PIER COUNSEL

NEW DELHI NCR | MUMBAI | BANGALORE | SILICON VALLEY | SINGAPORE

Primer on Data Protection and Information Technologies laws of India

January 2021

About Pier Counsel

Pier Counsel is a boutique law firm consisting of seasoned professionals. We are adept in providing comprehensive legal services across the entire spectrum of transactional, advisory, litigation and regulatory matters. Our areas of expertise include Corporate & Commercial; Private Equity, Venture Capital, Seed funding, Intellectual Property, Data Privacy, Media and Technology and Start-up advisory. Our success is driven by our core values which form the very foundation in defining our cohesive culture and what we stand for as a team. We have a lean Partner to Associate ratio which ensures the quality of services to the clients at all times. We provide a quick turnaround time, on-deck availability with quality, reliability and consistency for every client's deliverable.

We provide pragmatic and exceptional commercial service and strive to achieve results that exceed the expectations of our Clients while adding maximum value to their business.

We aim to be a reference to law firms in India and assist entrepreneurs to achieve their business objectives by providing innovative, efficient and effective legal solutions.

Disclaimer

Contacts

Feel free to reach out to us at info@piercounsel.com.

Acknowledgements

We appreciate the efforts of our interns, Miss Sakshi Kashyap, Miss Shinjini Agnihotri, Mr. Niteesh Sindhe and Miss Devashree Nimbhorkar in preparing this primer.

Introduction

The meteoric rise of technology in the recent decade has shown the potential of market disruption through the effective use of data. It is an established fact that the apt use of data can lead to the position of a market leader in a considerably lesser period of time. The potential of growth is of an exponential kind and the same is evinced with each passing day.

As has been the fact, The Government of India recognised the potential of disruption that can be caused due to the development of this new arena, brought in a number of Acts and rules to regulate the activities of such entities in order to combat the potential situation of disharmony and to meet the demands of the present-day times. The laws cannot be said to be in complete control of the impending situation but are significant enough to show some degree of constrain to the ever-evolving technological sector.

The document is an attempt to cover the legal purview of data protection laws existing in the country. In this document, a detailed study of Information Technology Act, 2000; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 has been undertaken to understand the ambit of data protection and information technologies laws present in the country.

The Information Technology Act, 2000

The information technology act, 2000 (Hereinafter *IT Act*) has over the period of time, gone through a myriad of changes to meet the demands of the dynamic world. According to its preamble, *it provides legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filings of documents with the Government agencies and further to amend the Indian Penal Code, Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.*

The IT Act was introduced by the Parliament to provide for a regulatory framework in light of the digital shift from physical paperwork. The Act gives electronic records legal standing and makes it easier to file paperwork with government bodies electronically. The core objective of the Information Technology Act 2000 was:

a) To provide legal recognition of e-records;
b) To provide legal recognition of digital signature. Traditional signatures are prone to forgery and tampering, hence insufficient for online transactions and contracts. Online transactions require unique and strong protection which is fulfilled by a digital signature;
c) To provide legal recognition for electronic governance. The term e-governance implies a technology-driven government where government adopts technology to provide efficient delivery of services, information, and education

Chapter III, S. 4 to S. 10-A of the Act provides provisions regarding E-Governance. The provisions under Chapter III of the act provide for the legal recognition of the core objective of the Act as abovementioned.

With a shift in society towards digitalisation, with opportunities and prospectus in the virtual space problems also arose in form of cyber frauds and crimes. Persons who were victims of cyber-offences had to seek protection under the Indian Penal code 1860 *(Hereinafter referred to as "IPC")* which was inadequate to deal with the growing menace of cyber offences. These offences were both novel and hi-tech, hence requiring new categorization which is dealt with under the IT Act 2000 after an amendment in 2008.

Cyber offences

The nature of crime has changed over the years, criminals do not need to reside in the same country or even the same hemisphere to commit offences or crimes. The reason is that the Internet has no borders, thus making it easier for offenders to commit crimes. The internet provides quick access to an online base of targeted consumers as well as plenty of opportunities to elude legal enforcement laws of the land.

To prevent such crimes from happening the Act has endowed the power to authorities for investigating and adjudicating computer offences, as well as penalties for cyber offences. It outlines violations like hacking computer systems, tampering with source code, electronic dissemination of obscene information, and penalties for computer or computer system damage.

The consequences for losing or damaging data relating to a computer system is defined under S. 43 of the Act. The section refers to a person who is responsible for the data loss on a computer network or system. In response, S. 44 deals with the data recovery failures, failures to retrieve lost information, returns, and so on. The phrase for such cyber-crime is included in S. 45. The following are some examples of such clauses:

a) Access to a computer network or system without authorization.
b) Data from a computer information system, network system, or database is copied, extracted, or downloaded. This includes the deletion of critical data, which can lead to data theft. Infringement of the Copyright Act, such as downloading an unpublished film or music, is also included.
c) Destroying or losing data by removing important files from a hard disc.
d) Refusing or triggering Refusal of Access to anyone on their own system.
e) Adding surcharges for extra services and adjusting the computer network's parameters.

Provisions dealing with Cyber offences

Chapter XI provides for the offences that are punishable under the IT Act with a fine, or imprisonment, or both.

Section	Particular
S. 66	Tampering with the computer source documents
S. 66	Computer-related offences

S. 66A *(Repealed)*	Punishment for sending offensive through communication service etc
S. 66B	Punishment for dishonestly receiving stolen computer resources or communication device
S. 66C	Punishment for identity theft
S. 66D	Punishment for cheating by personation by using computer resource
S. 66E	Punishment for the violation of privacy
S. 66F	Punishment for cyber terrorism
S. 67	Punishment for publishing or transmitting obscene material in electronic form
S. 67 A	Punishment for publishing or transmitting material containing sexually explicit acts, in the electronic form
S. 67B	Punishment for publishing or transmitting of material depicting children in sexually explicit acts, in electronic form
S. 67C	Preservation and retention of information by intermediaries
S. 72	Penalty of breach of confidentiality and privacy
S. 72A	Punishment for disclosure of information in breach of lawful contract
S. 73	Penalty for publishing electronic signature Certificate false in certain particulars.
S. 74	Publication for a fraudulent purpose.

As mentioned in the preamble of the IT Act, the Act aimed to govern and regulate the e-commerce and e-transactions happening in the country. But this left a large part of electronic activities outside the scope of the law such as identity theft, violation of privacy, etc. People had to register complaints of such offences under the provisions of the Indian Penal Code and other peripheral legislation. These legislations did not address the concerns of the people and hence to regulate cyber-offences amendments were brought to

the IT Act. It can be seen from the above table that amendments have been made to incorporate offences related to the human body in form of cyberstalking, cyberbullying (although these terms have not been specifically used under the Act).

One Section that has attracted a lot of controversies is S. 66A, it was struck down by the Supreme Court in the *Shreya Singhal v. Union of India* case, yet was continued to be enforced even after the passing landmark judgment. The Supreme court has directed the government, Ministry of Home Affairs not to register cases under S. 66A and sensitise the law enforcement agencies on the judgement of the Supreme Court.

Justices J. Chelameswar and R.F. Nariman in the *Shreya Singhal v. Union of India* declared Section 66A unconstitutional for *"being violative of Article 19(1)(a) and not saved under Article 19(2)."*[1] The bench further observed *that "Section 66A is cast so widely that virtually any opinion on any subject would be covered by it …and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total"*

The following are the provisions under which the aggrieved person filed a complaint previously. It is to be noted that a person may still file a complaint against a person under the following provisions-

Provision/Legislation	Particular
Sec.503 IPC	Sending threatening messages by e-mail
Sec 499 IPC	Sending defamatory messages by e-mail
Sec.463 IPC	Forgery of electronic records
Sec.420 IPC	Bogus websites, cyber frauds
Sec. 383 IPC	Web-Jacking
Sec. 500 IPC	E-Mail Abuse and Email Spoofing
Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985	Online sale of Drugs

[1] *Shreya Singhal v. Union of India* (2013) 12 S.C.C. 73

Co-relation of data protection, fundamental rights and the IT Act

With the advent of digitalisation, expansion of the virtual world and the inherent linkage formed between storage of personal data with digital entities has created a concern for the protection of personal data all over the world. Moreover, data protection and privacy of individuals has become the centre stage since the Big Data Politics and scams such as Cambridge Analytica, Facebook Papers, etc. have been unearthed.

Under the Indian jurisdiction 'Privacy' is a fundamental right under the Constitution as upheld in the landmark judgement of *Justice Puttaswami v. Union of India*. In line with this, data protection laws were aimed to be incorporated. These laws have been done so with the insertion of S. 43A and 72A in the IT Act that deals with the compensation for failure to protect personal data and punishment for disclosure of information in breach of lawful contract respectively.

> *Section 43A*
> *"If a body corporate is negligent in maintaining reasonable security practices and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."*

> *Section 72A:*
> *"Any person who, while providing services under the terms of lawful contract, has secured access to any personal information of an individual with the intent to cause wrongful gain or wrongful loss, discloses such information without the consent of such individual, to any other person, then such person committing such act shall be punished with imprisonment for a term which may extend up to 3 (three) years, or with fine which may extend up to INR 500,000 (Indian Rupees Five Hundred Thousand), or with both."*

The following sections deal with the rules that have been enacted under the IT Act and their correlation with data protection and privacy. Briefly, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,

2021 were enacted so as to shoulder the responsibility of data protection on the body corporates who stored or processed data of consumers. These rules are legal regulatory compliances that have to be undertaken by entities who fall under the ambit or scope of the Rules. The section has also discussed in detail other rules and regulations that are relevant to the IT Act.

The provisions of the IT Act are inapplicable on the following categories of documents:

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

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("*Security Rules*")

The IT Act under S. 43A provides for a set of rules, namely the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 *(Hereinafter referred to as "SPDI Rules")*, for every entity that owns or processes data in form of personal information. The Entity has to comply with the SPDI Rules in order to implement reasonable security practices for the protection of data. The entities included within the ambit of the SDPI Rules are those which collect, receive, possess, deal or handle information of provider of information.[2] Rule 3 defines "Sensitive

[2] Rule 4, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011,

Personal Information" as information relating to a person which consists of information regarding:[3]

(i) password
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details
(iii) physical, physiological and mental health condition
(iv) sexual orientation
(v) medical records and history
(vi) Biometric information
(vii) any detail relating to the above clauses as provided to body corporate for providing service and
(viii) any of the information received under the above clauses by body corporate for processing, stored, or processed under lawful contract or otherwise.

The SPDI Rules provides that a body corporate, defined under S. 43A of the Act, shall establish a privacy policy for handling or dealing in personal information, including sensitive personal data or information, and ensure that the same is accessible to those who have provided such information under a lawful contract.[4] Such policy shall be published on the website of the body corporate or any person acting on its behalf and shall include:

(i) clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal information collected;
(iii) Purpose for which information is being collected and used;
(iv) The manner of disclosure of information; and
(v) Reasonable security practices followed.

A body corporate must follow certain guidelines while collecting information such as:

a. Obtain consent from the user
b. Collection should be for a lawful purpose
c. The information shall be processed for the purpose for which it was collected
d. Ensure that the user is aware of the manner in which, and the purpose of, the information that will be used

[3] Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011,
[4] Rule 4, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011,

e. Allow person the choice to review the information provided and allow them to correct
f. Allow the person an option to not provide the information that is being sought
g. The user shall have the option to withdraw their consent provided earlier
h. Maintain security of the information
i. Designate a grievance officer whose contact details hall be displayed on the website of the body corporate

Additionally, SDPI Rules provide other safeguards for the protection of privacy, such as prior permission from the user regarding disclosure of information by the body corporate to a third party unless provided by law.[5] A body corporate cannot publish by itself or on someone's behalf any sensitive personal information. And in case, a third party receives sensitive personal information from a body corporate, it shall not disclose it further as per the SDPI Rules.

Rule 8 outlines the reasonable security practices and procedures that the collecting entity may use. International Standards (IS/ISO/IEC 27001) are some examples of standards that a body corporate can use to ensure data security. An auditor shall conduct reasonable security practices and procedures audit at least once a year or whenever the body corporate or a person acting on its behalf makes significant changes to its processes and computer resources.[6]

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Central Government notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 *(Hereinafter referred to as "Intermediary Rules, 2021")* to supersede the Information Technology (Intermediary Guidelines) Rules, 2011, and prescribe the minimum standard of due diligence that has to be observed by an intermediary. Intermediary 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, as well as anyone who receives, stores or transmits that record on behalf of another person.[7] Sub-section (2) of

[5] Rule 6 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[6] Rule 8, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011,
[7] S. 2 (1)(w), The Information Technology Act, 2000

Section 79 of the Act puts the obligation on the intermediaries to observe due diligence that is mandated by the Central Government. The Intermediary Guidelines entail the following duties for an intermediary, including social media intermediary, namely:[8]

I. Duty to publish: An intermediary shall publish the rules and regulations, privacy policy and user agreement for access of its resources by the users on its website, mobile application or both, as the case may be.

II. Duty to inform: An intermediary shall, by rules and regulations, privacy policy and user agreement, inform the user that it will not host, display, upload, modify, publish, transmit, store, update or share the information which:
   a. belongs to another person and to which the user does not have any right;
   b. is objectionable due to being defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, etc or otherwise inconsistent with or contrary to the laws in force;
   c. is harmful to a child;
   d. infringes any patent, trademark, copyright or other proprietary rights; (v) violates any law for the time being in force;
   e. deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
   f. impersonates another person;
   g. threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;
   h. contains a software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
   i. is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person.

III. Duty to inform annually: An intermediary shall annually notify its users (i) regarding any change in its rules, regulations privacy policy or user agreement and (ii) regarding termination of user's access right, in the event of non-compliance with the

[8] Rule 3, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

intermediary's rules and regulations, privacy policy, or user agreement for access or usage of the computer resource, it can also remove non-compliant information;

IV. Duty to not host certain information: An intermediary shall not host, store, or publish any unlawful information that is prohibited under any law in force at the time in relation to India's sovereignty and integrity.

V. Duty to retain: After cancellation of registration, an intermediary shall retain the information of users for a period of 180 (one hundred eighty) days.

VI. Duty of security: An intermediary shall take reasonable measures to ensure the security of its system by duly complying with rules and procedures enacted in this regard.

VII. Duty to assist: The intermediary shall provide assistance to the government agency lawfully authorized to investigate by providing information for the purposes of verification or any other reasons required by the authority in writing.

VIII. Duty to report: An intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team.

IX. Grievance mechanism: The intermediary shall have an appropriate mechanism for receipt in a timely manner and tracking of complaints.

The rules lay down additional due diligence that has to be observed by a significant social intermediary that has a user base above 50 lakhs.[9] Furthermore, intermediaries relating to news and current affairs content also have separate due diligence they have to follow.[10]

The scope and content available on OTT platforms are also covered by the Intermediary Rules, 2021. Uncensored content is available on OTT platforms without any mechanism for grievance redress or content censorship, which has drawn a lot of criticism. For OTT platforms, the Intermediary Rules have established a new grievance redress mechanism. The OTT platforms must now follow and adhere to the code of ethics outlined in the Intermediary Rules, and a three-tier structure consisting of the following will be established to ensure compliance and address grievances.

1. Internal Self-Regulating Mechanism: OTT platforms will create this mechanism to address any complaints about online curated content.
2. Self-Regulating Body: This is an independent body that will be led by a retired Supreme Court or High Court judge. The main responsibilities will be to monitor

[9] Rule 4, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

[10] Rule 5, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

compliance with the code of ethics, provide guidance to OTT platforms, and respond to grievances within a set time frame.

3. Oversight Mechanism: This mechanism will be developed by the Ministry of Information and Broadcasting (which is responsible for making policy decisions related to private and public broadcasting, cinema regulation and certification, and print media regulation). The main responsibilities will include publishing a self-regulatory body charter, developing a grievance portal for quick resolution of grievances, and forming an inter-departmental committee to hear grievances.

Major changes in the Rules over the erstwhile Information Technology (Intermediaries Guidelines) Rules, 2011

The following are some of the main changes in the Intermediary Rules, 2021 as they apply to intermediaries:

(a) Intermediary due diligence now includes:

- All intermediates must exercise due diligence [Rule 3].
- Additional Significant Social Media Intermediary due diligence requirements [Rule 4].
- Additional due diligence standards for other intermediaries, where relevant, as and when officially notified by the Central Government [Rule 6].

(b) Increased User Safety: Provision for direct requests for content takedown by affected individuals in specific cases of content relating to breach of bodily privacy, impersonation, or morphed imagery of the concerned individual in order to address the immediate need to prevent harm and emotional distress, particularly in instances of revenge porn and other similar cases [Rule 3(2)(b)].

(d) Revision in terms and conditions offered to users by the intermediaries:

- The terms and conditions have been clarified, simplified, and amended to address new issues.

(e) Clear timelines have been provided for:

- Grievance Resolution: 24 hours for acknowledgement/15 days for disposal [Rule 3(2)]

- The information must be removed from the platform within 36 hours of actual knowledge, based on a court order or a notice from the appropriate authority authorised by law [Rule 3(1)(d)].
- 72-hour time limit for providing information in response to a legal request [Rule 3(1)(j)].
- Retribution porn (sexual extortion/non-consensual porn publication/sexual act or behaviour including impersonation, etc.) and other comparable content: 24 hours [Rule 3(2)(b)].

Do the Rules affect the right to privacy of individuals?

In India, privacy is a fundamental right as observed in the landmark case of *Justice Puttaswami v. Union of India*[11]. The Rules place a strong emphasis on preserving individuals' online privacy. Several aspects of these Rules, as indicated in Part II, are concerned with the protection of privacy. The following are the provision of the Intermediary Rules, 2021 which places it in accordance with the fundamental right of privacy.

- Intermediaries must advise users that they should not share information that infringes on the privacy of another person, including bodily privacy [Rule 3(1)(b)].
- Intermediaries are expected to notify users on a regular basis that if their privacy policies are not followed, the intermediary has the authority to terminate access or block such information [Rule 3(1)(c)].
- If an individual comes across any platform content that depicts such person in full/partial nudity, in a sexual act, or through morphed images, such person may file a complaint with the relevant intermediary, who is then required to take all reasonable and practical measures to remove such content within 24 hours of receiving such complaint [Rule 3(2)(b)].

Yet, on the other hand, it can be said that certain rules of the Intermediary Rules, 2021 are incompatible with the fundamental right of privacy and, in fact, substantially harm it. Rule 4(2), in particular, significantly reduces end-to-end encryption, which has now become the privacy standard for mobile messaging networks. The rule provides that the intermediary on judicial order provide the competent authority as per the Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009 with identification of the first originator of the message for the prevention, detection,

[11] *Justice K.S. Puttaswami v. Union of India* (2017) 10 SCC 1

investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order. The scope of the purpose under which the authority may order the intermediary to identify the first originator of the message is wide in ambit. Hence, may come in conflict with the fundamental right of privacy if arbitrarily used.

It is important to note here that the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009 provide intermediaries with an extensive procedure and responsibility to be undertaken while dealing with intercepted or decrypted data.

Do the Rules affect the right to free speech and expression?

No, Article 19 of the Constitution provides the right to free speech and expression, and Article 19(2) establishes the appropriate limitations. These rights have been incorporated into the new Intermediary Rules for 2021. The Rules impose no additional requirements on users and do not impose any consequences on them. Furthermore, a rigorous grievance redressal process has been put in place to ensure that users whose content or access has been arbitrarily withdrawn can notify the intermediary for corrective action.

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

These rules contain the roles and responsibilities of the Indian Computer Emergency Response Team *(hereinafter referred to as "CERT")* which functions under the administrative control of the Department of Electronics and Information Technology, Ministry of Communications and Information Technology. It is entrusted with the following duties, namely:[12]

a. Collection, analysis, and dissemination of information on cyber incidents;
b. Forecast and alerts of cyber security incidents;
c. Emergency measures for handling cyber security incidents;
d. Coordination of cyber incidents response activities;
e. Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and

[12] Rule 9, The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

f. Such other functions relating to cyber security.

The CERT acts as a single point of contact for any incident that compromises the security of computer systems or jeopardizes data confidentiality. All cyber security incidents are to be reported to CERT within a reasonable amount of time after which an investigation or review shall be done for the resolution of the incident. CERT's level of assistance will vary depending on the type of incident, the affected entity, and the resources available to CERT.[13] However, CERT guarantees a prompt response to every incident reported. The following are the types of cyber security incidents that are to be reported to CERT:

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code links to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware
- Attacks on servers such as Database; Mail and DNS and network devices such as Routers
- Identity Theft spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on critical infrastructure, SCADA Systems and wireless networks
- Attacks on Applications such as E-governance, E-commerce, etc.

CONCLUSION

In recent years, with the rise and spread of new technology and technological developments, a rise in cyber-crimes also has been seen. Cybercrimes pose a significant risk to the human body and the business ecosystem as well. Thus, it has become pertinent that security measures against cybercrime be made an active component of a country's societal and economic safety aspects. To combat cybercrime, the Government of India amended the IT Act, 2000 and incorporated cyber-specific provisions. Cybercrime can be committed within or across the national boundaries via the internet, thus posing both, technical and legal challenges in investigating and prosecuting the crime.

IT Act and the rules enacted thereunder provide for a regulatory framework to govern and regulate entities involved in the activities of e-commerce and the processing of data. The

[13] Rule 12, The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

rules under the IT Act address varied aspects of the digital world from the security practices to the ethics that are to be followed by an Intermediary. The rules are also a result of the jurisprudence developed by the courts in India, for example, the Intermediary Rules, 2021 are aligned with the Supreme Court's order *In Re: Prajwala* for Significant Social Media Intermediary guideline.

With further developments in technology in form of cryptocurrency, blockchain, smart contracts, the IT Act and the rules thereunder will also have to evolve to accommodate the ever-growing and rapid changes in the world.

Our Offices

Gurugram

11th Floor, Emaar Tower-B, Digital Greens, Sector 61, Golf Course Extension Road, Gurugram, 122011.

Mumbai

1102, 11th Floor, Tower B, Peninsula Business Park, SB Road, Lower Parel, Mumbai, 400013

Bangalore

Q96. Chaithanya Smaran, Whitefield Hoskote Road, Kannamangala, Bangalore, 560067

Associate Offices

Silicon Valley

555 California Street, Suite #4925 San Francisco, CA 94104

Singapore

3, Phillip Street, #19-01, Royal Group Building, Singapore, 048693, Singapore

For more information reach out to us at contact@piercounsel.com

You may Download our firm profile here.