# Chronology of the Indian Cyber Law

**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:

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

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

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

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.

**2017**

The Government Open Data License National Data Sharing and Accessibility Policy was announced on 10th February, 2017.

**2018**

On 22nd May, 2018, the *Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018* came into force. These rules prescribe information security practices and procedures for protected systems.

On 20th December, 2018, the following Security and Intelligence Agencies were authorised for the purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource under the *Information Technology Act*:

1. Intelligence Bureau;
2. Narcotics Control Bureau;
3. Enforcement Directorate;
4. Central Board of Direct Taxes;
5. Directorate of Revenue Intelligence;
6. Central Bureau of Investigation;
7. National Investigation Agency;
8. Cabinet Secretariat (RAW);
9. Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only);
10. Commissioner of Police, Delhi.

This was done in exercise of the powers conferred by section 69(1) of the Information Technology Act read with rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

**2019**

The Central Government notified the Regional Forensic Science Laboratory, Northern Range, Dharamshala, District- Kangra (Himanchal Pradesh), as Examiner of Electronic Evidence within India, with the following scope:

1. Computer (Media) Forensics excluding Floppy Disk Drive;

2. Mobile Devices Forensics.