Review Document

The Information Technology Act, 2000

Author- Ms. Pooja Mandotar

THE INFORMATION TECHNOLOGY ACT, 2000

Introduction:

The Information Technology Act, 2000[1]gives lawful acknowledgment to exchanges completed by methods for electronic information trade and different methods for electronic correspondence, regularly alluded to as"electronic commerce", which includes the utilization of alternative to paper-based methods of correspondence and storage of data, to facilitate electronic filing of documents with the Government offices and further 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 and for issues associated therewith or coincidental thereto. The Information Technology Act, 2000 extends to the whole of India and it applies likewise to any offense or contravention thereunder committed outside India by any individual.

Significances and object of the act:

1. All electronic agreements made through secure electronic channels and are legally valid.
2. Legal recognition for digital signatures.
3. Safety efforts for electronic records and also digital signatures.
4. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized
5. Provision for establishing a Cyber Regulation Appellate Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.
6. Digital Signatures will use an asymmetric cryptosystem and also a hash function.
7. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities.

[1] https://www.indiacode.nic.in/handle/123456789/1999

8. Senior police officers and other officers can enter any public place and search and arrest without warrant.
9. The act also provides legal recognition to digital signatures which need to be duly authenticated by the certifying authorities.
10. The provisions of the I.T. Act have no application to negotiable instruments, power of attorney, trust, will and any contract for sale or conveyance of immovable property.

Non- Application of the Information Technology Act, 2000:

1. Negotiable Instrument(Other than a cheque) as defined in The Negotiable Instruments Act, 1881;
2. A power-of-attorney as defined in The Powers of Attorney Act, 1882;
3. A trust as defined in The Indian Trusts Act, 1882;
4. A will as defined in The Indian Succession Act, 1925 including any other testamentary disposition;
5. Any contract for the sale or conveyance of immovable property or any interest in such property;
6. Any such class of documents or transactions as maybe notified by the Central Government.

Important provision:

1. Section 2(d) -affixing electronic signature with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
2. Section 2(zc) - defines private key as a key pair used to create a digital signature.
3. Section 2(zd) - defines public key as a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
4. Section 5 - Legal recognition of electronic signatures, where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of (electronic signature) affixed in such manner as may be prescribed by the Central Government.

5. Section 15 - Secure electronic signature which states an electronic signature shall be deemed to be a secure electronic signature if— (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.
6. Section 61 - No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the [Appellate Tribunal] constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.
7. Section 65 - Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
8. Section 66 - If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
9. Section 67 - Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
10. Section 71 - Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or [electronic signature] Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

11. section 72 - Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
12. Section 74 - Whoever knowingly creates, publishes or otherwise makes available a 1 [electronic signature] Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
13. Section 75 - Act to apply for offence or contravention committed outside India.–(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Recent Amendment:

1. A major amendment was made in 2008. Amendment introduced-

a) Section 66A which penalized sending of "offensive messages".
b) Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".
c) It also introduced penalties for child porn, cyber terrorism and voyeurism. Amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (PratibhaPatil) on 5 February 2009.

2. The newly amended act came with following highlights −

a) It stresses on privacy issues and highlights information security.
b) It elaborates Digital Signature.
c) It clarifies rational security practices for corporations.
d) It focuses on the role of Intermediaries.
e) New faces of Cyber Crime were added.

The various offences and corresponding punishments thus summarized and tabulated below with detailed explanation in the following:

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000

LEGAL EAGLE
LAW FORUM

66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.
6B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyber terrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India,	Imprisonment up to life.

LEGAL LAW FORUM

		then he commits cyber terrorism.	
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child thus defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹200,000

69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

Loopholes:

1. ITA 2000 does not deal for Proper Intellectual Property Protection for Electronic Information and Data. Contentious yet very vital issues concerning online copyrights, trademarks and patents have been left unnoticed by the law, thereby leaving many loopholes.
2. It does not pay any heed on Domain Name related issues. It does not deal with the rights and liabilities of domain name holders.
3. It does not cover various evolving forms and manifestations of cybercrimes such as:

a) Cyber theft;
b) Cyber stalking;
c) Cyber harassment;
d) Cyber defamation;
e) Cyber fraud;
f) Chat room abuses;
g) Misuse of credit card numbers.

4. It does not touch upon antitrust issues.
5. It is not explicit about regulations of electronic payments.
6. How Facebook and WhatsApp got away without having to pay a penny[2]:
   Adv (Dr) Prashant Mali, cyber & privacy law expert at the Bombay High Court explains that the companies are covered within the definition of the "Intermediary" under Section 2(1) (w) of the Information and Technology Act, 2000. "WhatsApp and Facebook are covered by the 'safe harbour' provision under Sec-79 of the IT Act, 2000, which exempts intermediaries from liability in certain instances," says Mali.The law states that intermediaries will not be liable for any third party information, data or communication link made available by them. Furthermore, the guidelines do not specify any penalty or damage to be borne by a company if the rules are not followed. In addition, the Computer Emergency Response Team (CERT) does not penalize intermediaries to report a breach or unauthorized access on their own accord. The IT Act, 2000 does not also deal at all with the Intellectual Property Rights of Domain Name owners. Contentious yet very important issues concerning Copyright,

[2] https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html.

Trademark and Patent have been left untouched in the said law thereby leaving many loopholes in the said law.

Conclusion:

The information technology has brought it's scar in the form of cybercrime, moreover the new business environment required new regulations for it's legal endorsement as more and more business communities are moving towards electronic commerce and trans border contracts.The Information Technology Act 2000 is applicable to the whole of India, including any offense committed outside India, if such contravention involves a computer, computer system or computer network located in India. This has paved the way for the growth of e-commerce and e-transaction, thereby advancing economic growth and a new era of e-governance has come into existence which helps in bringing transparency, efficiency and accountability in governance.

LEGAL EAGLE
LAW FORUM

About the Author

My name is Pooja Mandotar and I am studying Bishop Cotton Women's Christian Law College, Bengaluru. My experience at LEGALEAGLE LAW FORUM, internship was for 4 weeks, which started with a zoom call to explain us regarding the research to be accomplished. After which I was given a set of 6 Bare Acts Title which was supposed to be completed by me. It was a great learning opportunity for me. The research work has made me to accept more in my composing aptitudes and has acquired a lot of certainty in me concerning my capacities to think and efficiently put it down in writing. I would like to thank the Organization for giving out an opportunity like this, especially during a pandemic situation, and a special thanks to the mentors for being so cooperative with me and clearing the doubts in a short span of time.