Fundamentals of Cyber Law

Rohas Nagpal
Asian School of Cyber Laws

Most of us are like overflowing cups - too full of opinions and prejudices. To see the light of wisdom, we must empty our cup a little.

Published in 2019 by Asian School of Cyber Laws.

Printed in India

The chosen case scenarios are for instructional purposes only and any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by Asian School of Cyber Laws, and the information and statements shall not be used for the purposes of advertising.

Contents

ONE

1. Introduction to Cyber Law

1.1 What is Cyber Law?

In order to arrive at an acceptable definition of the term Cyber Law, we must first understand the meaning of the term law.

Simply put, **law** encompasses the rules of conduct:
(1) that have been approved by the government, and

(2) which are in force over a certain territory, and

(3) which must be obeyed by all persons on that territory. Violation of these rules will lead to government action such as imprisonment or fine or an order to pay compensation.

The term **cyber** or **cyberspace** has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc) and even electronic devices such as cell phones, ATM machines etc.

Thus, a simplified **definition of cyber law** is that it is the "law governing cyber space".

The issues addressed by cyber law include:

- Cyber crime[1],
- Electronic commerce[2],
- Intellectual Property in as much as it applies to cyberspace[3],
- Data protection & privacy[4]

[1] An interesting definition of cyber crime was provided in the "Computer Crime: Criminal Justice Resource Manual" published in 1989. According to this manual, cyber crime covered the following:
(1) computer crime i.e. any violation of specific laws that relate to computer crime,
(2) computer related crime i.e. violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution,
(3) computer abuse i.e. intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more perpetrators made or could have made gain and / or one or more victims suffered or could have suffered loss.

[2] The term electronic commerce or Ecommerce is used to refer to electronic data used in commercial transactions. Electronic commerce laws usually address issues of data authentication by electronic and / or digital signatures.

[3] This encompasses (1) copyright law in relation to computer software, computer source code, websites, cell phone content etc (2) software and source code licenses (3) trademark law with relation to domain names, meta tags, mirroring, framing, linking etc (4) semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts (5) patent law in relation to computer hardware and software.

[4] Data protection and privacy laws address legal issues arising in the collecting, storing and transmitting of sensitive personal data by data controllers such as banks, hospitals, email service providers etc.

1.2 Need for Cyber Law

The first question that any student of cyber law must ask is whether there is a need for a separate field of law to cover cyberspace. Isn't conventional law adequate to cover cyberspace?

Let us consider cases where so-called **conventional crimes are carried out using computers** or the Internet as a tool. Consider cases of spread of pornographic material, criminal threats delivered via email, websites that defame someone or spread racial hatred etc. In all these cases, the computer is merely incidental to the crime. Distributing pamphlets promoting racial enmity is in essence similar to putting up a website promoting such ill feelings.

Of course it can be argued that when technology is used to commit such crimes, the effect and spread of the crime increases enormously. Printing and distributing pamphlets even in one locality is a time-consuming and expensive task while putting up a globally accessible website is very easy.

In such cases, it can be argued that conventional law can handle cyber cases. The Government can simply impose a stricter liability (by way of imprisonment and fines) if the crime is committed using certain specified technologies. A simplified example would be stating that spreading pornography by electronic means should be punished more severely than spreading pornography by conventional means[5].

[5] Section 292 of the Indian Penal Code relates to 'sale, distribution, import, export etc of an obscene book, pamphlet, paper, drawing, painting, representation etc'. The punishment provided under this section is imprisonment upto 2 years and fine upto Rs 2000 [on first conviction] and imprisonment upto 5 years and fine upto Rs 5000 [on subsequent conviction].

As long as we are dealing with such issues, conventional law would be adequate. The challenges emerge when we deal with more complex issues such as **'theft' of data**. Under conventional law, theft relates to "movable property being taken out of the possession of someone"[6].

The General Clauses Act defines movable property as "property of every description, except immovable property". The same law defines immovable property as "land, benefits to arise out of land, and things attached to the earth, or permanently fastened to anything attached to the earth". Using these definitions, we can say that the computer is movable property.

Let us examine how such a law would apply to a scenario where data is 'stolen'. Consider my personal computer on which I have stored some information. Let us presume that some unauthorised person picks up my computer and takes it away without my permission. Has he committed theft? The elements to consider are whether some movable property has been taken out of the possession of someone. The computer is a movable property and I am the legal owner entitled to possess it. The thief has dishonestly taken this movable property out of my possession. It is theft.

On the other hand, section 67 of the Information Technology Act, 2000 penalizes transmitting, publishing etc of lascivious material by electronic means. The punishment provided under this section is imprisonment upto 5 years and fine upto Rs 1 lakh [on first conviction] and imprisonment upto 10 years and fine upto Rs 2 lakh [on subsequent conviction].

[6] Section 378 of the Indian Penal Code defines theft as "Whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft."

Now consider that some unauthorised person simply copies the data from my computer onto his pen drive. Would this be theft? Presuming that the intangible data is movable property, the concept of theft would still not apply as the possession of the data has not been taken from me. I still have the 'original' data on the computer under my control. The 'thief' simply has a 'copy' of that data. In the digital world, the copy and the original are indistinguishable in almost every case.

Consider another example on the issue of **'possession'** of data. I use the email account rohasnagpal@gmail.com for personal communication. Naturally a lot of emails, images, documents etc are sent and received by me using this account. The first question is, who 'possesses' this email account? Is it me because I have the username and password needed to login and view the emails? Or it is Google Inc, because the emails are stored on their computers?

Another question would arise if some unauthorised person obtains my password. Can it be said that now that person is also in possession of my emails, because he has the password to login and view the emails?
Another legal challenge emerges because of the **'mobility'** of data. Let us consider an example of international trade in the conventional world. Sameer purchases steel from a factory in China, uses the steel to manufacture nails in a factory in India and then sells the nails to a trader in USA. The various Governments can easily regulate and impose taxes at various stages of this business process.

Now consider that Sameer has shifted to an 'online' business. He sits in his house in Pune (India) and uses his computer to create pirated versions of expensive software. He then sells this pirated software through a website (hosted on a server located in Russia). People from all over the world can visit Sameer's website and purchase the pirated software. Sameer

collects the money using a PayPal account that is linked to his bank account in a tax haven country like the Cayman Islands.

It would be extremely difficult for any Government to trace Sameer's activities.

It is for these and other complexities that conventional law is unfit to handle issues relating to cyberspace. This brings in the need for a separate branch of law to tackle cyberspace.

1.3 Chronology of the Indian Cyber Law

The outline of the chronological development of Indian cyber laws is as below:

Year	Development
2000	**1.** *Information Technology Act, 2000* came into force **2.** *Indian Penal Code, 1860* amended **3.** *Indian Evidence Act, 1872* amended **4**. *Bankers' Book Evidence Act, 1879* amended **5.** *Reserve Bank of India Act, 1934* amended **6.** *Information Technology (Certifying Authorities) Rules, 2000* came into force **7.** *Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000* came into force
2001	*Information Technology (Certifying Authority) Regulations, 2001* came into force
2002	**1.** *Executive Order* issued **2.** *Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates* issued. **3.** *Information Technology (Removal of Difficulties)*

	Order, 2002 passed. **4.** The Information Technology Act was amended by the *Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002*. **5.** *Cyber Regulations Appellate Tribunal (Salaries, Allowances and Condition of Service of other Officers and Employees) Rules, 2002* were passed.

2003	**1.** *Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003* were passed. ***2.*** *Cyber Regulations Appellate Tribunal (Salary, Allowances and other Terms and Conditions of Service of Presiding Officer) Rules, 2003* were passed. ***3.*** *Information Technology (Other Powers of Civil Court Vested in Cyber Appellate Tribunal) Rules 2003* were passed. **4.** *Information Technology (Other Standards) Rules, 2003* passed. **5.** The *Information Technology (Certifying Authorities) Rules, 2000* were amended. **6**. *The Chhattisgarh Citizen Service (Electronic Governance) Rules, 2003* passed.
2004	**1.** *Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004* passed. **2.** The *Information Technology (Security Procedure) Rules, 2004* passed. **3.** The *Information Technology (Certifying Authorities) Rules, 2000* were amended. **4**. *The Gujarat Information Technology Rules, 2004* were passed. **5**. *The Information Technology (Karnataka) Rules, 2004* were issued.
2006	The *Information Technology (Certifying Authorities) Rules, 2000* were amended.
2007	*The Rajasthan Cyber Cafe Rules, 2007* were passed.
2009	**1.** The *Information Technology (Amendment) Act, 2008* came into force. **2.** *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009* passed. **3.** *Information Technology (Procedure and Safeguard*

	for Monitoring and Collecting Traffic Data or Information) Rules, 2009 passed. **4.** *Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009* passed. **5.** The *Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009* passed. **6.** *Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009* passed. The *Information Technology (Certifying Authorities) Rules, 2000* were amended.
2010	**1**. *The Kerala Information Technology (Electronic Delivery of Services) Rules, 2010* passed.
2011	**1.** *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* passed. **2.** *Information Technology (Intermediaries guidelines) Rules, 2011* passed. **3.** *Information Technology (Electronic Service Delivery) Rules, 2011* passed. **4.** *Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* issued. **5.** A press note, on diligence to be observed by Intermediaries for hosting third party information, was issued. **6.** *Information Technology (Guidelines for Cyber Cafe) Rules, 2011* passed. **7**. *The Andhra Pradesh Information Technology (Electronic Service Delivery) Rules, 2011* were issued. **8**. *The Madhya Pradesh Information Technology (Regulation of Electronic Delivery of Citizen Services*

	and Appointment of Service Provider) Rules, 2011 were passed.
2013	**1.** Clarification on The *Information Technology (Intermediary Guidelines) Rules, 2011* under section 79 of the Information Technology Act, 2000 issued. **2.** *Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013* came into force. **3.** *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013* came into force. **4**. *Information Technology (Salary, Allowances and Terms and Conditions of Service of the Director General, Indian Computer Emergency Response Team) Rules, 2012* were passed on 24th January 2013. **5**. *Information Technology (Recognition of Foreign Certifying Authorities Operating under a Regulatory Authority) Regulations, 2013* came into force. **6**. *Information Technology (Recognition of Foreign Certifying Authorities not Operating under a Regulatory Authority) Regulations, 2013* came into force.
2015	**1.** Unique Identification Authority of India (UIDAI) systems declared as protected systems. **2.** *Digital Signature (End Entity) Rules, 2015* came into force. They deal with long term valid digital signatures. **3.** *Information Technology (Security Procedure) Amendments Rules, 2015* came into force. They make minor amendments to the Information Technology (Security Procedure) Rules, 2004. **4.** *Information Technology (Certifying Authorities) Amendment Rules, 2015* came into force. They make amendments to Information Technology (Certifying Authorities) Rules, 2000

2016	**1.** Indian Computer Emergency Response Team authorised to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. **2.** *Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2016* passed. **3.** *Information Technology (Certifying Authorities) (Amendment) Rules, 2016* passed. **4.** *Cyber Appellate Tribunal (Powers and Functions of the Chairperson) Rules, 2016* passed. **5.** Advisory on Functioning of Matrimonial Websites in accordance with the Information Technology Act, 2000 and Rules issued. **6**. *Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016* passed. **7**. *Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016* passed.

Other important related laws in India:

1. The Telecom Unsolicited Commercial Communication Regulations, 2007
2. The Telecom Commercial Communication Customer Preference Regulations, 2010
3. IN Domain Name Dispute Resolution Policy (INDRP)
4. INDRP Rules of Procedure
5. The Payment and Settlement Systems Act, 2007
6. Payment and Settlement Systems Regulations, 2008
7. Identity Verification Guidelines
8. National Cyber Security Policy, 2013
9. Guidelines for Foreign Direct Investment on E-commerce
10. Mobile Payment in India – Operative Guidelines for Banks

11. Mobile Banking Transactions in India – Customer Registration for Mobile Banking
12. Mobile Banking Transactions in India – Operative Guidelines for Banks
13. Master Circular on Credit Card, Debit Card, and Rupee denominated Co-branded Prepaid card Operations of Banks and Credit Card issuing NBFCs
14. Master Circular on Issuance and Operation of Pre-paid Payment Instruments in India

A brief explanation of these developments is mentioned below.

2000

The primary source of cyber law in India is the *Information Technology Act, 2000* (hereinafter referred to *Information Technology Act or IT Act*) which came into force on 17th October 2000.

The primary purpose of the *Information Technology Act* is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The *Information Technology Act* also penalizes various cyber crimes and provides strict punishments (imprisonment terms up to 10 years and compensation up to crores of rupees).

The *Indian Penal Code* (as amended by the *Information Technology Act*) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital Evidence is to be collected and proven in court as per the provisions of the *Indian Evidence Act* (as amended by the *Information Technology Act*).

In case of bank records, the provisions of the *Bankers' Book Evidence Act* (as amended by the *Information Technology Act*) are relevant.

Investigation and adjudication of cyber crimes is done in accordance with the provisions of the *Code of Criminal Procedure*, *Civil Procedure Code* and the *Information Technology Act*. The *Reserve Bank of India Act* was also amended by the *Information Technology Act*.

On 17th October 2000, the *Information Technology (Certifying Authorities) Rules, 2000* also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities. These rules also lay down the technical standards, procedures and security methods to be used by a Certifying Authority.

The *Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000* also came into force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal whose primary role is to hear appeals against orders of the Adjudicating Officers.

2001

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9th July 2001. They provide further technical standards and procedures to be used by a Certifying Authority.

Two important guidelines relating to Certifying Authorities were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the *Information Technology Act*. These guidelines were issued on 9th July 2001.

2002

An *Executive Order* dated 12th September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate.

Next were the *Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates*. These were issued on 16th December 2002.

Minor errors in the Act were rectified by the *Information Technology (Removal of Difficulties) Order, 2002* which was passed on 19th September 2002.

The *Information Technology Act* was amended by the *Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002*. This introduced the concept of electronic cheques and truncated cheques.

Cyber Regulations Appellate Tribunal (Salaries, Allowances and Condition of Service of other Officers and Employees) Rules, 2002 were passed. This provides for the nature and categories of officers and employees of the Cyber Appellate Tribunal and their scales of pay. Further, the Rules also provide for the regulation of the conditions of service of officers and employees of the Cyber Appellate Tribunal in the matter of pay, allowances, leave, joining time, provident fund, age of superannuation, pension and retirement benefits, medical facilities, conduct, disciplinary matters and other conditions.

2003

On 17th March 2003, the *Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003* were passed.

These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc.

These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the Public Interest Litigation (PIL) filed by students of Asian School of Cyber Laws (ASCL).

The Government had not appointed Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers.

The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this, the Central Government passed an order dated 23rd March 2003 appointing the "Secretary of Department of Information Technology of each of the States or of Union Territories" of India as the adjudicating officers.

The *Cyber Regulations Appellate Tribunal (Salary, Allowances and other Terms and Conditions of Service of Presiding Officer) Rules, 2003* prescribe the salary, allowances and other terms for the Presiding Officer of the Cyber Regulations Appellate Tribunal.

Information Technology (Other Powers of Civil Court Vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the Cyber Regulations Appellate Tribunal.

Also relevant are the *Information Technology (Other Standards) Rules, 2003*. An important order relating to blocking of websites was passed on 27th February, 2003. Under this, Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

The *Information Technology (Certifying Authorities) Rules, 2000* were amended.

The Chhattisgarh Citizen Service (Electronic Governance) Rules, 2003 were passed for effective implementation of e-governance services.

2004

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 have provided the necessary legal framework for filing of documents with the Government as

well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to Government bodies.

The *Information Technology (Security Procedure) Rules, 2004* came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records.

The *Information Technology (Certifying Authorities) Rules, 2000* were amended.

The Gujarat Information Technology Rules, 2004 were passed in order to regulate cyber cafes in the State of Gujarat. The Rules provide for maintenance of log register by cyber cafe owners, the responsibilities of cyber cafe owners, etc.

The Information Technology (Karnataka) Rules, 2004 were issued in order to regulate cyber cafes in the State of Karnataka. The Rules provide for maintenance of log register by cyber cafe owners, the responsibilities of cyber cafe owners, liability in case of non-compliance, etc.

2006

The *Information Technology (Certifying Authorities) Rules, 2000* were amended.

2007

The Rajasthan Cyber Cafe Rules, 2007 were passed with a view to regulate cyber cafes in Rajasthan. The Rules provide for maintenance of log register by cyber cafe owners, the responsibilities of cyber cafe owners, etc.

2009

The *Information Technology (Amendment) Act, 2008*, which came into force on 27th October, 2009 has made sweeping changes to the *Information Technology Act*.

The following rules have also come into force on 27th October, 2009:

(1) *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.*
(2) *Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.*

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

(4) The *Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009*

(5) *Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009*.

The *Information Technology (Certifying Authorities) Rules, 2000* were amended.

2010

The Kerala Information Technology (Electronic Delivery of Services) Rules, 2010 passed to improve delivery of e-services by the Government.

2011

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 passed. These rules define sensitive personal data or information and form the crux of India's data privacy law.

Clarification on *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* were also issued.

Information Technology (Intermediaries guidelines) Rules, 2011 passed. These rules explain the due diligence to be observed by intermediaries.

Information Technology (Electronic Service Delivery) Rules, 2011 passed. These rules relate to the system of Electronic Service Delivery by the Government.

Information Technology (Guidelines for Cyber Cafe) Rules, 2011 passed. This provides for registration of cyber cafes, maintenance of log register, identification of user, etc.

The Andhra Pradesh Information Technology (Electronic Service Delivery) Rules, 2011 were issued to improve delivery of e-services by the Government.

The Madhya Pradesh Information Technology (Regulation of Electronic Delivery of Citizen Services and Appointment of Service Provider) Rules, 2011 were passed to regulate the electronic delivery of citizen services, appointment of service provider and for the purpose of effective implementation of e-governance services.

2013

Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 issued. According to it, intermediaries should have a publicly accessible and published grievance redressal process by which complaints can be lodged. It also clarifies the words "..shall act within thirty-six hours." as mentioned in sub-rule (4) of Rule 3.

Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 came into force. They lay down the functions and duties of the National Critical Information Infrastructure Protection Centre.

Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 came into force. They lay down the detailed functions, responsibilities and services of the Indian Computer Emergency Response Team.

Information Technology (Salary, Allowances and Terms and Conditions of Service of the Director General, Indian Computer Emergency Response Team) Rules, 2012 were passed on 24th January 2013 regulating the qualifications, experience and other terms and conditions of service of the Director General, Indian Computer Emergency Response Team.

Information Technology (Recognition of Foreign Certifying Authorities Operating under a Regulatory Authority) Regulations, 2013 came into force in order to regulate the conduct of Foreign Certifying Authorities in India operating under a regulatory authority.

Information Technology (Recognition of Foreign Certifying Authorities not Operating under a Regulatory Authority)

Regulations, 2013 came into force in order to regulate the conduct of Foreign Certifying Authorities in India not operating under a regulatory authority.

2015

Unique Identification Authority of India (UIDAI) facilities, Information Assets, Logistics Infrastructure and Dependencies declared as protected systems under section 70 of the Information Technology Act.

Digital Signature (End Entity) Rules, 2015 came into force. They deal with long term valid digital signatures.

Information Technology (Security Procedure) Amendments Rules, 2015 came into force. They make minor amendments to the Information Technology (Security Procedure) Rules, 2004.

Information Technology (Certifying Authorities) Amendment Rules, 2015 came into force. They make amendments to Information Technology (Certifying Authorities) Rules, 2000.

2016

Indian Computer Emergency Response Team authorised to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2016 passed. These lay down the manner in which the information is authenticated by means of digital signatures.

Information Technology (Certifying Authorities) (Amendment) Rules, 2016 passed. These rules made a slight correction to the *Information Technology (Certifying Authorities) Rules, 2000*.

Cyber Appellate Tribunal (Powers and Functions of the Chairperson) Rules, 2016 passed. These rules lay down the powers and functions of the Chairperson of the Cyber Appellate Tribunal.

Advisory on Functioning of Matrimonial Websites in accordance with the Information Technology Act, 2000 and Rules issued. According to this advisory, "There have been instances where users of matrimonial websites falsify their marital status, age, height, personality, health, social and economic status. In most of the cases victims are women who fall prey to these fraudsters after getting introduced through fake profiles on matrimonial portal". This advisory has been issued to strengthen protective measures for all users of such websites.

Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 came into force on 26th March 2016. Through this legislation, the government plans to target delivery of subsidies and services by assigning unique identity numbers to individuals residing in India.

Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 were passed for the preservation and retention of information by intermediaries providing Digital Locker Facilities.

1.4 Key Terms and Concepts

1.4.1 Access

According to section 2(1)(a) of the IT Act

*"**access**" with its grammatical variations and cognate expressions means gaining entry into, instructing or*

communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

Essentials of the term "access"

1. Gaining entry into a computer, computer system or computer network.
2. Instructing the logical, arithmetical, or memory function resources of a computer, computer system or computer network.
3. Communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Let us examine the essential elements

Grammatical variations of access include terms such as accesses, accessed, accessing etc.

Cognate expressions are related words and phrases. Depending upon the situation, these could include "log on", "retrieve" etc.

Gaining entry into applies to physical access. The terms computer, computer system and computer network have been defined very widely under the IT Act. These terms may include the physical box (cabinet) in which a computer is housed. They may also include the physical room in which a computer network or super computer is housed.

Illustration: A massive super computer is housed in particular premises. Sameer breaks open the door and enters the premises. He has gained entry into the computer.

Illustration: A Government computer contains critical information in its hard disk. Sameer unscrews the cabinet of the computer in order to steal the hard disk. He has gained entry into the computer.

Instructing means "giving orders" or "directing". Instructing is essentially a one way process which does not require two-way communication between the instructor and the instructed.

Illustration: A Government computer contains critical information. Sameer enters the room where the computer is located and keys in some commands into the keyboard. He does not realise that the keyboard is disconnected from the computer. Here Sameer has **not instructed** the logical, arithmetic or memory functions of the computer.

Illustration: Sameer has set up his computer in such a way that he can remotely shut it down by sending an SMS. The process is:

1. He sends an SMS with the words "shutdown" to a particular service provider.
2. The service provider automatically forwards the contents of the SMS to Sameer's personal email address.
3. Sameer's computer is running an email client (e.g. Microsoft Outlook) that is configured to automatically download emails from his account every 5 minutes.
4. The email client is also configured to run a file called "shutdown.bat" every time it downloads an email with the words "shutdown" in it.
5. This "shutdown.bat" file shuts down Sameer's computer within a few seconds.
6. This enables Sameer to shutdown his computer even when he is not in the same country.

   This is an illustration of instructing the logical, arithmetic or memory functions of the computer.

Communicating with is essentially a two-way process that involves exchange of information.

Illustration: Sameer is a hacker attempting to steal some information from Sanya's computer. He first remotely scans Sanya's computer using specialised software. The software sends out queries to Sanya's computer which replies to the queries. As a result of this, Sameer obtains details of the

operating system installed on Sanya's computer. Sameer has communicated with Sanya's computer.

1.4.2 Computer

According to section 2(1)(i) of the IT Act

"computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

Simply put, a computer has the following characteristics:

1. It is a high-speed **data processing device** or system.
2. It may be **electronic**, **magnetic**, **optical** etc.
3. It performs **logical**, **arithmetic**, and **memory functions**
4. These functions are performed by manipulations of electronic, magnetic or optical impulses.

Computer includes

1. all input facilities,
2. all output facilities,
3. all processing facilities,
4. all storage facilities,

5. all computer software facilities, and

6. all communication facilities

which are connected or related to the computer in a computer system or network.

Let us examine the important terms used in this definition:

According to American law, **electronic** means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. [Title 15, Chapter 96, Sub-chapter I, section 7006(2), US Code].

Magnetic means having the properties of a magnet; i.e. of attracting iron or steel e.g. parts of a hard disk are covered with a thin coat of magnetic material.

Simply put, an **optical computer** uses light instead of electricity to manipulate, store and transmit data.
Optical data processing can perform several operations simultaneously (in parallel) much faster and more easily than electronics.

Optical fibre is the medium and the technology associated with the transmission of information as light pulses along a glass or plastic wire or fibre.

Optical fibre carries much more information than conventional copper wire and is in general not subject to electromagnetic interference.

A **data processing device or system** is a mechanism that can perform pre-defined operations upon information.

The following are illustrations of **functions** in relation to a conventional desktop personal computer.

- saving information on a hard disk,
- logging on to the Internet,
- retrieving stored information,
- calculating mathematical formulae.

Logical functions, simply put, refer to non-arithmetic processing that arranges numbers or letters according to a pre-defined format e.g. arranging numbers in ascending order, arranging words alphabetically etc.

Arithmetic functions, simply put, are operations concerned or involved with mathematics and the addition, subtraction, multiplication and division of numbers.

Memory functions, simply put, refer to operations involving storage of data.

Input facilities are those which transfer information from the outside world into a computer system. E.g. keyboard, mouse, touch screen, joystick, microphone, scanner etc.

Output facilities are those which transfer data out of the computer in the form of text, images, sounds etc to a display screen, printer, storage device etc.

Hard disks, USB disks, floppies, CDs etc. act as both input and output facilities.

Processing facilities primarily refers to the Central Processing Unit (CPU) of a computer. Referred to as the "brain" of the computer, the CPU processes instructions and data.

Storage facilities include hard disks and other data storage facilities. This term would also include the physical cabinet in which a computer is housed.

Computer software facilities refer to the operating system and application software that are essential for a computer to function in a useful manner.

Communication facilities include the network interface cards, modems and other devices that enable a computer to communicate with other computers.

Illustrations: Considering the wide definition given to the term computer by the IT Act the following are examples of "computers":

- desktop personal computers
- mobile phones
- microwave ovens
- computer printers
- scanners
- installed computer software
- Automatic Teller Machine (ATM)
- "smart" homes which can be controlled through the Internet

Case Law

In an interesting case, the Karnataka High Court laid down that **ATMs are not computers**, **but are electronic devices under the Karnataka Sales Tax Act, 1957**.

Diebold Systems Pvt Ltd [a manufacturer and supplier of Automated Teller Machines (ATM)] had sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 (KST Act) on sale of ATMs.

The majority view of the ARA was to classify ATMs as "**computer terminals**" liable for **4% basic tax** as they would fall under Entry 20(ii)(b) of Part 'C' of Second Schedule to the Karnataka Sales Tax Act.

The Chairman of the ARA dissented from the majority view. In his opinion, ATMs would fit into the description of **electronic goods**, parts and accessories thereof. They would thus attract **12% basic tax** and would fall under Entry 4 of Part 'E' of the Second Schedule to the KST Act.

The Commissioner of Commercial Taxes was of the view that the ARA ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals.

The High Court of Karnataka acknowledged that **the IT Act provided an enlarged definition of "computers"**. However, the Court held that **such a wide definition could not be used for interpreting a taxation related law** such as the Karnataka Sales Tax Act, 1957.

The High Court also said that an **ATM is not a computer by itself** and **it is connected to a computer** that performs the tasks requested by the persons using the ATM. The computer is connected electronically to many ATMs that may be located at some distance from the computer.

Diebold Systems Pvt Ltd vs. Commissioner of Commercial Taxes ILR 2005 KAR 2210, [2006] 144 STC 59(Kar)

1.4.3 Data

According to section 2(1)(o) of the IT Act

"data" means 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 internally in the memory of the computer;

Simply put, data is

1. a representation of information, knowledge, facts, concepts or instructions,

2. prepared or being prepared in a formalized manner,

3. processed, being processed or sought to be processed in a computer.

Illustration: Sanya is typing a document on her computer. The moment she presses keys on her keyboard, the corresponding alphabets are shown on her screen. But in the background some parts of the document are stored in the RAM of her computer (*being processed*) while other parts are stored on the hard disk (*processed*). At any given instant, some information would be passing from her keyboard to the computer (*sought to be processed*).

Data can be in many forms such as

1. computer printouts,

2. magnetic storage media e.g. hard disks,

3. optical storage media e.g. CD ROMs, DVDs, VCDs

4. punched cards or tapes i.e. a paper card in which holes are punched.

Illustration: The electronic version of this book stored on your computer or on a CD would be "data". A printout of the electronic version of this book will also be "data".

1.4.4 Computer Software

Computer **software** is a general term that describes a collection of:

1. computer programs,
2. procedures and
3. documentation.

Computer **hardware**, on the other hand, consists of the physical devices that can store and execute computer software.

Illustration: Sanya downloads the OpenOffice software from the Internet. In effect, what she downloads is an **executable** file. She double-clicks on the executable file and begins to **install** the software on her computer. During the installation she specifies the part (drive and folder name etc) of the hard disk where the software files must be saved. During the installation the software also makes entries in system files (e.g. registry) maintained by the operating system (e.g. Windows 10). Once the installation is complete, Sanya can **run the software**. When she runs the software, relevant software files get loaded into **RAM** and are subsequently executed in the **CPU** (central processing unit).

Computer software can be divided into two fundamental categories – **system software** and **application software**. Application software uses the computer directly for performing user tasks. System software enables the application software to use the computer's capabilities.

Analogy: An oil company drills for oil on the sea bed. This oil is then processed and provided to the customer in the form of petrol for his car. Here the petrol is like the application software – it helps the user to run his car. The oil company is like the system software – it enables the petrol to be taken to the user.

1.4.5 Computer System

According to section 2(1)(l) of the IT Act

"computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

Simply put, a computer system has the following characteristics:

1. it is a device or collection of devices which contain data or programs,

2. it performs functions such as logic, storage, arithmetic etc,

3. it includes input and output support systems,

4. it excludes non-programmable calculators.

Illustrations: Laptop computers, Cell phones, sophisticated laser printers, high-end scanners.

In an interesting judgment, it was held by an American court that the **Internet** falls under the definition of computer system and the use of email is accessing a computer[7].

1.4.6 Computer Network

According to section 2(1)(j) of the IT Act

"computer network" means the inter-connection of one or more computers or computer systems or communication device through –

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained

Simply put, a computer network is the interconnection of one or more computers or computer systems or devices through:

- **Satellite:** Satellite Internet connection is an arrangement in which the outgoing and incoming data travels through a satellite. Each subscriber's hardware

[7] State of Pennsylvania v. Murgallis [No. 189 MDA 1999 (Pa. Super.Ct., June 2, 200)]. This judgment also relied upon the findings of the court in Reno v. ACLU that "The Internet is an international network of interconnected computers." [521 U.S. 844, 117 S.Ct. 2329, 138 L.Ed.2d 874, 884 (1997)]

includes a satellite dish antenna and a transceiver (transmitter / receiver). The dish antenna transmits and receives signals.

- **Microwave**: The term microwave refers to electromagnetic waves of a particular frequency. Microwave frequencies are used in radars, Bluetooth devices, radio astronomy, GSM mobile phone networks, broadcasting and telecommunication transmissions etc.

- **Terrestrial line** includes fibre optic cables, telephone lines etc.

- **Other communication media:** Communication media refers to any instrument or means that facilitates the transfer of data, as between a computer and peripherals or between two computers. Other ways in which two computers can be connected include cables, hubs, switches etc.

TWO

2. Legislative Framework

2.1 Information Technology Act

Information Technology Act, 2000 (IT Act) came into force on 17th October 2000. It has 94 sections divided into 13 chapters.

According to its preamble, the IT Act basically seeks to:

- ✓ provide legal recognition for **electronic commerce**[8],
- ✓ to facilitate **electronic filing of documents** with the Government agencies,
- ✓ to **amend** the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934,

[8] Electronic commerce or e-commerce includes transactions carried out by means of electronic data interchange and other means of electronic communication which involve the use of alternatives to paper-based methods of communication and storage of information.

Electronic Data Interchange (EDI) is the exchange of standardized business documents from computer to computer. The key to EDI is the fact that all the documents exchanged conform to a common computer-readable format. Instead of sending email messages (which do not follow a set format), EDI allows for structured information to be exchanged. The most important EDI standard is the UN/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce & Transport).

- ✓ promote **efficient delivery of Government services** by means of reliable electronic records,

- ✓ give favourable consideration to the **Model Law on Electronic Commerce** adopted by the United Nations Commission on International Trade Law (UNCITRAL).

The major issues addressed by the IT Act relate to:

1. **Electronic records:** authentication of electronic records using digital signatures; legal recognition of electronic records & digital signatures; use of electronic records & digital signatures in Government; retention of electronic records; publication in Electronic Gazette; attribution and acknowledgment of receipt of electronic records, time and place of dispatch and receipt of electronic record; secure electronic record, secure digital signature and security procedure.

2. **Establishing of authorities:** appointment and functions of Controller and other officers; establishment, procedures and functioning of Cyber Appellate Tribunal; Adjudicating Officers.

3. **Certifying Authorities:** recognition of foreign Certifying Authorities; functioning and control of Certifying Authorities, digital signature certificates; duties of subscribers such as generating a private-public key pair, acceptance of digital signature certificate and control of private key.

4. **Cyber crimes:** penalties for damage to computer and for failure to furnish information; factors to be taken into account by an adjudicating officer; offences relating to tampering with source code, hacking,

cyber-pornography, disobeying Controller's orders, unauthorised access to protected system, misrepresentation, breach of confidentiality and privacy and Digital Signature Certificate frauds; offences by companies; confiscation of computers etc, investigation of offences, police powers; liability of Network Service Providers.

5. **Special issues:** extra-territorial jurisdiction of the IT Act; overriding effect of the IT Act; protection of action taken in good faith.

6. **Administrative issues:** powers of the Central & State Governments and the Controller to make rules and regulations.

7. **Amendments:** amendments to Indian Penal Code, Evidence Act, Reserve Bank of India Act and the Bankers' Books Evidence Act.

2.1.1 Extent and Jurisdiction of the IT Act

To understand the extent and jurisdiction of the IT Act, we must examine sections 1(2) and 75 of the Act.

Not only does the IT Act apply to the whole of India, but also to contraventions committed outside India, by anyone, involving a computer located in India.

Illustration: Kylie Minogue, an Australian national, residing in USA, gains unauthorized access to a computer located in India and deletes information. In this case, she will be liable under the provisions of the IT Act.

However, there are exceptions to the term "any person". Certain persons are exempt from prosecution under the IT

Act. These include the President of India and the Governors of Indian states[9], Foreign Heads of State and Ambassadors of foreign countries[10].

2.1.2 Applicability of the IT Act

The IT Act does not apply to the following:

1. Negotiable instrument (other than a cheque),

Section 13(1) of the Negotiable Instruments Act, 1881 defines a "negotiable instrument" as a promissory note, bill of exchange or cheque payable either to order or to bearer.

[9] Article 361(2) of the Constitution of India states that "No criminal proceedings whatsoever shall be instituted or continued against the President, or the Governor of a State, in any court during his term of office." Article 361(3) states "No process for the arrest or imprisonment of the President, or the Governor of a State, shall issue from any court during his term of office."

[10] The principle of diplomatic immunity is enshrined in the "Vienna Convention on Diplomatic Relations" of 1961. The convention mentions that "the purpose of such privileges and immunities is not to benefit individuals but to ensure the efficient performance of the functions of diplomatic missions as representing States". This has been codified in India under the Diplomatic Relations (Vienna Convention) Act, 1972. Similar immunities are conferred on United Nations officers by the United Nations (Privileges and Immunities) Act, 1947.

Illustration of a promissory note: Suppose Sameer owes some money to Siddharth. He could give a written signed promissory note as under:

> I, Sameer Singh, promise to pay Siddharth Sharma the sum of Rs 20,000 on 12th January 2009.
>
> (Signed)
>
> Sameer Singh

Illustration of a bill of exchange

Suppose Pankaj owes money to Sameer and Sameer in turn owes some money to Siddharth. Sameer could give a written signed bill of exchange to Siddharth as under:

> Mr. Pankaj, please pay Siddharth Sharma the sum of Rs 20,000 on 12th January 2009.
>
> (Signed)
>
> Sameer Singh

A **cheque** is a special type of bill of exchange. It is drawn on banker and is required to be made payable on demand.

When the IT Act was originally passed in 2000, it did not apply to negotiable instruments. This changed after the Negotiable Instruments (Amendments & Miscellaneous Provisions) Act, 2002 came into force and amended the IT Act.

Now the IT Act applies to cheques but not to other negotiable instruments such as bills of exchange, promissory notes etc.

This Act also introduced two concepts that have had a major impact on banking in India. These concepts are "**cheque in the electronic form**" and "**truncated cheque**".

A **cheque in the electronic form** contains the exact mirror image of a paper cheque. It is generated, written and affixed with a digital signature in a secure system.

Cheque Truncation is the settlement of clearing transactions on the basis of images and electronic data without the physical movement of the cheques.

2. Power-of-attorney

A power-of-attorney includes any instruments empowering a specified person to act for and in the name of the person executing it [Section 1A of the Powers-of-Attorney Act, 1882].

Illustration: Sameer is travelling to USA for 2 years. During this period he is keen on selling his house in India. He can give a "power of attorney" to his friend Pooja. Using this power of attorney, Pooja can sign documents on Sameer's behalf and can sell his house.

3. Trust

According to section 3 of the Indian Trusts Act, 1882, a trust is an obligation annexed to the ownership of property.

Illustration: Sameer is a rich man who has contracted a serious disease. He wants to protect the interests of his 10 year old son. He transfers all his property to a "trust". He appoints his brother as the "trustee" to take care of the "trust property". Sameer will be the "author of trust" or the "testator", while his son will be the "beneficiary".

Thus, when a property is held by one person as trustee for the benefit of another, it can be regarded as a trust. To summarize, a testator sets up a trust for the benefit of the beneficiary. The trustee looks after the trust property.

4. Will

A will is the legal declaration of the intention of the testator, with respect to his property, which he desires to be realized after his death.

In other words, a Will or a Testament means a document made by a person whereby he disposes of his property. However, such disposal comes into effect only after the death of the testator.

Codicil is an instrument made in relation to a Will, explaining, altering or adding to its dispositions and is deemed to be a part of the Will.

5. Any contract for the sale or conveyance of immovable property or any interest in such property;

A **sale** is a transfer of ownership in exchange for a price. **Conveyance** includes a voluntary transfer of property from one person to another by means of a written instrument.

Immovable property includes land, benefits to arise out of land and things attached to the earth, or permanently fastened to anything attached to the earth. However, section 3 of the Transfer of Property Act excludes standing timber, growing crops or grass as immovable property.

6. Any such **class of documents or transactions** as may be notified by the Central Government in the Official Gazette.

2.2 Indian Penal Code

The Indian Penal Code (IPC) extends to the whole of India except the State of Jammu and Kashmir. It contains 23 Chapters with 511 Sections.

Indian Penal Code applies to every person including a foreigner for any violation committed in India. Under some circumstances, Indian Penal Code also applies to offences committed abroad.

One of the most important amendments to the Indian Penal Code was the substitution of the word "document" for the words "document or electronic record" by the Information Technology Act, 2000. This automatically brought several cyber crimes within the purview of the Indian Penal Code. These include:

1. wrongful translation of an electronic record by a public servant,
2. avoiding delivering an electronic record in court,
3. destroying electronic evidence,
4. forging electronic records

The issue of **defamatory** websites, especially profiles on public networking websites, is penalised by section 500 of the Indian Penal Code. The punishment is imprisonment upto 2 years and / or fine. The issues of fake websites (phishing) and fake emails (email spoofing) are also addressed by the Indian Penal Code[11].

[11] The relevant extract of section 464 of Indian Penal Code is: "A person is said to make a false document or false electronic record—First—Who dishonestly or fraudulently—…….(b) makes or transmits any electronic record or part of any electronic record;….with the intention of causing it to

2.3 Indian Evidence Act

Indian Evidence Act establishes the rules to be followed in producing evidence in a Court of law.

The nature of electronic evidence is such that in almost all cases where any electronic record is to be produced as evidence, it will actually be a copy of the original record that will be exhibited and not the original.

Keeping in mind the peculiarities of digital evidence, Indian Evidence Act was amended by the IT Act.

The most important amendment was the introduction of section 65B which relates to the admissibility of electronic records as evidence. This section lays down several conditions that must be met before electronic information can be accepted as evidence. This also provides for validation of computer output such as printouts, CDs, hard disks etc.

This section states as under:

65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of

---

be believed that such ……electronic record …..was made…by the authority of a person by whom ….it was not made".

any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:—

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official

position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,—

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

'Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.'

Section 65B of the Indian Evidence Act relates to admissibility of electronic records as evidence in a Court of law. It states

that a computer output will be deemed to be a document and will be admissible as evidence in any proceeding provided the following criteria are met with:

1. the electronic record containing the information should have been produced by the computer during the period over which the same was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

2. information contained in the electronic record was regularly fed into the computer in the ordinary course of the said activities;

3. the computer was operating properly or, if not, then during the period in which it was not operating properly or was out of operation, during that interval the electronic record or the accuracy of its contents were not affected; and

4. the information contained in the electronic record should be a reproduction or derivation from the information fed into the computer in the ordinary course of the said activities.

All the computers (whether by way of a combination of computers or different computers, or interlinked computers) used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer.

As a result of this section, when any evidence is to be produced, a certificate to that effect is required to be given additionally which will –

(a) identify the electronic record and describe the manner in which it was produced;

(b) give particulars of the device which was involved in production of the electronic record showing that the same was produced by a computer and showing that compliance has been made with the conditions mentioned in the said section;

(c) the said statement is required to be signed by a person holding a responsible official position in relation to the operation of the relevant device or management of the relevant activities.

(d) It would be sufficient that the statement is made to the best of the knowledge and belief of the person making it.

The computer holding the original evidence does not need to be produced in court. A printout of the record, or a copy on a CD, hard disk, pen drive etc can be produced in court.

However, some conditions need to be met and a certificate needs to be provided. These conditions and the certificate are best explained using a detailed illustration.

Note: This certificate is for illustration purposes only and does not constitute legal advice. Please **do not** use in a real scenario. If you require a legally valid certificate format for use in a real scenario, please email us on info@asianlaws.org

Illustration

Noodle Ltd is an Internet Service Provider. The police are investigating a cyber crime and need details about the

user of a particular IP address. They have requested Noodle for these details.

What Noodle is going to give the police is a printout of records stored in its computer systems. The following authenticated certificate has to be attached to this printout.

Certificate u/s 65B of Indian Evidence Act issued in relation to the printout titled "Information relating to IP address 10.232.211.84"

I, the undersigned, state to the best of my knowledge and belief that:

1. The printout titled "Information relating to IP address 10.232.211.84" issued on 1st June 2016 contains information stored in the ABC server being used by Noodle Ltd to provide Internet connection services to its customers in India.

2. The said printout was produced by the ABC server during the period over which the ABC server was used regularly to store and process information for the purposes of activities regularly carried on over that period by lawfully authorised persons.

3. During the said period, information of the kind contained in the electronic record was regularly fed into the ABC server in the ordinary course of the said activities.

4. Throughout the material part of the said period, the computer was operating properly.

5. The information contained in the electronic record reproduces such information fed into the computer in the

ordinary course of the said activities.

6. I am in a responsible official position in relation to the operation of the ABC server.

Signed on this 1st day of June 2016.

Pooja Singh
System Administrator,
Noodle Ltd

Anvar P.V v. PK Basheer & Ors.
[2014] 10 SCC 473

IN THE HON'BLE SUPREME COURT OF INDIA
E.P. No.3 OF 2011, CIVIL APPEAL NO. 4226 OF 2012
Decided on: 18 September, 2014
Appellant: Anvar P.V
Vs
Respondent: PK Basheer and Ors.
Bench: P.Sathshivam CJ, Kurian Joseph, Rohinton Fali Nariman.JJ

Summary of the case

In the general election to the Kerala Legislative Assembly held on 13.04.2011, the first Respondent was declared elected to 034 Eranad Legislative Assembly Constituency. The Appellant contested the election as an independent candidate and stood second in terms of votes. The Appellant sought to set aside the election under Section 100(1)(b) read with Section 123(2)(ii) and (4) of The Representation of the People Act, 1951 and also sought for a declaration in favour of the Appellant. By order dated 16.11.2011, the High Court of Kerala held that the election petition to set aside the election is not maintainable. The Hon'ble Supreme Court dismissed the appeal on several grounds, one of them being that the Appellant did not produce any certificate along with the electronic evidence which is essential under Section 65(B) of the Indian Evidence Act, 1872 ('Evidence Act'). The main issue which the Supreme Court dealt with was regarding fulfilment of ingredients of Sections 65(A) and 65(B) of the Evidence Act regarding admissibility of electronic evidence in the form of CD.

Observations of the Supreme Court

1. Electronic record produced for the inspection of the court is documentary evidence under Section 3 of The Indian Evidence Act, 1872 (hereinafter referred to as 'Evidence Act').

2. The person needs to state in the certificate that the same is to the best of his knowledge and belief. Most importantly, such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic record sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

3. The Supreme Court overruled the case of *State (NCT of Delhi) vs. Navjot Sandhu alias Afsan Guru* [Appeal (Crl.) 373-375 of 2004] and held that an electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same has to be accompanied by a certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

4. As the Appellant admittedly did not produce any certificate in terms of Section 65B of the Evidence Act

in respect of the CDs, therefore, the same cannot be admitted in evidence.

2.4 Code of Criminal Procedure

The Code of Criminal Procedure, 1973 (CrPC) is essentially a law of procedure. It covers several relevant issues including:

1. procedure to be followed for the filing of criminal complaints,
2. procedure to be followed by the police for investigation,
3. procedure to be followed for the conviction of offenders,
4. search and seizure operations,
5. confiscation of computers etc,
6. hierarchy of courts in India,
7. sentences that various Courts can pass,
8. summons and warrants,
9. appeals, reference and reviews of judgments and Court orders,
10. bails and bonds.

2.5 Bankers' Books Evidence Act

The Banker's Books Evidence Act, 1891 lays down the rules of evidence in relation to **bankers' books**. Generally, bankers' books[12] would be cited as evidence where any financial transaction involving the banking system is in question or has to be examined.

The IT Act has amended the Banker's Books Evidence Act to confer equal status on electronic records as compared to paper based documents. If a "certified copy" of printouts of bankers' books has to be given, then such printouts must be accompanied by **three certificates.**

Let us take a simple illustration to understand the contents of these certificates.

> **Note:** These certificates are for illustration purposes only and do not constitute legal advice. Please **do not** use in a real scenario. If you require legally valid certificate formats for use in a real scenario, please email us on info@asianlaws.org

Illustration: Sameer issued a cheque to Pooja for Rs 3 lakh. The cheque was dishonoured by Sameer's bank (Noodle Bank Ltd) as the balance in Sameer's account was only Rs. 50,000. Pooja has filed a case against Sameer under section 138 of the Negotiable Instruments Act for the cheque "bouncing".

Pooja has requested Noodle Bank for a certified copy of Sameer's bank account statement (for January 2016) for

[12] Bankers' books include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank. These can be in paper form or printouts of data stored in bank computers.

producing in court as evidence. The printout of the bank statement will be accompanied by the following 3 certificates:

Certificate u/s 2A(a) of the Banker's Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that:

1. Mr. Sameer Sen is holding account no. 12345 with the Pune branch of the Noodle Bank Ltd.

2. The accompanying bank account statement is a printout of the transactions and balances in the said bank account for the period beginning 1st January 2016 and ending 31st January 2016.

Siddharth Sharma
Manager, Pune branch
Noodle Bank Ltd

Certificate u/s 2A(b) of the Banker's Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that the enclosed "Information Security Policy of Noodle Bank Ltd" contains the true and correct information relating to the computer system used to store bank account related information of Noodle Bank customers and including the following information:

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) other factors that will vouch for the integrity and accuracy of the system.

Pooja Singh
System Administrator, Pune branch, Noodle Ltd

Enclosed: Information Security Policy of Noodle Bank

Certificate u/s 2A(c) of the Banker's Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that:

1. The Noodle computer system described more accurately in the "Information Security Policy of Noodle Bank Ltd" operated properly at the material time when the said system was used to take the printout relating to the transactions and balances in the bank account no. 12345 for the period beginning 1st January 2016 and ending 31st January 2016 was taken.

2. The printout referred to above is appropriately derived from the relevant data stored in the said system.

Pooja Singh
System Administrator, Pune branch, Noodle Ltd

The importance of the certificates discussed above is stressed in the State Bank of India vs. Rizvi Exports Ltd case[13].

State Bank of India (SBI) had filed a case to recover money from some persons who had taken various loans from it. As part of the evidence, SBI submitted printouts of statement of accounts maintained in SBI's computer systems. The relevant certificates as mandated by the Bankers Books of Evidence Act (as amended by Information Technology Act) had not been attached to these printouts. The Court held that these documents were not admissible as evidence.

2.6 Payment and Settlement Systems Act

The Payment and Settlement Systems Act, 2007 (PSS Act) provides for the regulation and supervision of payment systems in India by the Reserve Bank of India (RBI).

[13] II(2003)BC96. DEBT RECOVERY APPELLATE TRIBUNAL, ALLAHABAD [T.A. No. 1593 of 2000 Decided On: 01.10.2002]

According to the Act, a payment system "enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them". It does not include stock exchanges or clearing corporations set up under stock exchanges.

Payment systems include the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations.

Two regulations have been made under this Act –

1. Board for Regulation and Supervision of Payment and Settlement Systems Regulations, 2008. This deals with the constitution, composition, powers and functions of the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS).

2. Payment and Settlement Systems Regulations, 2008. This covers matters like form of application for authorization for commencing or carrying on a payment system, determination of standards of payment systems etc.

The Payment and Settlement Systems (Amendment) Act, 2015 received the assent of the President on the 13th May, 2015.

THREE

3. Judicial Framework

Cyber crimes under Chapter 9 of the IT Act come under the jurisdiction of Adjudicating Officers. Appeals from orders of the Adjudicating Officers lie to the Cyber Appellate Tribunal and appeals from the orders of the Cyber Appellate Tribunal lie to the High Court. Other cyber crimes come under the jurisdiction of the criminal courts.

Case law is the law that is established through the decisions of the courts and other officials. Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the Courts helps clarify the real objectives and meaning of such laws.

In India, courts are bound by decisions of higher courts in the hierarchy. The apex court in India is the Supreme Court. **Article 141 of the Constitution of India** states that "the law declared by the Supreme Court shall be binding on all courts within the territory of India"[14].

[14] In Bengal Immunity Co. v. State of Bihar, Das [(1955) 2 SCR 603 (628)], Actg. C.J. of the Supreme Court of India stated that: Article 141 which lays down that the law declared by this Court shall be binding on all Courts within the territory of India quite obviously refers to Courts other than this Court. The corresponding provision of the Government of India Act, 1935 also makes it clear that the Courts contemplated are the Subordinate Courts.

The hierarchy of courts is further enshrined in the **Code of Civil Procedure, 1908**[15] and the **Code of Criminal Procedure, 1973**[16].

It must also be borne in mind that a single Judge must follow the decision of a division Bench. A division bench must follow the decision of a full bench of the same court. The importance of precedents in the Indian legal system has been highlighted by the Supreme Court as under[17]:

> *Precedents which enunciate rules of law form the foundation of administration of Justice under our system. It has been held time and again that a single Judge of a High Court is ordinarily bound to accept as correct judgments of Courts of coordinate jurisdiction and of Division Benches and of the Full Benches of his Court and of this Court. The reason of the rule which makes a precedent binding lies in the*

[15] Section 3 of the Code of Civil Procedure, 1908: "For the purposes of this Code, the District Court is subordinate to the High Court, and every Civil Court of a grade inferior to that of a District Court and every Court of Small Causes is subordinate to the High Court and District Court".

[16] Section 15(1) of the Code of Criminal Procedure, 1973: "(1) Every Chief Judicial Magistrate shall be subordinate to the Sessions Judge; and every other Judicial Magistrate shall, subject to the General control of the Session Judge, the subordinate to the Chief Judicial Magistrate."
Section 10(1) of the Code of Criminal Procedure, 1973: "(1) All Assistant Sessions Judges shall be subordinate to the Sessions Judge in whose court they exercise jurisdiction."

Section 19(1) of the Code of Criminal Procedure, 1973: "(1) The Chief Metropolitan Magistrate and every Additional Chief Metropolitan Magistrate shall be subordinate to the Sessions Judge, and every other Metropolitan Magistrate shall, subject to the general control of the Sessions Judge, be subordinate to the Chief Metropolitan Magistrate."

[17] Tribhovandas v. Ratilal, AIR 1968 SC 372

desire to secure uniformity and certainty in the law.

Another category of precedents are those that are liable to be disregarded in certain circumstances. As an illustration, the decision of a Single Judge of the Bombay High Court is binding on the subordinate Courts in Maharashtra, but is not binding on a Division Bench of the Bombay High Court.

Another category of precedents are those that have persuasive value. As an illustration, the decision of a Single Judge of the Bombay High Court has only persuasive value before a Single Judge of the Delhi High Court.

The hierarchy of criminal courts in India is illustrated below:

Supreme Court
(Can pass any sentence authorized by law)

High Court
(Can pass any sentence authorized by law)

Sessions Court / District Court / Additional Sessions
(Can pass any sentence authorized by law.
Death sentences are subject to confirmation by the High Court)

Assistant Sessions Court
(Can sentence for up to 10 years jail)

Chief Judicial Magistrate / Chief Metropolitan Magistrate
(Can sentence for up to 7 years jail)

Metropolitan Magistrate / Judicial First Class Magistrate
(Can sentence for up to 3 years jail)

Judicial Second Class Magistrate
(Can sentence for up to 1 year jail)

The hierarchy of authorities/courts under IT Act is illustrated below:

Supreme Court

High Court

Cyber Appellate Tribunal

Adjudicating Controller Officer

FOUR

4. Quasi-judicial Framework

4.1 Adjudicating Officers

The chief responsibility of Adjudicating Officers (AO) under the IT Act is to adjudicate on cases under section 43, 44 and 45 of the IT Act e.g. unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, computer manipulations etc.

The Secretary of Department of Information Technology in each state and Union Territory is the Adjudicating Officer for that state or Union Territory.

Chapter 9 of the IT Act and the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 contain the relevant provisions.

The outline of the procedure is as under:

1. The complaint to the AO must be made on plain paper along with the fee payable. The fee is calculated on the basis of damages claimed by way of compensation.

2. The AO then issues a notice fixing a date and time for further proceedings to all the necessary parties. On that date the AO explains the allegations to the respondent.

3. If the respondent pleads guilty, the AO can impose suitable penalty.

4. Otherwise, based on the complaint, investigation report, submissions etc. the AO can either dismiss the matter or hear the matter.

5. The AO can get the matter investigated by an officer in the Office of Controller or CERT-IND or by the concerned Deputy Superintendent of Police.

6. The AO can impose penalty after considering the – (A) amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; (B) the amount of loss caused to any person as a result of the default; (C) the repetitive nature of the default.

7. The AO must attempt to decide the matter within 6 months and must promote on-line settlement of disputes.

8. If the matter involves violation of Chapter 11 of the IT Act, then the AO can transfer the case to a Magistrate.

9. When an adjudication is pending before an AO, the same matter cannot be pursued before any court, Tribunal etc.

10. If a complaint appears to be frivolous then the AO can fine and penalize the complainant.

11. Certifying Authorities, the Controller and other officers / agencies established under the Act and other government agencies like CERT-IND are required to promptly assist the AO.

The list of Adjudicating Officers and their contact information can be obtained from:

http://cca.gov.in/adju-offlist.jsp

Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 contain provisions relating to:

1. qualifications and experience of an AO,
2. scope and manner of holding enquiry,
3. orders of the AO,
4. service of notice and orders,
5. fee to be paid,
6. treatment of frivolous complaints,
7. compounding of contraventions.

The Secretary of Department of Information Technology in each State and Union Territory is the adjudicating officer for that State or Union Territory.

4.2 Cyber Appellate Tribunal

Appeals against the orders of AO and the Controller lie with the Cyber Appellate Tribunal (CAT).

The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 contain detailed procedural and other provisions relating to the functioning of the CAT. The outline of these rules is:

1. An appeal must be filed within 45 days and a fee of Rs. 2,000 is payable when such appeals are filed.

2. No appeal can be made in case the AO order is made with the consent of the parties.

3. The CAT can confirm, modify or set aside the order appealed against.

4. The CAT must try to dispose appeals within 6 months.

These rules also contain detailed procedural and other provisions relating to the functioning of the CAT.

The major issues covered by these rules are:

1. form, procedure and fee for filing applications before the CAT,

2. scrutiny of applications,

3. service of notice of application on the respondents,

4. filing of reply by the respondents,

5. decision of applications,

6. ex-parte hearing of applications,

7. registration of legal practitioners clerks,

8. power, functions and duties of the Registrar.

9. The *Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003* prescribe the salary,

allowances and other terms for the Presiding Officer of the CAT.

10. *Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003* provided some additional powers to the CRAT.

4.3. Controller of Certifying Authorities

The primary role of the Controller of Certifying Authorities (CCA) is to regulate the working of the **Certifying Authorities** (CA). A CA is a business organization that issues digital signature certificates to subscribers. This sets the base for the development of electronic commerce and governance in India.

The CCA also has **investigation powers** u/s 28 of the IT Act. The CCA can also **direct a person to decrypt information** under his control. If such a person refuses to comply with the CCA directions he faces 7 years imprisonment u/s 69 of the IT Act.

4.4. Overview

Section 9 of the Code of Civil Procedure, 1908 provides that courts have the jurisdiction to try all suits unless their jurisdiction is either expressly or impliedly barred. Section 61 of the IT Act expressly bars jurisdiction of civil courts to entertain suit or proceeding in respect of any matter which an AO or CAT are empowered to adjudicate upon.

The AO under section 46 has a limited power to adjudicate cases arising out of Chapter 9 of the IT Act. However, this power to adjudicate comes with a certain pecuniary limit i.e. matters in which the claim for injury or damage does not exceed rupees five crore. Jurisdiction in respect of claim for

injury or damage exceeding rupees five crore shall vest with the competent court.

As we have seen above, the CCA also has powers to investigate under section 28 of the IT Act.

Any person aggrieved by an order made by the Controller or the AO may appeal to the CAT under section 57 of the IT Act. The CAT was formed in October 2006[18]. After a short period of coming into existence, the office of the Chairperson has been lying vacant since June 2011 and is not currently functional. Appeals from the CAT lie to the High Court under section 62 of the IT Act.

[18] http://meity.gov.in/writereaddata/files/Chapter-1.pdf at para 2.2

FIVE

5. Investigative Framework

The investigation of cyber crimes covered by the Indian Penal Code is done by the police. For cyber crimes covered by the IT Act, investigation can be done by an officer not below the rank of a Inspector of police.

Power to investigate offences is covered by section 78 of the Information Technology Act. This section states as under:

78. Power to investigate offence.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

According to section 2(h) of the *Code of Criminal Procedure*, "investigation" includes all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorised by a Magistrate in this regard.

Section 28 of the *Information Technology Act* empowers the following to investigate any contravention of the Act and allied rules and regulations: (1) the Controller (2) any officer authorised by the Controller.

Additionally, section 78 of the *Information Technology Act* empowers a police officer not below the rank of Inspector to

investigate offence under the Act. Offences are defined under Chapter XI of the Act.

Additionally, rule 4(i) of the *Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003* authorizes the Adjudicating Officer to get a matter or report investigated from an officer in the Office of Controller or CERT-IND or from the concerned Deputy Superintendent of Police [Inspector], to ascertain more facts and whether prima facie there is a case for adjudicating on the matter or not.

Additionally, section 80 of the *Information Technology Act* provides a special power to police officers not below the rank of an Inspector of Police and to other Government officers authorised by the Central Government. Such authorised persons can enter and search any public place. Public places include cyber cafes, hotels, shops etc accessible to the public.

Additionally, they can arrest without warrant any person found in such a public place who is reasonably suspected of:

(1) having committed an offence under the Act,

(2) committing an offence under the Act,

(3) being about to commit any offence under the Act.

The steps most commonly followed in the investigation and trial of a criminal case are outlined as under (Note: CrPC stands for *Code of Criminal Procedure, 1973*):

1. The complainant approaches the local police station to file a complaint.

2. The police listen to the facts disclosed by the complainant. If the facts disclose a non-cognizable offence then the police make an entry in a special register for non-cognizable complaints. This register is regularly submitted to the local magistrate. A non-cognizable case is one in which the police cannot arrest a person without a warrant.

3. If the facts disclose a cognizable offence then an FIR (First Information Report) is lodged. The FIR is numbered, dated and a copy is given to the complainant. A copy is also submitted to the local Court. A cognizable case is one in which the police can arrest a person without a warrant e.g. cyber terrorism is punishable with life imprisonment and is a cognizable offence.

4. The police then begin the investigation. They may visit the scene of the crime, question witnesses and suspects etc.

5. A person being questioned by the police is legally bound to give true answers. **Exception:** A person is not legally bound to answer a question if the answer can incriminate him. This exception is provided by section 161 of CrPC. The right against self-incrimination is vested by the Constitution of India.

6. The police can write down the statements made by the witnesses, suspects etc. The person making the statement is

not required to sign it. Note: A person can voluntarily make a statement or confession to a Court.

7. The police cannot threaten a person into making any statement.

8. The police can search any house, office etc and seize evidence. They do not need a search warrant for this.

9. If some evidence is to be collected from abroad, the Court can make an order which is then forwarded by the Central Government to the suitable authority in the relevant countries.

10. The police can arrest and confine a suspect. The freedom of an arrested person is restricted by the police. The police are empowered to use force if a person attempts to evade arrest. An arrested person must be informed about the grounds for his arrest.

11. The police can search the arrested person and recover evidence.

12. The arrested person must be produced before a Court within 24 hours of his arrest. The Court can then do one of the following:

(a) release the arrested person on bail,

(b) send the arrested person into the custody of the police so that the police can carry out their investigation (police custody),

(c) send the arrested person to jail (judicial / magisterial custody).

It is a common misconception that Courts are closed on weekends and public holidays and a person will have to wait till a Monday to be produced before a Court. There is always at least one criminal court functioning on every holiday and weekend.

13. After completing the investigation, the police are required to submit their report and relevant documents to the Court.

14. After studying the investigation report, the Court can dismiss the complaint if there are insufficient grounds against the accused persons.

15. If there are sufficient grounds to proceed against the accused, the Court can take cognizance of the case and frame charges against the accused.

16. If the accused person pleads guilty to the charges then the court can convict him under the relevant law and impose sufficient imprisonment term and / or fine.

17. If the accused person does not plead guilty to the charges, the trial takes place. The prosecution and the defence argue the case, examine witnesses and place evidence before the court.

18. If scientific reports are provided as evidence, then the Court can call the scientific expert to Court to examine him e.g. the director, deputy director or assistant director of a Central or State Cyber Forensic Laboratory is usually summoned to court in cases involving cyber crime and digital evidence.

19. After hearing the arguments, the Court gives the judgment. If the accused is found guilty then the court can convict him under the relevant law and impose sufficient imprisonment

term and / or fine. The convicted person can appeal to a higher court against this judgment.

20. If the accused is found not guilty, then the court can acquit him. The Court can also order the complainant to pay compensation if the case appears to be frivolous.

21. Once a person has been tried by a Court, he cannot be prosecuted again for the same offence or for another offence based on the same facts. It does not matter whether the person was convicted or acquitted.

Cyber Crime Investigation

Cyber Crime Investigation is the collecting, analyzing and investigation of digital evidence and cyber trails.

This digital evidence and cyber trail may be found in computer hard disks, cell phones, CDs, DVDs, floppies, computer networks, the Internet etc.

Digital evidence and cyber trails can be hidden in pictures (steganography), encrypted files, password protected files, deleted files, formatted hard disks, deleted emails, chat transcripts etc.

Given below are some of the cases that cyber crime investigators are called in to solve. All these cases involve recovery and analysis of digital evidence and cyber trails

(1) Divorce cases
(2) Murder cases
(3) Organized crime, Terrorist operations, Extortion
(4) Defamation, Pornography
(5) Online banking / share trading / credit card fraud
(6) Smuggling, Tax evasion, Money laundering

(7) Virus attacks, Cyber sabotage, Source code theft
(8) Phishing attacks, Email hijacking, Denial of service
(9) Counterfeit currency, stamp papers, postage stamps etc.

The actual process of the investigation of any computer related crime begins with an external examination of the premises. Normally, for this part of the investigation, the rules and regulations of investigation and forensics related to traditional crimes also apply to some extent.

This part of the investigation basically assists the computer forensics expert in adjudging the strengths and vulnerabilities of the network. It also helps him in deciding the steps to be taken to investigate the crime and also the peculiarities of the incident.

A cyber crime investigator also has to decide whether it is prudent to confiscate computer resources from the suspect's premises or to complete the investigation at the scene.

Confiscating and carrying out the investigation off-site would involve proper packaging and transporting of the computers and accessories, reassembling them at the laboratory and then recreating the network or configuration.

Section 76 of the IT Act relates to confiscation of computers and related accessories. These can be confiscated if they have been used in respect of a contravention of the IT Act or any related rules, orders or regulations.

This can be a complex and sensitive issue and hence the cyber crime investigator must decide based on the volume of evidence, technical and infrastructural issues and time available.

Cyber Forensics is a wide term that encompasses computer forensics (gathering evidence from computer media seized at the crime scene) and network forensics (gathering digital evidence that is distributed across networks).

Digital evidence is the foundation of any case involving computers. Searching, examining, collecting, and preserving digital evidence has to be done in such a manner that the court can rely upon the evidence to deliver its judgment. Any errors in gathering, developing, or presenting digital evidence can adversely affect the trial.

As per the definition provided by the Computer Emergency Response Team of the Asian School of Cyber Laws (ASCL-CERT):

> *Cyber Forensics is the discovery, analysis, and reconstruction of evidence extracted from and / or contained in a computer, computer system, computer network, computer media or computer peripheral.*

Discovery implies recovery of something previously unknown or unrecognized. Analysis is the detailed examination of something made in order to understand its nature or determine its essential characteristics. Reconstruct means to construct again, to rebuild, and to form again or anew. Evidence refers to all documents including electronic records produced for the inspection of the Court. Extract means to take out or derive.

Broadly speaking, Cyber Forensics involves:

(1) finding and decrypting password protected information, encrypted information and steganography content
(2) tracing the source of e-mail
(3) tracking software piracy

(4) recovering deleted data
(5) matching information to computers that created them
(6) remotely monitoring computers and
(7) preserving digital evidence for presentation in court.

Some of the basic techniques that are used for cyber crime investigation are:

(1) whois search
(2) IP tracing from ISP
(3) analyzing a web server log
(4) analyzing email headers
(5) tracking an email account
(6) recovering deleted evidence
(7) cracking passwords
(8) handling encrypted information
(9) handling steganographic information
(10) handling hidden data
(11) using keyloggers for investigation.
Section 80 of the Information Technology Act relates to power of the police and other officers to enter, search, etc.

SIX

6. *Protection of Privacy and Data*

Privacy refers to the right of an individual where one can choose the extent to which he or she would like to disclose information/data which pertains to him or her. Data protection refers to the policies and laws mainly focussing on the privacy of an individual which aim to curtail intrusion into one's privacy which is caused mainly by the collection, storage and dissemination of one's personal data. All the information or data which relate to a person who can be identified from that information or data, is known as personal data of that individual. The Supreme Court of India in a landmark decision (Justice Puttuswamy v. UOI[19]) in August 2017 recognized that right of privacy was a fundamental right.

The present law on data protection in India is embodied in the form of Section 43A of the IT Act read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The IT Act deals with both civil and criminal cases of violation and exploitation in respect of personal data.

Section 43A was inserted by the Information Technology (Amendment) Act, 2008. As per Section 43A, where a body corporate[20] possesses, deals with, or handles any sensitive

[19] *Writ Petition (Civil) No. 494 of 2012* decided on August 24, 2017

[20] "Body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities as defined in Section 43A of the IT Act.

personal data or information in a computer resource (which is owned, controlled or operated by it), is found negligent of implementing reasonable security practices, which causes wrongful loss/gain to any person, such a body corporate is be liable to pay damages by way of compensation to the affected person.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 deal with safeguarding the 'sensitive personal data or information' of a person.

Some examples of sensitive personal data or information include password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation, medical records and history, biometric information, etc. Section 72 of the IT Act penalises a person, who in pursuance of any powers under the IT Act, Rules or Regulations has secured access to any information, and he discloses such information without the consent of the person concerned. Also, section 72A punishes any person (including an intermediary) who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, and he discloses such material to any other person, without the consent of the person concerned or in breach of a lawful contract. While section 72 is applicable only to persons who, while exercising powers under the IT Act, Rules or Regulations, have gained access to information, there is no such restriction under section 72A.

However, there are certain exceptions to the rule. Under section 69 of the IT Act, any person authorised by the Government if it is necessary in the interest of the sovereignty, security and integrity of India, can intercept, monitor or

decrypt any information generated, transmitted, received or stored in any computer resource. Further, such Government Agency shall not share or publish such information with any other person[21].

[21] Rule 6 of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

SEVEN

7. Related issues

7.1 Certifying Authorities

The Information Technology (Certifying Authorities) Rules, 2000 cover various issues relating to Certifying Authorities (CAs) including:

1. creation and verification of digital signatures,
2. the information technology architecture that CAs may support,
3. information that digital signature certificates must contain,
4. eligibility for licensing of certifying authorities,
5. form, information and fees to be submitted with an application for license to become a CA,
6. requirement for cross certification with other licensed CAs,
7. validity, renewal and suspension of license granted to a CA,
8. conditions under which the Controller may refuse to grant a license or refuse to renew a license,
9. security guidelines for CAs,
10. requirements prior to ceasing activities as a CA,
11. database of disclosure records of CAs to be maintained by the Controller
12. issue of digital signature certificates by a CA
13. generation of digital signature certificates.

14. compromise and revocation of digital signature certificates,
15. fees that CAs can charge,
16. annual audits of CA operations
17. confidentiality of digital signature certificate applications and subscriber information.

Further technical and other regulations are provided in the *Information Technology (Certifying Authority) Regulations, 2001.*

There are 2 important **guidelines** relating to CAs:

(1) Guidelines for submission of application for licence to operate as a Certifying Authority,

(2) Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates.

7.2 Intermediaries

Section 79 of the Information Technology Act relates to exemption from liability of intermediary in certain cases. This section states as under:

79. Exemption from liability of intermediary in certain cases.

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication-link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if –

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not –

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if –

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation – For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

As per section 2(1)(w) of the Information Technology Act, the term "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record.

The term includes: telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

Intermediaries are not liable for any third party information, data, or communication-link made available or hosted by them. "Third party information" means any information dealt with by an intermediary in his capacity as an intermediary. This exemption is provided to them subject to the condition that:

(1) their function is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;

(2) the intermediary does not – initiate the transmission, (ii) select the receiver of the transmission, or select or modify the information contained in the transmission;

(3) the intermediary observes due diligence while discharging his duties under this Act and also observes guidelines prescribed by the Central Government.

This exemption is not applicable if:

(1) the intermediary has conspired or abetted or aided or induced in the commission of the unlawful act; or

(2) the intermediary fails to expeditiously remove or disable access to that material (without vitiating the evidence in any manner) upon being informed about the unlawful act.

> **Illustration:** Sameer creates an obscene profile using the free social networking website provided by Google. As long as Google is unaware about this, it is not liable.
>
> If Google is informed about this profile (by a user, the police etc), and it does not remove access to the profile, then it will be liable.
>
> If Google sends out promotional emails that contain obscene matter then it will be liable as that is not third party information.

Section 67C of the *Information Technology Act* is also relevant. Under this section, intermediaries are required to: (1) preserve and retain information specified by the Central Government (2) for the time period specified by the Central Government.

As per the Information Technology (Intermediaries Guidelines) Rules, 2011 an intermediary is required to preserve information and associated records for at least ninety days for investigation purposes.

> **Illustration:** The Central Government specifies that all search engines must keep a record of the IP addresses of users searching for certain key words e.g. "rdx". The Government also specifies that the date and time of the

search by the user must be recorded and stored for 3 years.

Noodle search engine stores only the IP address of the user and not the date and time when the user made the search. The Noodle management would be liable under this section.

Several liabilities have been imposed on intermediaries under the *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009*.

Additionally, several liabilities have been imposed on intermediaries under the *Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009*. Additionally, several liabilities have been imposed on intermediaries under the *Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009*.

The Information Technology (Intermediaries Guidelines) Rules, 2011 lays down the due diligence requirements to be complied with by the intermediaries.

In the Bazee.com[22] case, Mr. Avnish Bajaj, the CEO of Bazee.com was arrested after a media clip containing sexually explicit material was posted for sale on the website. While the Delhi High Court quashed the criminal proceedings against Mr. Bajaj, it held that the website hosting the video can be held liable under the Indian Penal Code 1860 and the IT Act. It was after this case that the lacuna in the IT Act was acknowledged and an amendment was carried out under which

[22] Avnish Bajaj v State; (2005) 3 CompLJ 364 Del

intermediaries may be exempt from liability for content posted on their web platform.

The validity of section 79 was challenged before the Hon'ble Supreme Court in the case of Shreya Singhal vs. UOI[23]. The Supreme Court held that Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.

Further, the Information Technology (Intermediary Guidelines) Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as Section 79(3)(b) i.e. the knowledge spoken of in the said sub-rule must only be through the medium of a court order.

7.3 Digital Signatures as Evidence

Simply put, a person can authenticate a document by affixing his digital signature. Conceptually, a digital signature is similar to a hand written signature. Let us take a simple illustration to understand how digital signatures work.

Illustration

Sanya uses her computer to generate a public and private key pair. Simply put, these keys are very large numbers.

[23] AIR 2015 SC 1523

She then stores her private key very securely on her computer. She uploads her public key to the website of a licensed certifying authority (CA). She also couriers a filled in application form and photocopies of her passport and Income Tax PAN card to the CA.

After following some verification procedures, the CA sends Sanya a hardware device by post. This device contains Sanya's digital signature certificate. The digital signature certificate contains Sanya's public key along with some information about her and the CA.

Sanya then has to accept her digital signature certificate.

All digital signature certificates are stored in the online repository maintained by the Controller of Certifying Authorities.

Each Certifying Authority stores digital signature certificates issued by it in an online repository.

In order to digitally sign an electronic record, Sanya uses her private key.

In order to verify the digital signature, any person can use Sanya's public key (which is contained in her digital signature certificate).

In case Sanya had originally generated her private key on a smart card or USB Crypto Token then the subsequent signatures created by her would be **secure digital signatures**.

Note: The smart card / crypto token have a chip built into it, which has crypto modules to enable the signing

operation to happen in the device itself. The private key does not come out of the device in its original form.

In case Sanya had generated and stored her private key on a hard disk, floppy, CD, pen drive etc then subsequent signatures are not secure digital signatures.

Illustration 1: Pooja has filed a case against Sameer. An electronic record alleged to have been digitally signed by Sameer is presented as evidence to the Court. The digital signature is verifiable using the public key contained in a digital signature certificate issued by Noodle Ltd to Sameer.

The Court has to ascertain whether the said digital signature is Sameer's. The opinion of Noodle Ltd is relevant in this case.

Illustration 2: Pooja has filed a case against Sameer. An electronic record alleged to have been digitally signed by Sameer is presented as evidence to the Court.

It has to be proved in court that the digital signature is that of Sameer.

To do this the Court can ask the Controller of Certifying Authorities or the relevant Certifying Authority (e.g. Noodle Ltd in this case) to produce the digital signature certificate issued to Sameer.

The Court can then ask someone to verify the digital signature using the public key contained in Sameer's digital signature certificate.

Illustration 3: Pooja has filed a case against Sameer. An electronic record to which a Government official has

affixed a secure digital signature is presented as evidence to the Court.

It does not have to be proved in court that the digital signature is actually that of the Government official.

The Court can also assume that the secure digital signature is affixed by the Government official with the intention of signing or approving the electronic record.

Illustration 4: Pooja has filed a case against Sameer. An electronic record alleged to have been digitally signed by Sameer is presented as evidence to the Court.

The Court asks the Controller of Certifying Authorities to produce the digital signature certificate issued to Sameer. The Court can presume that all the information contained in the digital signature certificate is correct. It cannot presume the correctness of unverified information relating to Sameer.

The Court can then ask someone to verify the digital signature using the public key contained in Sameer's digital signature certificate.

Illustration 5: Pooja has filed a case against Sameer. A 5-year-old electronic record to which a Government official has affixed a digital signature is presented as evidence to the Court.

Ever since its creation the said record has been in the custody of the relevant Government department. It can be presumed by the Court that the digital signature was affixed by the said official or an authorised person.

7.4 Offences by companies

A company is a legal person separate from its members or shareholders. Let us take a simple illustration to understand this concept.

> **Illustration**
> Sameer and Pooja form a company called Noodle Ltd. They each pay Rs 1000 into the bank account of Noodle Ltd as payment for 100 shares of Noodle Ltd. In the eyes of the law, Sameer, Pooja and Noodle Ltd are 3 different and distinct legal persons. If Noodle Ltd owes the bank some money, then Noodle Ltd has to pay that money. The personal property of Sameer and Pooja cannot be taken away by the bank.
>
> Sameer and Pooja are the shareholders of Noodle Ltd. Even though they control 100% of the shares of Noodle and control all decisions made by Noodle, they are not personally liable for money owed by Noodle. Their liability is restricted to the money paid for the shares held by them.

What this chapter addresses are the liabilities of a company and its officials in case the company violates the provisions of the IT Act e.g. if a company runs a website and pornographic content is published by this website. The term company includes partnership firms, societies etc.

This section can best be understood using the following **illustration**.

Noodle Ltd runs a website that provides jokes to its subscribers in return for a monthly payment. Sameer and Pooja are Directors of the company. Sameer looks after the day-to-day operations of the website including the creative department which makes up new jokes.

Siddharth is an employee of Noodle Ltd. He comes up with a visual joke that is obscene in nature. Sameer allows the joke to be uploaded to the Noodle website and from there it is downloaded by hundreds of subscribers.

One of the subscribers files a case against Noodle Ltd under section 67 of the IT Act. The following will be liable for prosecution: Noodle Ltd, Pooja, Sameer.

If Pooja can prove that she was not aware of the decision to publish the obscene joke, then she will not be liable.

If Siddharth's role in creating the joke can be proved, then he also will be liable.

7.5 Phone Tapping

Under section 5(2) of the Telegraph Act, 1885, both the Central Government and the State Government have the right to tap phones if it is necessary to do so in the interest of the sovereignty, integrity and security of India.

The issue of phone tapping was brought into light when Peoples Union for Civil Liberties[24] appealed to the Supreme Court highlighting the incidents of indiscriminate telephone tapping and further sought clarification on the law regarding telephonic tapping in India.

[24] People's Union for Civil Liberties (PUCL) vs. Union of India; (1997) 1 SCC 301

The Supreme Court in this case took notice of the existence of privacy as a part of a fundamental right of an individual. The Supreme Court held that a mechanism to prevent indiscriminate telephone tapping must be in place and laid down guidelines under which interception may take place.

EIGHT

8. International Framework

8.1 International treaties

The first comprehensive international effort dealing with the criminal law problems of computer crime was initiated by the **Organisation for Economic Co-operation and Development** (OECD)[25].

The United Nations Commission on International Trade Law (UNCITRAL) formulated the UNCITRAL Model Law on Electronic Commerce in 1996. The Model Law is intended to facilitate the use of modern means of communication and storage of information. It is based on the establishment of a functional equivalent in electronic media for paper-based concepts such as "writing", "signature" and "original".

The **Convention on Cybercrime** of the Council of Europe is currently the only binding international instrument on the issue of cyber crime. The convention serves as a guideline for countries developing a comprehensive national legislation

[25] Twenty countries originally signed the Convention on the Organisation for Economic Co-operation and Development on 14 December 1960. Since then a further ten countries have become members of the Organisation. The Member countries of the Organisation are: Australia, Austria, Belgium, Canada, Czech republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States.

against Cybercrime. It also serves as a framework for international cooperation between State Parties to the treaty[26].

The Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.

8.2 Laws of major countries

Being at the forefront of computer technology, and being the country that developed what is today referred to as the Internet, the **USA** has been the global leader in developing laws relating to cyber crime.

In 1977, Senator Abraham Ribicoff introduced the first Federal Systems Protection Act Bill. This evolved into House Bill 5616 in 1986, which resulted in the Computer Fraud and Abuse Act of 1987 established as Article 1030, Chapter 47 of Title 18 of Criminal Code. The US states of Florida, Michigan, Colorado, Rhode Island and Arizona were the first to have computer crime laws based on the first Ribicoff bill[27].

Some of the earlier relevant federal legislations include the Communications Fraud and Abuse Act of 1986, the Electronic

[26] The signatories to the Convention are: Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[27] See "Computer Crime: Criminal Justice Resource Manual" published in 1989, downloadable from:
http://www.eric.ed.gov/ERICWebPortal/contentdelivery/servlet/ERICServlet?accno=ED332671

Communications Privacy Act of 1986, the Credit Card Fraud Act of 1984, the Federal Copyright Act of 1976 and the Wire Fraud Act.

Also relevant are provisions of the Electronic Fund Transfer Act (Title XX of Financial Institutions Regulatory and Interest Rate Control Act of 1978) and the Federal Privacy Act of 1974 (codified in 5 USC Sect. 552a).

Some of the more recent US legislations relevant to cyber law are the 'No Electronic Theft' Act (1997), the Digital Millennium Copyright Act (1998), the Internet Tax Freedom Act (1998), the Child Online Protection Act (1998), the U.S. Trademark Cyberpiracy Prevention Act (1999), the Uniform Electronic Transactions Act (UETA) (1999), the Uniform Computer Information Transactions Act (UCITA) (2000), the Electronic Signatures in Global & National Commerce Act (E-Sign) (2000), the Children's Internet Protection Act (2001) and the USA Patriot Act (2001).

In **China**, the relevant laws are the Computer Information Network and Internet Security, Protection and Management Regulations (1997), the Regulations on Computer Software Protection (2002) and the Criminal Law of the People's Republic of China (1979) as revised in 1997.

In **Australia** the relevant law for cyber crime is the Cybercrime Act (2001) and the revised Criminal Code Act (1995). For electronic commerce, the relevant law is the Electronic Transactions Act 1999. Also relevant is The Commonwealth's Privacy Act (1988).

In **Canada**, the relevant law for cyber crime is the Criminal Code as amended to include computer crimes. For electronic commerce, the relevant law is the Electronic Transactions Act (2001).

In **Malaysia**, the relevant law for cyber crime is the Computer Crimes Act (1997). For electronic commerce, the relevant law is the Digital Signatures Act (1997).

In **Singapore** the relevant law for cyber crime is the Computer Misuse Act. For electronic commerce, the relevant law is the Electronic Transactions Act (1998).

In **United Arab Emirates (UAE)**, the relevant law for cyber crime is the Federal Law No. 2 of 2006 Combating Information Technology Crimes. For electronic commerce, the relevant law is the Law No. 2 of 2002 of the Emirate of Dubai – Electronic Transactions and Commerce Law.

In the **United Kingdom** the relevant laws for cyber crime are the Forgery and Counterfeiting Act (1981), Computer Misuse Act (1990), Data Protection Act (1998), Terrorism Act (2000), Regulation of Investigatory Powers Act (2000), Anti-terrorism, Crime and Security Act (2001) and Fraud Act (2006). For electronic commerce, the relevant laws are the Electronic Communications Act (2000) and the Electronic Signatures Regulations (2002).

In **Japan** the relevant laws for cyber crime are the Unauthorized Computer Access Law (Law No. 128 of 1999) and the Online Dating Site Regulating Act (June 2008).

The **European Union** passed the General Data Protection Regulation which came into force on 25th May 2018. The said Regulation aimed at creation of a uniform law across member states.

NINE

9. Basic legal terms and concepts

9.1 Act

In common language, the term Act is synonymous with the terms **legislation**, **statute** and **law**.

The Constitution of India specifies issues for which only the Central Government can make laws e.g. defence, telecommunications. Such laws are also called **Central Acts** and are passed by the Parliament.

After being passed by the Parliament, the Act must receive the assent of the President of India. In the final stage, the Act must be notified in the Official Gazette. The Act does not come into force till it is notified in the Official Gazette.

Illustration: The Information Technology Act was passed by the Parliament and received the assent of the President of India on 15 August 2000. It was notified in the Official Gazette on 17 October 2000. If a person had violated the provisions of this Act on 16 October 2000, he would not be liable as the Act was not in force in India.

The Constitution of India also specifies issues for which only the State Government can make laws e.g. shops such as cyber cafes. Such laws are also called **State Acts** and are passed by the State Legislature.

After being passed by the State Legislature, the Act must receive the assent of the Governor of the state. In the final stage, the Act must be notified in the Official Gazette of the respective state.

An Act is generally divided into the following parts:

- **Preamble** which gives the intention behind the Act
- Extent and applicability of the Act
- **Definitions** and interpretations of important terms
- Main **provisions**
- Penalties and **punishments** for violating the Act
- Powers of Government and its officials to make rules and regulations

9.2 Preamble to an Act

The preamble to an Act reveals the **intention** behind an Act, contains the essential features of the Act and the socio-political objective it seeks to address.

Courts refer to the preamble of an Act only when the provisions of the Act are ambiguous or too general. The preamble is expected to express the scope, object and purpose of the Act more comprehensively. It may narrate the grounds and cause for making the statute.

9.3 Extradition

Extradition is the delivery of a person accused of a crime in one country by the other country where he has sought refuge.

Illustration: Sameer has committed a crime in India and then escaped to USA. The US government could extradite Sameer to India so that he can face trial for his crime.

The delivery takes place pursuant to an existing treaty or an ad hoc arrangement. Extradition is based on the broad principle that it is in the interest of civilized communities that crimes should not go unpunished.

The domestic law of the nation from whom the extradition of the person is sought plays a crucial role in determining whether the State seeking the extradition would be granted its request or not.

Extradition Act, 1962 is the relevant law in India[28].

9.4 Rules & Regulations

Rules and regulations are made under powers given by an Act. They are part of "law".

[28] India has entered into extradition treaties with Belgium(1958), Bhutan (1997), Canada (1987), Hong Kong 1997), Nepal(old Treaty) (1963), Netherlands (1989), Russia (2000), Switzerland (1996), UAE (2000), U.K. (1993), USA (1999), Uzbekistan (2002), Spain (2003), Mongolia (2004), Turkey (2003), Germany (2004), Tunisia (2004), Oman (2005), France (2005), Poland (2005), Korea(ROK) (2004), Bahrain (2005), Bulgaria (2006), Ukraine (2006), South Africa (2005), Belarus (2008), Kuwait (2007) and Mauritius (2008). Additionally India has extradition agreements with Australia (1971), Fiji (1979), Italy (2003), Papua New Guinea (1978), Singapore (1972), Sri Lanka (1978), Sweden (1963), Tanzania (1966), Thailand (1982) and Portugal (2002). Source: Central Bureau of Investigation website http://www.cbi.gov.in/interpol/extradition.php

Illustration: Section 87 of the Information Technology Act empowers the Central Government to make rules to carry out the provisions of the said Act. Under this power the Central Government passed the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003.

Rules and regulations cannot go against the Act under which they have been passed. They also cannot go beyond the scope of the Act.

9.5 Offences

If a person does something which is punishable by any law, then such an act is called an offence and the offender is liable to be punished.

Illustration: Section 66 of the IT Act lays down that a person who deletes someone's data is punishable for "hacking". If Sameer deletes Siddharth's data, then he is liable to be punished for hacking under section 66.

If a person does not do something which he must do under any law, then such an omission is also an offence and the offender is liable to be punished.

Illustration: Section 69 of the IT Act requires a person to cooperate with Government officials during an investigation. Sameer does not hand over his passwords to the police. He is liable for punishment under section 69.

9.6 Intention

Intention is a **state of mind** and is also known as **mens rea**. It can be understood with the help of the following illustration.

Illustration:

Pooja has rejected Sameer's proposal for marriage. Sameer is angered by this refusal and decides to delete some files from her laptop. These files relate to some very important software programs being developed by Pooja. To do this he enters her house without permission.

The act of entering her house without permission is an offence punishable by the Indian Penal Code. The motive for this offence is to destroy property belonging to Pooja.

If he had succeeded in deleting these files he would have been liable for punishment for hacking. Destroying someone's data in order to cause the victim wrongful loss is called hacking and is punishable with 3 years jail and / or Rs. 2 lakh fine.

However, once he enters Pooja's house, he sees that a thief is stealing Pooja's laptop computer. He attacks the thief in order to stop the theft. The laptop is destroyed in the resulting scuffle.

Now even though Pooja's data has been destroyed, Sameer is not liable for hacking. This is because his intention was to protect Pooja's laptop from being stolen.

Mere intention is not punishable. The person must commit the offence with the particular intention in order to be liable for punishment.

When many people commit an offence in furtherance of a **common intention**, each of those people is liable for the acts. A joint liability is imposed on them.

9.7 Abettor

When a person **instigates** or helps or facilitates the commission of offence by another, he can be said to be an abettor.

Illustration:

Pooja has rejected Sameer's proposal for marriage. Sameer is angered by this refusal and decides to hack into Pooja's laptop and delete some files.

These files relate to some very important software programs being developed by Pooja.

He discloses his plan to his friends Siddharth and Mahesh. Siddharth obtains hacking software for Sameer while Mahesh lends his computer to Sameer. Sameer then succeeds in hacking Pooja's computer and deleting her files.

Here it can be said that Siddharth and Mahesh have abetted the offence committed by Sameer.

9.8 Double Jeopardy

A **person cannot be tried more than once for an offence**. When a person has been prosecuted for an offence and has been acquitted or convicted, he cannot again be prosecuted for the same offence.

Exception
Sameer hacks into Pooja's computer. He is prosecuted for the offence of hacking under section 66 of the IT Act and sentenced to 2 years jail.

Later it is discovered that at the time of the hacking he had also misused Pooja's computer to upload pornographic content onto the Internet. He can now be prosecuted for violating section 67 of the IT Act which relates to publishing cyber pornography.

9.9 First Information Report (FIR)

This is the information relating to a cognizable offence given to a police officer. The police investigation proceeds on the basis of FIR.

A **cognizable offence** is one in which the police can arrest a suspect without a warrant from the court. e.g. hacking, publishing cyber pornography, tampering with computer source code, unauthorized access to a protected system.

Any person can give information about a cognizable offence to the police. e.g. a cyber café visitor can inform the police about pornography being viewed from the cyber café.

The police officer must write down this information and take the signature of the informant. The recorded information must be read over to informant and a copy must be given to him.

9.10 Imprisonment

Imprisonment or confinement in prison can be of two types, **simple** and **rigorous** (i.e. with hard labour). The Court can

also sentence a convict to undergo a prison term that is partly simple and partly rigorous.

Life imprisonment is imprisonment for life. The Government can commute life imprisonment to imprisonment up to 14 years for a convict.

9.11 Fine

Most criminal laws empower the Court to award fines in addition to imprisonment terms. The fine is to be paid by the convict and goes to the Government. The Court can also order the convict to undergo additional imprisonment if he does not pay the fine.

9.12 Compensation

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

9.13 Damages

Simply put, damages are the compensation for legal injury. Damages can be of various types:

1. **Compensatory damages** are allowed as a recompense for injury actually suffered.

   Illustration: Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

2. **Consequential damages** are consequential upon the act complained of.

   Illustration: Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

3. **Exemplary or punitive damages** are awarded as a punishment and serve as a warning to others.
   Illustration: Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

4. **General damages** are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

   Illustration: Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs. 10 lakh as compensation.

9.14 Compound

In Concise Oxford Dictionary in Law, the meaning for the word "compound" is given as: (a) condone a liability or offence in exchange for money etc., (b) forbear from prosecuting (a felony) from private motives, and Law come to terms with a person, for foregoing a claim etc., for an offence. For the expression "Compounding" in Ramanathan Aiyar's Law Lexicon, is "Arranging, coming to terms, condone for money; arranging with the creditor to his satisfaction."

TEN

10. Cyber Law & Your World

Cyber Law affects our world in more ways than we can imagine. Think / discuss how the following issues are affected by cyber law.

Aadhaar card

_____
_____
_____

Algorithms

_____
_____
_____

Apps

_____
_____
_____

ATMs

_____
_____
_____

Automobile Event Data Recorders & Privacy

_____
_____
_____

Biometrics

Blocking of information

Blogs

Body Scanners

Budapest Convention on Cybercrime

Business models in cyberspace

Children's Online Privacy

Cloud Computing

_____
_____
_____

Computer Databases

_____
_____
_____

Computer Software

_____
_____
_____

Cookies

_____
_____
_____

Credit, debit & cash cards

_____
_____
_____
_____

Crime as a service

_____
_____
_____

Crypto-currencies

_____
_____
_____

Cryptography Export

Cyber crime

Cyber Crime Investigation

Cyber Forensics

Cyber Havens

Cyber Inheritance

Cyber Insurance

Cyber Monitoring

Cyber Propaganda

Cyber Security

Cyber Terrorism

Cyber Warfare

Dark web

Data breaches

Decryption of Information

Demat accounts

Digital Evidence

Digital lockers

Digital wills

Domain Names

Drones and UAVs

E-courts

E-governance

E-tenders

Ecommerce

Electronic & Digital Signatures

Electronic contracts

Electronic Payment Systems

Electronic voting machines

Email

EU Data Protection Directive

Extradition of cyber criminals

Facebook Facial Recognition

Facebook Privacy

Financial records

Fonts

Freedom of speech in cyberspace

Google Street View

Governance of the Internet

Government sponsored cyber attacks

Grievance platforms

Hacking - whitehat, grayhat, blackhat

Hactivism

Hashtags

Health records

HTML Frames

ICANN's gTLD Program

ICANN's Trademark Clearinghouse

Information Technology Law Compliance

Instant messaging

International & regional treaties

Internet censorship

Internet of Things

IP addresses

Jurisprudence of cyber law

Kindle type devices

Liabilities of Intermediaries

Locational Privacy

Madrid System - International Trademark System

Malware

Medical Record Privacy

Meta tags

Mobile payments

Mobile wallets

Model laws

Monitoring and Collecting Traffic Data

Music streaming

Net banking

Net neutrality

Online auctions

Online gambling & gaming

Online pharmacies

Online regulatory filing

Online reputation

Online share trading

Online tax filing

Open source technologies

Organized Hacking Groups

Patent trolls

Patents in cyberspace

Plagiarism

Platforms like shopify

Rating and review platforms

Regulatory filing

Reverse engineering

Right to be forgotten

Search Engine Privacy

Semiconductor Layout & Design Law

Smart homes

Smartphones

Social Networking Privacy

Software Licenses

Source code

Space missions signal from outer space / Mars

Spam

Standards for security and incident response

Stock audio

Stock images and photos

Stock video

Talent-on-demand

Taxation

Telemedicine

Torrent, p2p and file-sharing

Trademarks in cyberspace

Tweets

Use of proxies

Video conferences

Video makers - using characters etc.

Video streaming

Virtual employees

Virtual offices

Virtual worlds

Vulnerability exchanges

Wearable technology

Web archive

Web hosting

Website policies

WiFi networks

Wikipedia