after 7 years from the date of first reporting. All information regarding non-individuals shall be of permanent nature.

9.7.3 Personal information in respect of an individual that is no longer required in terms of sub-regulations 9.7.1 and 9.7.2 should be destroyed, erased or made anonymous. Credit Information Companies and Credit Institutions shall develop guidelines and implement procedures to govern the destruction of personal information.

104 Solicitation of personal data from individual concerned:

Where a credit institution collects personal data for inclusion in a credit information report or in a generally available publication, and such data is solicited by the credit institution from an individual concerned, the credit institution shall take such steps as are, in the circumstances, reasonable to ensure that, before such data is collected or, if that is not practicable, as soon as practicable after such data is collected:

(a) the individual concerned is informed of:

(i) the purpose for which such data is being collected, and if the collection of such data is authorised or required by or under any law in force, the fact that the collection of such data is so authorised or required; and

(ii) any person to whom, or anybody or agency to which, it is the collector's usual practice to disclose personal data of the kind so collected.

(b) the collector shall ensure having regard to the purpose that:

(i) the personal data collected is relevant to such purpose and is up to date and complete;

(ii) the collection of such data does not intrude to an unreasonable extent upon the personal affairs of the individual concerned; and

(iii) such data maintained by the collector is protected by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorized access, use, modification or disclosure, and against any misuse.
(i) the purpose for which such data is being collected, and if the collection of such data is authorised or required by or under any law in force, the fact that the collection of such data is so authorised or required; and

(ii) any person to whom, or anybody or agency to which, it is the collector's usual practice to disclose personal data of the kind so collected.

This principle is quite similar to the transparency principle as defined by Article 29 Working Party: the transparency principle requires that individuals should be provided with the information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. Nevertheless, Section 16 doesn’t encompass indirect collection of data as this is foreseen in the European directive.

This Section also provides for obligation of proportionality and security for the collector of data.

i) Section 19. Remedies to individuals

This Section foresees the possibility for individuals to file complaint before the Reserve Bank against a credit information company, credit institution or specified user for contravening any provisions of the Act.

The Reserve Bank is empowered to impose penalty or reprimand credit information company, credit institution or specified user having contravened the Act.

j) Section 18. Procedure to be adopted

---

105 19. REMEDIES TO INDIVIDUALS:
(1) An individual may file before the Reserve Bank a written complaint against a credit information company, credit institution or specified user, as the case may be for contravening any provisions of the Act.
(2) On receipt of a complaint under sub-regulation, the Reserve Bank, may if so satisfied prima-facie about the alleged contravention, issue notice to the concerned Credit Information Company, Credit Institution or Specified User, as the case may be, calling upon them to show cause as to why the amount specified in the notice should not be imposed on the company for the alleged contravention;
Provided, that before imposing such penalty, reasonable opportunity of being heard shall also be given to such Credit Information Company, Credit Institution or the Specified User, as the case may be.
(3) If in the opinion of the Reserve Bank, the allegation made against such Credit Information Company, Credit Institution or the Specified User, is found to be proved, the Reserve Bank may;
(a) impose such penalty as it may deem appropriate, in accordance with the Act; or
(b) reprimand such erring Credit Information Company, Credit Institution or the Specified User, as the case may be.

106 18. Procedure to be adopted: Every Credit information company shall include in their policies and practices to give effect to the principles and procedure in relation to;
(a) protection of personal data;
(b) accepting complaints, enquiries and disposal thereof;
(c) imparting training to their staff about their policies and practices with respect to credit information; and
supply of brochures for information of the public in respect thereof;
(d) establishing one or more compliance committees to oversee the suitability, adequacy of the practice and procedure adopted by them and application thereof in their functions; and
(e) adoption of appropriate documentation in relation to their members for furnishing and collecting data, information and credit information.
This Section imposes adaptation of the credit information companies policies and practices to the principles and procedures in relation to:

(a) protection of personal data;
(b) accepting complaints, enquiries and disposal thereof;
(c) imparting training to their staff about their policies and practices with respect to credit information; and supply of brochures for information of the public in respect thereof;
(d) establishing one or more compliance committees to oversee the suitability, adequacy of the practice and procedure adopted by them and application thereof in their functions; and
(e) adoption of appropriate documentation in relation to their members for furnishing and collecting data, information and credit information.

This Section ensures a proper enforcement.

3.3.5.3. Regulations made by the Government in exercise of the powers conferred by Section 36 of the Credit Information Companies (Regulation) Act, 2005

These Rules foresee some procedures that must be taken by credit institution, credit information company and specified user to ensure accuracy, completeness and protection of data, prohibition of unauthorised access, use or disclosure and fidelity and secrecy obligations.

a) Chapter III. Steps and security safeguards to be taken by credit institution for ensuring accuracy completeness and protection of data

This Chapter provides for rules and procedures that must be taken by every credit institution to ensure accuracy, completeness and protection of data.

Rule 20. Steps for Security and Safeguards to be taken by Credit Institution

This Rule imposes on every credit institution a duty to **elaborate appropriate policy and safeguards procedure** specifying the steps and security safeguards that must be adopted:

- in their operation relating to collection, processing and collating of data by them relating to their identified borrower;
- steps for security and protection of the data and the credit information maintained at their end; and

---

107 Section 20. 20. Steps for Security and Safeguards to be taken by Credit Institution.

Every credit institution, in existence in India on the commencement of these rules, before the expiry of three months from such commencement, and every other credit institution before the expiry of three months of commencing their business in India, shall formulate appropriate policy and procedure, duly approved by its board of directors, specifying therein the steps and security safeguards, to be adopted generally in their operation relating to:

(a) collection, processing and collating of data by them relating to their identified borrower;
(b) steps for security and protection of the data and the credit information maintained at their end; and
(c) appropriate and necessary steps for maintaining, an accurate, complete and updated data and credit information, in respect of their identified borrower, and to ensure the accuracy and completeness thereof while furnishing the same to a credit information company or making disclosure thereof to anyone else, in accordance with the Act.
appropriate and necessary steps for maintaining, an accurate, complete and updated data and credit information, in respect of their identified borrower, to ensure the accuracy and completeness thereof while furnishing the same to a credit information company or making disclosure thereof to anyone else, in accordance with the Act.

This Rule relates to the principle of data quality and security since it provides for an obligation for the credit institution to elaborate policies and procedures to ensure data’s accuracy and security.

**Rule 21. Collection of Data and Maintaining Credit Information**

This Rule states that credit institutions may collect relevant data pertaining to its identified borrower and the possible guarantor, when it is necessary and appropriate to maintain data and credit information accurate and complete. A procedure must be taken to fulfil this obligation

This relates to the principle of proportionality.

**Rule 22. Accuracy of data provided by a credit institution**

(1) A credit institution may:
(a) collect all such relevant data in respect of its identified borrower and the guarantor or the person who has given or has proposed to give guarantee or offer security for the borrower, as it may deem necessary and appropriate for, maintaining an accurate and complete data and credit information, in respect of the borrower; and
(b) shall use subject to the provisions of the Act, an appropriate and generally accepted procedures with utmost due diligence, for such purpose.

(2) Without prejudice to the generality of the policy and procedure adopted as per rule 20 and sub-rule (1), with respect to collection of data and maintaining credit information, a credit institution shall also collect and include all relevant and authentic available data and information as per Form-II for;
(a) establishing the identity of the borrower;
(b) relating to the credit facilities granted or to be granted, by a credit institution to the borrower; and
(c) other information.

(1) Before furnishing data or an information or credit information to a credit information company or making disclosure thereof to anyone else, in accordance with the Act, every credit institution shall adopt an appropriate and generally accepted procedures with utmost due diligence to check and ensure that, the credit information is accurate and complete with reference to the date on which such information is so furnished or disclosed.

(2) If for any reason beyond its control, it is not possible for the credit institution to furnish credit information, complete as per sub-rule
(1), the credit institution while furnishing the credit information to a credit information company or making disclosure thereof to anyone else, in accordance with the Act, shall make a remark to such effect with reference to the date up to which the accuracy and completeness of the credit information, has been verified and found to be correct.

(3) Subject to provisions of sub-sections (2) and (3) of section 21 of the Act, the manner and time as provided therein and the provisions of the regulations, in respect of alteration and updating of credit information on request of a borrower in accordance with said provisions, if a credit institution after furnishing the data or information or credit information, to a credit information company or making disclosure thereof to anyone else, in accordance with the Act, discovers of its own, or is informed about, any inaccuracy, error or discrepancy therein the credit institution shall;
(a) latest by third working day, send the intimation to the credit information company or the individual, as the case may be, of such inaccuracy, error or discrepancy;
(b) take immediate steps to correct such inaccuracy, error or discrepancy; and
According to this Rule, every credit institution must adopt an appropriate and generally accepted procedures, before furnishing data or an information or credit information to a credit information company or disclose them to anyone else, to check and ensure that, the credit information is accurate and complete with reference to the date on which such information is so furnished or disclosed.

This Rule completes the data quality principle, imposing introduction of procedures to ensure data quality before disclosure to credit information companies and other persons.

This Rule further provides that if for any reason beyond its control, it is not possible for the credit institution to furnish complete and updated credit information, the credit institution, while furnishing the credit information must make a remark to such effect with reference to the date up to which the accuracy and completeness of the credit information has been verified and found to be correct.

If a credit institution after furnishing the data or information, discovers of its own, or is informed about, any inaccuracy, error or discrepancy therein the credit institution must:

- send the intimation to the credit information company or the individual, as the case may be, of such inaccuracy, error or discrepancy;
- take immediate steps to correct such inaccuracy, error or discrepancy;
- the credit institution must forward the corrected data or information to the credit information company or the individual, within period of 15 days from the date of inaccuracy’s discovery. If the credit institution cannot comply with this provision, it must inform the credit information company.

In case of failure, without sufficient reason, the credit institution will be liable for contravention of the provisions of the Act.
All those principles reinforce the principle of data quality.

Rule 23. Disclosure of disputed data by a credit institution

(c) the credit institution shall forward the corrected particulars of the data or information or credit information, to the credit information company or the individual, as the case may be, within period of fifteen days from the date when the credit institution had discovered such inaccuracy, error or discrepancy or information in respect thereof was given to it.

(4) A credit institution failing to take steps as per clause (a) to (c) of sub-rule (3), without any sufficient reason shall be liable for contravention of the provisions of the Act.

(5) If for any reason beyond its control it is not possible for a credit institution to take immediate steps as per clause (c) of sub-rule (3), the credit institution shall inform the credit information company or the individual, as the case may be, of the steps taken by it at their end for correction of such inaccuracy, error or discrepancy and also the reasons for its inability to comply with the provisions of clause (c) of sub-rule (3) within the time stipulated therein.

If in the opinion of a credit institution, correction of any inaccuracy, error or discrepancy as referred to in the rule 22, is likely to take further time on account of any dispute raised by the borrower in respect thereof, with the credit institution or before a court of law, or any forum, or tribunal or any other authority, in such cases the credit institution shall;

(a) while furnishing such data or information or credit information to a credit information company or making disclosure thereof to anyone else, in accordance with the Act, include an appropriate remark to reflect the nature of the inaccuracy, error or discrepancy, found therein and the pendency of the dispute in respect thereof and in

110 23. Disclosure of disputed data by a credit institution.
This Rule foresees procedure to ensure data accuracy when correction of any inaccuracy is likely to take further time on account of any dispute raised by the borrower in respect thereof, with the credit institution or before a court of law, or any forum, or tribunal or any other authority.

In such case, the credit institution must include an appropriate remark to reflect the nature of the inaccuracy and the pendency of the dispute while furnishing the data or information to credit information companies or, if the data or information have already been furnished, inform the credit information company.

Rule 24. Updating of the credit information by Credit Institution

This Rule imposes a general obligation of updating data. When there is any change in the data, information or credit information, already furnished to a credit information company, credit institution must continue to update such data, information or credit information promptly or in any event, by the end of each reporting period not exceeding 30 days, until the termination of the respective account relating to such credit information and furnish the updated credit information to the credit information company at the earliest possible opportunity.

Rule 25. Data security and system integrity safeguards

A credit institution shall adopt an appropriate and generally accepted procedures with utmost due diligence and take all such measures in its daily operations as may be necessary to safeguard and protect the data, information and the credit information maintained at its end against any improper access to or mishandling of the same including the following; namely:

(a) the minimum standards for physical and operational security including site design, fire protection, environmental protection;
(b) round the clock physical security;
(c) instructions for removing, labelling and securing the removable electronic storage media at the end of the session or working day;
This Rule obliges credit institutions to adopt appropriate and generally accepted procedures and to take all such measures in its daily operations as may be necessary to safeguard and protect the data, information and the credit information against any improper access or mishandling.

This Rule reinforces the security principle since it provides examples of technical and organisational measures (comprehensive succession plan for the key personnel to ensure that non-availability of a person does not disrupt the system, procedure for change of software and hardware, disaster recovery and management plan, …).

b) Chapter IV. Steps and security safeguards to be taken by credit information companies and, specified user for ensuring accuracy, completeness and protection of data

Rule 26. Formulation and adoption of the procedure by Credit Information Company

(d) physical access to the critical systems to be on dual control basis;
(e) comprehensive succession plan for the key personnel to ensure that non-availability of a person does not disrupt the system;
(f) paper based records, documentation and backup data containing all confidential information to be kept in secure and locked containers or filing system, separately from all other records;
(g) procedure to ensure that the records to be accessed by authorized persons on need to know basis;
(h) details of creation of firewalls and stress testing of systems through ethical hacking to evaluate and ensure its robustness;
(i) protecting systems against obsolescence;
(j) procedure for change of software and hardware;
(k) disaster recovery and management plan; and
(l) steps to be taken when handing over systems for maintenance to prevent unauthorized access or loss of data.

113 26. Formulation and adoption of the procedure by Credit Information Company.

(1) Every credit information company in existence on the commencement of these rules, shall within three months of the commencement of these rules, and every credit information company to whom a certificate of registration has been granted in accordance with the Act after the commencement of these rules shall within three months of such grant consider and decide the requisite steps, as it may deem necessary to be adopted generally in their operation and formulate policy and procedure duly approved by its board of directors and adopt the same with respect to their following operations namely:-
(a) collection, processing and collating of data, information and the credit information relating to their identified borrower, obtained and received by them from a member credit institution or credit information company, as the case may be;
(b) steps for security and protection of such data, information and the credit information maintained at their end; and
(c) appropriate and necessary steps for maintaining, an accurate, complete and updated data, information and credit information, in respect of their identified borrower, and to ensure the accuracy and completeness thereof while furnishing the same to a specified user or making disclosure thereof to anyone else, in accordance with the Act;
(2) Without prejudice to the generality of the policy as formulated and procedure as adopted, under sub-rule (1), every credit information company shall include in its such policy and procedure, the following namely:-
(a) the minimum number of identification parameters that must be satisfied before crystallizing the identity of a borrower;
(b) essential criterion in relation to the extent of tolerance limit against each parameter within which each identification parameter will be considered to be satisfied;
(c) the procedure and parameters for verifying and certifying that the entire data, information and the credit information, obtained and received by them, from a member credit institution, a credit information company, or from any other permissible source, as the case may be, in respect of their identified borrower, has been collated without any distortion thereof and such collated data, information and credit information maintained with the credit information company inaccurate, updated and complete up to the date of such certification;
This Rule imposes on every credit information company a duty to consider and decide the requisite steps, as it may deem necessary to be adopted generally in their operation and formulate and adopt policy and procedure in respect with:

- collection, processing and collating of data, information and the credit information relating to their identified borrower obtained and received by them from a member credit institution or credit information company;
- steps for security and protection of the data, information and the credit information maintained at their end; and
- appropriate and necessary steps for maintaining, an accurate, complete and updated data, information and credit information, in respect of their identified borrower, to ensure the accuracy and completeness thereof while furnishing the same to a credit information company or making disclosure thereof to anyone else, in accordance with the Act.

Every credit information company must include in its policy and procedure:

- the minimum number of identification parameters that must be satisfied before crystallizing the identity of a borrower;
- essential criterion in relation to the extent of tolerance limit against each parameter within which each identification parameter will be considered to be satisfied;
- the procedure and parameters for verifying and certifying that the entire data, information and the credit information, obtained and received by them, from a member credit institution, a credit information company, or from any other permissible source, in respect of their identified borrower, has been collated without any distortion thereof and such collated data, information and credit information is accurate, updated and complete up to the date of such certification;
- the procedure for making a notation, in the data, information or credit report obtained and received from a member credit institution, or a credit information company, or from any other permissible source, in respect of their identified borrower;
- inclusion of condition in their policy and procedure that if a member credit institution or a credit information company after forwarding the data, information or credit information, in respect of an identified borrower to a credit information company has failed to take necessary steps for updating and completing their earlier forwarded data, information or credit information, in the time as specified in the regulation in this behalf, the

(d) the procedure for making a notation, in the data, information or credit report obtained and received by them from a member credit institution, or a credit information company, or from any other permissible source, as the case may be and maintained at their end in respect of their identified borrower is not found to be updated on the date of carrying out necessary verification and certification thereof as per clause (c) of sub rule (2), with reference to the date up to which the same was certified at their end to be accurate, updated and complete; and
(e) inclusion of condition in their policy and procedure that if a member credit institution or a credit information company after forwarding the data, information or credit information, in respect of an identified borrower to a credit information company has failed to take necessary steps for updating and completing their earlier forwarded data, information or credit information, within the time as specified in the regulation in this behalf, the recipient credit information company shall, within three working days from such specified time, enquire and ascertain from such credit institution or the credit information company, as the case may be, the reason for their such failure.
recipient credit information company must, within three working days from such specified time, enquire and ascertain from such credit institution or the credit information company, the reason for their such failure.

Rule 27. Accuracy of data provided by a credit institution or credit information company

This Rule imposes the same duties as the ones imposed to the credit institutions in Rule 22:

According to this Rule, every credit information company must adopt an appropriate and generally accepted procedure, before furnishing data, information or credit information to a specified user or disclose them to anyone else, to ensure that:

- the procedures laid down under Rule 26 have been duly complied;
- the identity of the identified borrower has been duly verified (according to the policy and procedure set up on this behalf);
- the data, information or credit information to be furnished or disclosed in respect of such borrower is accurate, complete and updated with reference to the date mentioned therein.

114 27. Accuracy of data provided by a credit institution or credit information company

(1) Before furnishing data, information or credit information, in respect of an identified borrower to a specified user or making disclosure thereof to anyone else, in accordance with the Act, every credit information company shall by applying an appropriate and generally accepted procedure with utmost due diligence verify and ensure that:
(a) its policy and procedure adopted as per rule 26, in relation to clause(a) to (c) of sub-rule (1) and clause (a) to (e) of sub – rule (2) thereof, has been duly complied with and all the verification, certification as per said provisions has been made;
(b) the identity of the identified borrower has been duly verified as per the parameters included in this behalf in said policy and procedure ; and
(c) the data, information or credit information to be furnished or disclosed in respect of such borrower is accurate, complete and updated with reference to the date mentioned therein.

(2) If for any reason beyond its control, it is not possible for the Credit Information Company to furnish complete and updated data, information or credit information, as per sub-rule (1), the Credit Information Company shall make a remark therein to such effect with reference to the date up to which its accuracy and completeness has been verified and found to be correct.

(3) Subject to provisions of sub-sections (2) and (3) of section 21 of the Act, in respect of alteration and updating of credit information on request of a borrower, for which the credit institution shall follow the manner and time as specified therein and in the regulations, if a Credit Information Company, after furnishing the credit information to a specified user or making disclosure thereof to anyone else, in accordance with the Act, discovers of its own, or is informed about, an inaccuracy, error or discrepancy in respect of the data, information or credit information, the Credit Information Company shall;
(a) latest by third working day, send the intimation to the specified user or the individual, as the case may be, of such inaccuracy, error or discrepancy, provided that it would not be necessary to send the intimation if the information was supplied by the Credit Information Company more than one year ago;
(b) take immediate steps to correct the inaccuracy, error or discrepancy found; and
(c) the Credit Information Company shall forward the corrected particulars of the data, information or credit information, to the specified user or the individual, as the case may be, within period of fifteen days from the date when the Credit Information Company had discovered or was informed of such inaccuracy, error or discrepancy.

(4) If it is not possible for the Credit Information Company to furnish corrected information within a period of fifteen days as per clause (c) of sub-rule (3), for any reason beyond its control, the Credit Information Company shall inform the specified user or the individual, as the case may be, of the steps taken by it at their end for correction of such inaccuracy, error or discrepancy and also its inability to comply with the provisions of clause (c) of sub-rule (3);
(5) A Credit Information Company failing to take steps as per clause (a) to (c) of sub-rule (3), without any sufficient reason for its inability to comply with said provisions, shall be liable for contravention of the provisions of the Act.
This Rule further provides that if for any reason beyond its control, it is not possible for the credit information company to furnish complete and updated data, information or credit information, the credit information company, while furnishing the credit information must make a remark to such effect with reference to the date up to which the accuracy and completeness of the data, information or credit information has been verified and found to be correct.

If a credit information company after furnishing the data, information or credit information, discovers of its own, or is informed about, any inaccuracy, error or discrepancy therein the credit information company must:

- send the intimation to the specified user or the individual, as the case may be, of such inaccuracy, error or discrepancy;
- take immediate steps to correct such inaccuracy, error or discrepancy;
- forward the corrected data, information or credit information to the specified user or the individual, within period of 15 days from the date of inaccuracy’s discovery. If the credit institution cannot comply with this provision, it must inform the specified user or the individual.

In case of failure, without sufficient reason, the credit information company will be liable for contravention of the provisions of the Act.

**Rule 28. Disclosure of disputed data by a credit institution**

This Rule foresees procedure to ensure data accuracy when correction of any inaccuracy is likely to take further time on account of any dispute raised by the borrower in respect thereof, with the credit institution or before a court of law, or any forum, or tribunal or any other authority.

In such case, the credit information company must include an appropriate remark to reflect the nature of the inaccuracy and the pendency of the dispute while furnishing the data, information or credit information to the specified user or making disclosure thereof to anyone.

In the opinion of a Credit Information Company, correction of any inaccuracy, error or discrepancy in respect of the data, information or credit information, discovered by or informed to, the Credit Information Company, as referred to in the rule 22, is likely to take further time on account of any dispute raised by the borrower in respect thereof, with the credit institution or before a court of law, or any forum, or tribunal or any other authority, in such cases the Credit Information Company shall;

(a) while furnishing such data, information or credit information to a specified user or making disclosure thereof to anyone else, in accordance with the Act, include an appropriate remark to reflect the nature of the inaccuracy, error or discrepancy therein and the pendency of the dispute in respect thereof and in any subsequent disclosure of such disputed data, information or credit information, the Credit Information Company shall also disclose such remark;

(b) in case such data, information or credit information has already been furnished to a specified user or disclosed to anyone else, the credit information company shall inform the specified user or the individual, as the case may be, to include remark of such inaccuracy, error or discrepancy therein and the pending dispute in respect thereof provided that it would not be necessary to send the intimation if the information was supplied by the credit information company more than one year ago; and

(c) in such cases, as per provided under provisions of second proviso to sub-section (3) of section 21 of the Act, the entries in books of the concerned credit institution shall be taken into account for the purposes of credit information relating to such borrower.
else, or, if the data, information or credit information have already been furnished, inform the specified user or individual.

Rule 29. Formulation and adoption of the procedure by Specified user\textsuperscript{116}

Every specified must:

- consider and decide steps as it may deem necessary for ensuring and verifying the accuracy and completeness of data, information or credit information, received from a credit information company, before using the same in relation to an identified borrower;
- protection thereof from unauthorized disclosure, or use and;
- formulate and adopt an appropriate policy and procedure in this behalf.

Every specified user shall include in its such policy and procedure:

- the level of officers who will be authorized to access the data, information and credit information received from a Credit Information Company;
- the minimum number of identification parameters that must be satisfied before crystallizing the identity of a borrower;
- the minimum number of parameters which shall be satisfied to decide that the credit information accessed is in respect of the same borrower for whom the credit decision is to be taken;
- the procedure to be adopted by the specified user, while accessing the credit information maintained by a Credit Information Company, so as to take notice of any remark included by the Credit Information Company in respect of the credit information;

Every specified user must adopt and apply all such measures in its daily operations, as are provided under rule 25 with respect to data security and system integrity safeguards for

\textsuperscript{116} 29. Formulation and adoption of the procedure by Specified user

(1) Every Specified user in existence on the commencement of these rules, shall within three months of the commencement of these rules, and every Specified user coming into existence after the commencement of these rules, shall within three months of its commencing its business, consider and decide such requisite steps as it may deem necessary for ensuring and verifying the accuracy and completeness of data, information or credit information, received from a credit information company, before using the same in relation to an identified borrower, protection thereof from unauthorized disclosure, or use and formulate and adopt an appropriate policy and procedure in this behalf, duly approved by its board of directors.

(2) Without prejudice to the generality of the policy as formulated and procedure as adopted, under sub-rule (1), every Specified user shall include in its such policy and procedure, the following namely:-

(a) the level of officers who will be authorized to access the data, information and credit information received from a Credit Information Company;
(b) the minimum number of identification parameters that must be satisfied before crystallizing the identity of a borrower;
(c) the minimum number of parameters which shall be satisfied to decide that the credit information accessed is in respect of the same borrower for whom the credit decision is to be taken;
(d) the procedure to be adopted by the specified user, while accessing the credit information maintained by a Credit Information Company, so as to take notice of any remark included by the Credit Information Company in respect of the credit information; and
(e) every specified user shall adopt and apply all such measures in its daily operations, as are provided under rule 25 with respect to data security and system integrity safeguards for ensuring the protection of the data and the credit information obtained from a credit information company, against any improper access, use or mishandling thereof.
ensuring the protection of the data and the credit information obtained from a credit information company, against any improper access, use or mishandling thereof.

c) Chapter V. Prohibition from unauthorised access or use or disclosure

Rule 30. Prohibition from unauthorized access or use or disclosure

Every credit information company or credit institution or specified user, in possession or control of data and credit information, shall adopt procedures to ensure that only authorized persons are permitted to access or use or disclose data relating to the credit information maintained by them.

(1) Every credit institution, credit information company, and every specified user, existing before the commencement of these rules shall within three months of such commencement of these rules, and every credit institution, credit information company or specified user coming into existence after the commencement of the rules shall within three months of the commencement of their business, consider and decide such requisite steps, as they may deem necessary to ensure, that the data, information and the credit information maintained at their end, is duly protected against an unauthorized access and formulate and adopt an appropriate policy and procedure in this behalf duly approved by its board of directors.

(2) Without prejudice to the generality of the policy as formulated and procedure as adopted, under sub-rule (1), every credit institution, credit information company, and every specified user, shall include in its such policy and procedure to ensure the application of procedure and caution and secure the object as provided hereinafter namely:

i) policy and procedure to secure the confidentiality of the data, information and credit Information maintained at their end;

ii) policy and procedure to ensure that access to the data, information and credit Information maintained at their end is permitted only to such of their managers or employees or designated officers, who are duly authorized for the purpose on a need to know basis;

iii) policy and procedure to ensure and control, access to the data, information and credit Information, terminals, and networks, maintained at their end, by means of physical barriers including biometric access control and logical barriers by way of passwords;

iv) policy and procedure to ensure that the passwords used in this behalf is not shared by anyone else than who is authorized in this behalf and the passwords are changed frequently but on irregular intervals;

v) policy and procedure to ensure that the best practices in relation to the deletion and disposal of data, especially where records or discs are to be disposed of off-site or by external contractors, are followed;

vi) policy and procedure to ensure that the system adopted for the purpose shall provide for protection against an unauthorized modification or deletion of the data, information and credit information maintained at their end;

vii) policy and procedure to ensure maintenance of log of all accesses to data, including the following namely:-

(a) the identity of the person seeking access to the data or credit information maintained at their end;

(b) the date and time of such access;

(c) the identity of the borrower whose data or credit information were so accessed; and

(d) the records and entries pertaining to such log is preserved for minimum period of for 2 years and the same could be available for examination by auditors / or by the Reserve Bank, as the case may be;

viii) policy and procedure to ensure that the records and entries pertaining to maintenance of log of all unsuccessful attempts to access data or credit information maintained at their end, all incidents involving a proven or suspected breach of security in respect thereof including therein ;

(a) the requisite particulars the records affected, if any and action taken in respect of such access; and

(b) procedure for security incidence reporting and response;

ix) maintenance and review of records and entries of log, on a regular and frequent basis to detect and investigate any unusual or irregular patterns of use of or access to data including creation of the audit trails and verification thereof;

x) the format for disclosure of credit information;

xi) the circumstances in which the credit information can be disclosed;

xii) the use to which credit information can be put;

xiii) training of staff in good security practices;

xiv) guidelines for the use and access of information systems by external contractors; and

xv) protection against pilferage of information while passing through the public and private networks.
Every credit information company or credit institution or specified user, in possession or control of data and credit information, must adopt procedures to ensure that only authorized persons are permitted to access or use or disclose data relating to the credit information maintained by them.

Steps must be taken by every credit institution, credit information company and specified user to:
- ensure and verify the accuracy and completeness of data, information or credit information, received from a credit information company, before using the same in relation to an identified borrower;
- ensure protection thereof from unauthorized disclosure, or use; and
- formulate and adopt an appropriate policy and procedure in this behalf.

Specific provisions must be incorporated in those general procedures and policies to prevent any unauthorized access. These provisions foresee organisational as well as technical measures.

d) Chapter VI Fidelity and secrecy

Rule 31. Obligation for Fidelity and Secrecy

Every credit information company or credit institution or specified user, in possession or control of data, information and credit information must adopt all reasonable procedures to ensure that their managers, officers, employees are obliged to fidelity and secrecy in respect of credit information under their control or to which they have access.

General policies must be adopted to this end. These policies must also contain specific rules foreseeing that:

(3) Without prejudice to the generality of the procedure adopted under sub-rule (1), every credit information company shall enter into a formal written agreement with the specified users specifying therein;
(a) extent of their obligation to comply with the rules in providing and in utilizing the data, information and credit information;
(b) the types of controls and procedures to be applied in the event of the specified user seeking access to the database of the credit information company; and
(c) method to apply controls to ensure that only the data to which specified user is entitled are released.

31. Obligation for Fidelity and Secrecy

Every credit information company or credit institution or specified user, in possession or control of data, information and credit information shall adopt all reasonable procedures to ensure that their managers, officers, employees are obliged to fidelity and secrecy in respect of credit information under their control or to which they have access.

(1) Every credit information company or credit institution or specified user existing before the commencement of these rules shall within three months of such commencement of these rules and every credit institution or credit information company or specified user within three months of commencement of their business after coming into force of the rules shall formulate the policy and procedure duly approved by its board of directors specifying therein the steps to be taken by them to ensure compliance of the fidelity and secrecy obligation by their managers, officers, employees with respect to data, information and credit information under their control.

(2) Without prejudice to the generality of the policy and procedure as adopted under sub-rule (1), such policy and procedure shall include the following; namely:
(a) their employees, authorized personnel, agents, contractors and other persons who deal with or have right to access data, information and credit information shall comply with confidentiality obligation and shall sign covenants with them;
(b) their every chairperson, director, member, auditor, advisor, officer or other employee of shall, before entering upon his duties, make a declaration in Form III for complying with such fidelity and secrecy obligation.
employees, authorized personnel, agents, contractors and other persons who deal with or have right to access data, information and credit information must comply with confidentiality obligation and shall sign covenants with them; 
- every chairperson, director, member, auditor, advisor, officer or other employee must, before entering upon his duties, make a declaration in Form III\(^{119}\) for complying with such fidelity and secrecy obligation.

3.4. The Public Financial Institutions Act of 1993

This Act codifies India’s tradition of maintaining confidentiality in bank transactions.

In India the bankers have an obligation to maintain secrecy of the account. The account of the customer in the books of the bank records all his financial dealings and depicts the true state of his financial position. If any third party is able to get free access to such records his reputation may suffer. The banker is therefore under an obligation to take utmost care in keeping secrecy about the accounts of its customers. Thus the banker cannot disclose any information regarding his customer’s accounts to a third party and he has to ensure that all necessary precautions are taken to prevent any such information leak. In the case of Kattabomman Transport Corporation Ltd. v. State Bank of Travancore and others\(^{120}\), it was held that among the duties of the banker towards the customer is the duty of secrecy, which arises out of the banker customer relationship. However it needs to be mentioned that the duty of the banker to maintain secrecy is not an absolute one, there are some exceptions, when the law requires such disclosures to be made or when the practices and usages permit such disclosure.

3.5. The Indian Telegraph Act

Wiretapping is regulated under the Telegraph Act of 1885. Due to numerous phone taps scandals, the Supreme Court defined wiretaps as “serious invasion of an individual’s privacy”\(^{121}\).

The Indian Telegraph Act of 1885 in its article 5 allows authorities to intercept messages.

5. Power for government to take possession of licensed telegraphs and to order interception of messages

(1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government, or any officer specially authorised in this behalf by the Central Government or a State Government, may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

\(^{119}\) See Form III annexed to the Rules  
\(^{120}\) AIR 1992 Ker.351, The leading case in England is Tournier v. National Provincial Bank of England (1924) 1 KB 461 (CA)  
(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the government making the order or an officer thereof mentioned in the order:

Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

According to section 7(2)(b), the Government may prescribe rules providing precautions to be taken for preventing the improper interception or disclosure of messages but it has been highlighted in the PUCt v Union of India 1996 Case that no such rules have been enacted by the Government at that time. However, in the context of wiretapping by the government, the Supreme Court laid out guidelines defining who can tap phones and under what circumstances:

- Only the Union Home Secretary, or his counterpart in the States, can issue an order for a tap;
- The government must prove that this is the only mean to obtain the sought information;
- The Court mandated the development of a high-level committee to review the legality of each wiretap.\(^\text{122}\)

3.6. Common Law

Unlawful attacks on the honor and reputation of a person can invite an action in Tort and-or Criminal law. Moreover, under the case law of Torts in India, the right to privacy in a way protects females from observation. The Bombay High Court had held that an invasion of privacy is an actionable wrong and that a man may not open new doors or windows in his house, or make any new apertures or enlarge old ones in a way which will enable him to overlook those portions of his neighbour’s premises which are ordinarily secluded from observation and so intrude upon his privacy.\(^\text{123}\) In another interesting case where a window opened by the defendant gave a view, not of the plaintiff’s private apartments, but of an open courtyard outside his house, it was held that there has been no invasion of the plaintiff’s privacy which would have forced the defendant to keep the windows closed for ever.\(^\text{124}\)

The Allahabad High Court had held that the customary right of privacy is confined to the protection of pardanashin women\(^\text{125}\) and to those parts of the house which are ordinarily occupied by females and which have been so occupied and used for a period sufficiently long to establish a right of privacy.\(^\text{126}\)

---

\(^{123}\) Nathubhai v. Chhaganlal (1900) 2 Bom LR 454
\(^{124}\) Keshav Harsha v. Ganapat Hirachand (1871) 8 BHCR (ACJ) 87.
\(^{125}\) Generally Muslim women wearing purdah, which is a kind of veil to cover their body including face
\(^{126}\) Bholan Lal v. Altaf Hussein, ILR (1945) All 607
4. Procedural/ Enforcement Mechanisms

4.1. Absence of any Data Protection Authority in India

Since there isn’t any Data Protection Authority in India, the system of courts, as described above, is the main vector by which individuals can obtain a remedy.

4.2. Specific Relief Act

A mature legal system endeavours to provide not merely a remedy for every right infringed, but also an adequate remedy. The Specific Relief Act provides that effective remedial action.

It provides preventive relief in the form of temporary and perpetual injunctions (sections 37 and 38) to the plaintiff to prevent the breach of an obligation existing in his favour, whether expressly or by implication. For example, a person can move against any service provider to a court and plead for issuing injunction against a service provider, if he feels that the service provider is not fulfilling its contractual obligations or preventing the breach of an obligation existing in his favour. The court can perpetually enjoin the defendant (service provider) from the assertion of a right, or from the commission of an act, which would be contrary to the rights of the plaintiff.

Further, the plaintiff in a suit for perpetual injunction under section 38, or mandatory injunction under section 39, may claim damages either in addition to, or in substitution for, such injunction and the court may, if it thinks fit, award such damages (section 40).

5. Industry codes of practice

There is no industry specific code of practice related to privacy. Nevertheless, most of the companies in outsourcing/BPO space have their respective code of practice related to privacy.

Conclusion

Certain points can be pinpointed:

- The Supreme Court of India has construed a general Right to Privacy from Article 21 of the Constitution. However, this Right is not absolute as it can be curtailed according to a procedure established by law or when there is a superior countervailing interest. This right is also limited to the first generation of rights (the first cases of the Supreme Court only involve domiciliary visits). No general right relating to personal data protection has been developed so far;

- The Indian conception of privacy is rather different from the European one. From this perspective, it is interesting to note that the Right to Privacy is also used in India to protect women’s right as well as to protect home from police intrusion;

session, it is often quoted in India as an Act containing provisions pertaining to data protection. The research has analyzed several provisions but, according to us, none of them seems to offer an adequate protection. The concept of “personal data” is not even defined. Moreover, the contractor considers that the proposed amendments to this Act – which have not been adopted so far – will not be sufficient to ensure an adequate protection within the meaning of Directive 95/46/EC. In general, the IT Act is more an Act related to e-commerce and cyber crime than a data protection Act.

- The Indian Contract Act provides for an alternative solution for European data exporters. As explained above, Indian data importers may be asked to sign a contract imposing them duties pertaining to data protection. Nevertheless, this remains a subsidiary solution.

- The Credit Information Companies (Regulation) Act, 2005 contains certain provisions ensuring data protection but it is limited in its scope. It only imposes duties on credit information companies, credit institutions and specified users while processing credit information. This Act foresees rules pertaining to the credit information accuracy and security, contains a purpose limitation principle, foresees a period of credit information preservation, a right to access and a right of rectification. However it does not contain rules ensuring a comprehensive right to information. Moreover, no specific authority has been established to ensure the respect of these provisions under this Act. Nevertheless, Rules and Regulations that could be adopted under Article 20(f) of this Act could provide for an adequate protection in the field of credit information.

- Regarding the procedural and enforcement mechanisms, the research has analyzed the different ways of enforcement: general ones (courts and tribunals system) as well as specific ones (under the IT Act, Rules and Regulations that could be adopted under the Credit Information Companies Act, etc…). Given the absence of any general data protection Act, no Data Protection Authority has been established in India. However, it is noteworthy to precise that Regulations taken by the Reserve Bank of India – still not adopted – foresees, in Section 19, that the Reserve Bank is empowered to impose penalty or reprimand any credit information company, credit institution or specified user having contravened the Act. On this ground, the Reserve Bank could be considered as a specific Data Protection Authority in the field of credit information. Nevertheless, a more in-depth analysis will be needed to determinate its role and powers.