AD EDUXIAN JOURNAL
A Quarterly Multidisciplinary Blind Peer Reviewed & Refereed Online International Journal
Google Scholar Indexing IF: 1.024
Vol (2), Issue (1), Feb-April 2025 ISSN: 3048-7951

SHADES OF ACCESS: CYBER lAWS RELATING TO RTI ACT, 2005

Vivek Swami* & Dr. Ravinderjeet Kaur**

Review: 15/05/2025 Acceptance: 28/05//2025 Publication: 16/06/2025

Abstract:
Being a welfare State, the Government of India enacted Information Technology Act, 2000 to provide legal recognition to the transaction being carried by electronic data. The Information Technology Act,2000 came into existence w.e.f. 18.10.2000. By doing so, cyber crime/cyber frauds shall come to an end because IT Act, 2000 has provided protection to the citizens of India. The Government of India has also notified the Right to Information Act, 2005 for providing accessible information to the citizens of India. As per this act, now citizens of India has got right to seek information about the project of the State/ Government of India. The Right to Information Act, 2005 shall also be helpful in getting information about the cases of cyber crime because now the citizens have got right to ask for the stage of cases of cyber fraud. Since before 2005, there was no provision for getting information about the progress of the case of a person so it is very good step taken by the government for the welfare of citizens of India.

Keywords: Electronic data, legal recognition, digital technology, cyber security, digital system, computer resource, public authority, third party information, punishment, right to information.

Introduction:

The fact that cybercrime is on the rise in India is no secret. The innocent people of India are being targeted by criminals, which has caused great concern among the Indian people. Because cybercriminals in India have come up with a plethora of new techniques, no amount of effort by the Indian government to curb cybercrime has been effective. Here are a few instances of cyber crime: Following a raid on a phoney contact centre in Mohali's Industrial Area Phase 8 on June 25, 2024, 37 individuals were apprehended by the police. The 37 individuals were indicted by the Mohali police under sections 406, 420, and 120B of the IPC. Now that the Enforcement Directorate has requested the records of the Mohali police station, they can move forward with the investigation of the 100 crore embezzlement case.

Indian Air Force retired personal fell prey to cyber scam in September 2024, losing 3.64 lakhs rupees while attempting to settle a petrol bill in Pune. The retired officer received a call from someone threatening to cut off gas service unless the debt was paid by 9:00 p.m. The cybercrime has been reported in Pune city using a First Information Report (FIR).

A Chandigarh-based doctor in September 2024 Homoeopathic Medical College and Hospital employees in Sector 26 fell victim to a Rs 39.7 lakh scam involving con artists pretending to be from the Enforcement Directorate (ED) and the Communication Regulatory Authority of India. A caller asserted that his SIM card, which is associated with Aadhaar, was used for illicit purposes and was associated with terrorist operations. The complainant stated that he was contacted by a man posing as SB Shiradkar, an officer from Lucknow's Enforcement Directorate, who had been transferred to a phone call from what seemed like a police station. Scammer threatened cooperation by wire transfers of monies purportedly for RBI audits and investigations, threatening 5-7 years in prison if he did not. Scammers demanded many payments spread out over weeks while displaying fake RBI letters with the emblems of the Reserve Bank of India. The doctor had wired Rs 39.70 Lakh despite the prospect of jail time. The con artists also preyed on the victim's father, an eye surgeon and head of department at Guru Nanak Mission Hospital in Jalandhar; they told him his son was in police custody and took almost Rs 12 lakh from him. The Vardhman Group conned Shri S.P. Oswal out of 7 crores of rupees in August 2024. Here is the order in which cyber scams typically occur:

August 27 Shri SP Oswal received a voice call from a scammer posing as a TRAI offical. He also received a whatsapp call from a person posing as a CBI Officer from Mumbai.

August 28 Mr.Oswal received 25 to 30 calls and started transferring money to the callers' accounts.

August 29 Mr.Oswal paid rupee 7 crore to the callers in 5 installments.

August 30 Mr.Oswal came to know that he has become a victim of cyber crime and he approached the police.

September 17 police arrested two accused from Assam and recovered a some of rupee 5.25 crore.

The Central Government has notified the Information Technology Act, 2000 to avoid cyber fraud, which is as under. On May 9, 2000, the then-Minister of Information and Technology presented the measure to the president for signature, and the law was subsequently enacted by the parliament. Restrictions on cyber fraud were introduced by the Information Technology Act, 2000, which came into effect on October 18, 2000.

Transactions conducted by electronic data interchange and other forms of electronic communication, sometimes known as "Electronic Commerce, are granted legal status by the Information Technology Act, 2000.

Cyber Security: Cyber Security means protecting of Information relating to computer from unauthorized access.

Cyber Café: It means any place from where access to internet is offered by any person**.**

Digital signature:

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.

Computer Resource means computer, computer system, computer nertwork, data, computer data base or software.

Digital Signature Certificate means a digital signature certificate issued under the IT Act 2000 .

License: Controller has the authority to grant license or reject the same. Cases of Cyber-attacks in India:

In accordance with the data received in the Parliament, nearly 1.16 million cases of cyber-attacks in India were reported in India in 2020.

Computer Emergency Response Team (CERT-In):

The functions, establishment and working of the Computer Emergency Response Team which is as under:

- ✓ CERT-In is operational from 2004.
- ✓ CERT-In comes within the Ministry of Electronics and Information Technology.
- ✓ It has been established as a nodal agency to deal with cyber crime i.e. hacking and phishing.

The functions of the CERT-in is as under: Collection, analysis and dissemination of information on cyber incidents

- ✓ Forecast and alerts of cyber security incidents
- ✓ Emergency measures for handling cyber security incidents
- ✓ Coordination of cyber incident response activities
- ✓ ○Issue guidelines, advisories".
- ✓ Along with 26 other intelligence and security organisations, the CERT-In is currently not subject to the Act.

Important Section of Information Technology Act 2000 relating to offences :

Tempering with computer source document : This includes knowing and purposeful actions such as modifying, erasing, or concealing computer source code or encouraging another individual to do the same. Two lakh rupees in fines or three years in prison, or both, is the maximum penalty for these acts. What we call a computer's "source code" is actually its blueprint, instructions, design, and code.

Computer related offences: The crime of hacking falls under this category and carries a maximum penalty of three years in prison or five lakh rupees fine, or both.

Punishment for dishonestly receiving stolen computer resource: Any infraction of this provision may result in a fine of up to one lakh rupees or three years imprisonment, or both. The defendant ought to have known, or should have known, that the device was taken.

Punishment for identity theft: Offenders may face a maximum fine of Rs 1 lakh and/or a jail sentence of three years for this offence.

Punishment for cheating: Creating a phoney profile, obtaining unauthorised access to an account, and hacking into someone's tax account are all instances of social media fraud. A term of up to three years in jail is the sanction for deceit. A sum of up to one million rupees.

Punishment for capturing, publishing or transmitting an image of a person's private area without consent: Punishment : Anyone found guilty of a violation of this clause faces a maximum penalty of two lakh rupees in fines or three years in prison, or both.

Punishment for Cyber Terrorism: If you are found guilty of cyber terrorism, you might face a punishment of up to ₹15,000,000 or a maximum of 15 years in prison, with no chance of parole. Cyber terrorism is a crime that does not permit bail and carries a maximum penalty of five years in prison and a fine of up to one million Indian rupees.

Punishment for publishing or transmitting electronic material: The punishment is a prison term of up to five years and a fine of up to ten lakh rupees. "Second or subsequent conviction, The punishment is imprisonment up to seven years and a fine of up to ten lakh rupees. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Intermediaries: Intermediaries are those such as Internet Service Provider (ISP), who preserve and retain information as specified by the Central Government. The Central Government can prescribe the duration, manner, and format for preserving and retaining information. Intermediaries who intentionally or knowingly violate the provisions of the section can be punished with imprisonment for up to three years and/or a fine.

Importance of Information Technology Act 2000

- ✓ The Information Technology Act, 2000 has provided legal recognition to electronic records.
- ✓ As per section 4 of the Information Technology Act, 2000, now there is a legal recognition to electronic signatures as equivalent of physical signatures.
- ✓ There shall be the Controller of Certifying Authorities (CCA), a government body responsible for issuing guidelines for security of digital signatures and certificates.
- ✓ It is compulsory for companies to obtain consent from consumers before getting personal information.
- ✓ There is a provision for compensation in case of damage or misuse of their personal data.
- ✓ The Government of India is authorized to criminalize cybercrime.
- ✓ The Cyber Appellate Tribunal is to be established to adjudicate the cases relating to cyber crimes.
- ✓ The IT Act 2000 vouch save the critical information.

Objectives:

- ✓ The IT Act 2000 shall be helping in promoting and delivery of government services electronically.

- ✓ There is a provision of penalties under this act.
- ✓ Promote the expansion of electronic data.

Features:

- ✓ The Government of India has to regulate electronic commerce.
- ✓ The IT Act 2000 bestows responsibilities of intermediaries
- ✓ CERT-In (Indian Computer Emergency Response Team) is responsible for cyber security and cyber incident response.

Information Technology Act 2000 and its amendments:

1. **Amendment of 2008**
   Section 66A of the Information Technology Act 2000 was amended in the year 2008 relating to penalty for sharing offensive messages.
   Amendment Bill 2015
   In the year 2015, section 66A was again amended for safeguarding the fundamental right but later on it was proved to be violative of Article 19 of the constitution.
   Section **4** of the Information Technology Act, 2000, deals with the legal recognition of electronic records. It states that if a law requires information to be in writing, typed, or printed, then the requirement is satisfied if the information is:
   Made available in an electronic form
   Accessible so that it can be used for reference
   This means that electronic records are given the same legal recognition as paper-based documents.
   Section 5 of IT Act of 2000 in India pertains to the legal recognition of electronic signatures.

Explanation

a. If a law requires a signature or document to be signed, then an electronic signature can beused instead.
b. Central Government
c. The Central Government can prescribe the manner in which an electronic signature should be done.

Interpretation; The term signed can refer to a person's handwritten signature or mark on a document.

Purpose

a. The IT Act 2000 was introduced to regulate electronic activities and data storage in response to the rise in cybercrime and data-related offenses.
b. Section 6 of the Information Technology Act (IT Act) of 2000 deals with the use of electronic records and signatures in the government and its agencies. The section states that:
   i. The appropriate government can prescribe the manner and format for filing, creating, or issuing electronic records.
   j. The appropriate government can also prescribe the method of payment for filing, creating, or issuing electronic records.
   k. If a law requires a form, application, or other document to be filed with a government

office, the appropriate government can prescribe an electronic form to satisfy the requirement.

l. The IT Act was introduced in response to the rise in cybercrime and data-related offenses in India.
m. Section 7 of the IT Act of 2000 pertains to retention of electronic records.
n. The electronic record must include details that identify the origin, destination, date.
o. The electronic record must be kept in the format in which it was originally generated, sent, or received.
p. The electronic record must be kept in a format that can be shown to accurately represent the information originally generated, sent, or received.
q. The Information Technology Act (IT Act) of 2000 was introduced in response to the rise of cybercrimes and data-related offenses in India". One of the main objectives of the Act is to promote electronic governance.

Information Technology Act 2000 Sections

Appellate Tribunal

According to section 48 of the IT Act of 2000, the appellate tribunal for this act will be the Telecom Dispute Settlement And Appellate Tribunal, which was set up under section 14 of the Telecom Regulatory Authority of India Act, 1947. The jurisdiction of the appellate tribunal will be specified by the Central Government through a notification.

Advantages: Courts began to accept electronic correspondence (emails, texts, etc.) as evidence with the passage of the Information Technology Act of 2000. Involvement in electronic trade or business is permissible for companies. Compensation for damages is included in the provision.Various forms of cybercrime, including hacking, spamming, identity theft, and phishing, are punished by the Act.

a. Thanks to digital signatures, transactions are now quite simple.
b. Statutory remedies are now available for unauthorised access or hacking.
c. The Indian government can now use e-governance to post notices online.
d. Companies can now offer digital certifications.

Disadvantages:

a. Many forms of cybercrime, including cyberstalking, cyberfraud, abuse in chat rooms, and theft of internet hours, are not addressed by the ITAct of 2000.
b. The problems related to domain names are not being resolved by the Information Technology Act of 2000.
c. Important matters like privacy and content regulation have gone unaddressed in the IT Act. Additionally, protection of intellectual property rights associated with computer programs and networks is not included.

Right to Information Act- 2005

Examining such a system in government organisations before 2005 was important for the public good since it helped identify problem areas brought about by ineptitude, waste, and corruption. The right to information is enshrined in the Constitution, as the Supreme Court has pointed out in citing Articles 19 and 21.

Consider a homeowner who requested a new electrical connection but had an extended period of waiting before it could be set up. The failure to identify the cause of the holdup has resulted in corruption in some cases due to the delay in establishing new electrical connections. There are a number of additional ways in which public agencies can experience delays. It is common practice for regular people to be asked to return to the same officenumerous times to get their problems fixed, even though it is unreasonable to presume that all government organisations are the same.

In a case titled as ***State of Uttar Pradesh vs. Union of Inda***[i]; In a recent ruling, the Hon'ble Apex Court emphasised the importance of public agents being held accountable for their actions in all public offices. The court argued that a transparent system of government would eliminate nepotism, ineffective leadership, and delays in open offices. According to this view, public officials should be held to high standards of personal responsibility for their actions, and those found guilty should face severe consequences.

The Hon'ble Apex Court in ***S.P. Gupta vs Union of India and others***[ii]maintained that a democratic system guarantees citizens the right to know how their government is run. Furthermore, the Hon'ble Apex Court ruled that the government's apparatus is ill-prepared to enhance the conventional bureaucracymindset.

The Right to Information Act was enacted on October 10, 2005. Citizens of India have the authority to request information from the relevant authorityaccording to the Right to Information (RTI) act of 2005.

The Right to Information (RTI) Act, 2005, encourages openness and responsibility in government operations. Information can be requested across India under the RTI Act, 2005.

The RTI Act, 2005 encompasses all organisations, including NGOs and PSUs, that were established under a law or a government notification and received substantial funding from the government.

Objectives:

- **a.** By the RTI Act,2005, now information is accessible.
- **b.** The RTI Act, 2005 promote transparency and accountability.
- **c.** It would help in reducing corruption and red tapism.

Significance:

- **a.** Article 19(1)(a) and Article 21 of the Constitution guarantee fundamental rights, which are protected by the RTI Act 2005.
- **b.** The responsibility for carrying out the provisions of the RTI Act 2005 rests with the public authorities.

c. When judging on an appeal or application under the act, a quasi-judicial power is being exercised.

IMPORTANT FEATURES OF RIGHT TO INFORMATION ACT, 2005

As per the Act, every citizen has right to get information.

a. Information encompasses several aspects such as reviewing tasks, paperwork, and records, taking notes on files, and so on.
b. Any citizen can apply to the PIO or APIO for information in order to receive it. Within 30 days, the requested information must be provided.
c. An appeal can be lodged if the data is not furnished within thirty days.
d. The highest fine for failing to provide information is Rs. 25,000/-. Within 48 hours, you can get information that pertains to a person's life or liberty.
e. The government of India (GOI) and the state governments (State Govt.) are each tasked with establishing an information commission.
f. The ways in which the Right to Information Act of 2005 might counteract cybercrime. This is what needs to be said:
g. Every Indian government agency, whether established by statute, executive order, or constitutional provision, is subject to the Right to Information Act of 2005. Any private entity that the government owns, controls, or provides major funding to is likewise subject to this regulation.

Access to information: Every Indian citizen has the legal right to see official documents and data kept by their government, as stated in Section 2(f)(j) of the Right to Information Act, 2005. As part of this, you have the right to request electronic copies of documents, records, and work.

Transparency and accountability: Indian citizens can aid in the fight against corruption by taking use of the Right to Information Act of 2005, which mandates openness and responsibility on the part of government agencies.

Exemption to Computer Emergency Response Team-in: Section 24(2) of the Right to Information Act 2005 states that intelligence or security organisations might be exempted from the RTI Act by the Central Government. Nonetheless, among the duties of the Computer Emergency Response Team is the gathering,analysis, and simulation of data pertaining to cyber events. In order to prevent cybercrime in India, it may be useful to get information from various offices in accordance with the Right to Information Act of 2005. The fact that cybercriminals sometimes use tactics like digital arrest, phone scams in which they pretend to be family members in order to steal money or access sensitive information, and other similar tactics is concerning.

Conclusion

The Government of India passed the Information Technology Act of 2000 in response to the plight of the innocent victims of cybercrime. It is widely recognised that cyber crime has decreased following this act, and now individuals are expressing their issues to the relevant governmental authorities in an effort to get them

addressed. A lot of work needs to be done by both the government and the people of India to regulate cyber crimes, even if the government is taking major measures in that direction

*Research Scholar, RIMT-School of Legal Studies, RIMT University, Mandi Gobindgarh.

**Assistant Professor, RIMT-School of Legal Studies, RIMT University, Mandi Gobindgarh.

[i] 1975 AIR 865.
[ii] 1982 (2) SCR 365.