



## Defining “Cyber Crimes”

The term “cyber-crimes” is not defined in any statute or rulebook. The word “cyber” is slang for anything relating to computers, information technology, internet and virtual reality. Therefore, it stands to reason that “cyber-crimes” are offences relating to computers, information technology, internet and virtual reality.

One finds laws that penalise cyber-crimes in a number of statutes and even in regulations framed by various regulators. The Information Technology Act, 2000 (“IT Act”) and the Indian Penal Code, 1860 (“IPC”) penalise a number of cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other.

## Parallel Provisions in the IPC and IT Act

Many of the cyber-crimes penalised by the IPC and the IT Act have the same ingredients and even nomenclature. Here are a few examples:

**Hacking and Data Theft:** Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.

Section 378 of the IPC relating to “theft” of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words “movable property” are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both.

It may be argued that the word “corporeal” which means ‘physical’ or ‘material’ would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that “*whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description<sup>1</sup> for a term which may extend to 2 (two) years, or with fine, or with both.*” This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

Section 425 of the IPC deals with mischief and states that “*whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief*”. Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.

---

<sup>1</sup> Imprisonment of “either description” means simple imprisonment or rigorous imprisonment.

**Receipt of stolen property:** Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 (three) years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

**Identity theft and cheating by personation:** Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 66D of the IT Act prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 419 of the IPC also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to 3 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personation' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Section 468 of the IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine. Forgery has been defined in section 463 of the IPC to mean the making of a false document or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

In this context, reference may also be made to section 420 of the IPC that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 (seven) years, and shall also be liable to fine.

The only difference between the punishments prescribed under sections 66C and 66D of the IT Act and section 419 of the IPC is that there is no maximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that the imprisonment may extend to 7 (seven) years. Further, whilst the IT Act contemplates both the imposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offence could be punished with imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation to the offence of identity theft is that the latter requires the offence to be committed with the help of a computer resource.

**Obscenity:** Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac). The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac) and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lac).

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, *inter alia*, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 3 (three) months, or with fine, or with both.

## Cyber-crimes not provided for in the IPC

The following cyber-crimes penalised by the IT Act do not have an equivalent in the IPC.

**Section 43(h) of the IT Act:** Section 43(h) read with section 66 of the IT Act penalises an individual who charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network. A person who tampers with the computer system of an electricity supplier and causes his neighbour to pay for his electricity consumption would fall under the aforesaid section 43(h) of the IT Act for which there is no equivalent provision in the IPC.

**Section 65 of the IT Act:** Section 65 of the IT Act prescribes punishment for tampering with computer source documents and provides that any person who knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) 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 for up to 3 (three) years or with a fine which may extend to Rs. 3,00,000 (Rupees lac) or with both.

To a certain extent, section 409 of the IPC overlaps with section 65 of the IT Act. Section 409 of the IPC provides that any person who is in any manner entrusted with property, or with any dominion over property in his capacity as a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life or with imprisonment of either description for a term which may extend to 10 (ten) years, and shall also be liable to a fine. However, section 65

of the IT Act does not require that the person who tampers with or damages or destroys computer source documents should have been entrusted with such source code. Under section 409 of the IPC, criminal breach of trust should have been committed by someone to whom the property was entrusted.

**Violation of privacy:** Section 66E of the IT Act prescribes punishment for violation of privacy and provides that any person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.

There is no provision in the IPC that mirrors Section 66E of the IT Act, though sections 292 and 509 of the IPC do cover this offence partially.

Section 292 of the IPC has been discussed above. Section 509 of the IPC provides that if any person intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, such person shall be punished with simple imprisonment for a term which may extend to 1 (one) year, or with fine, or with both. Unlike section 66E of the IT Act which applies to victims of both genders, section 509 of the IPC applies only if the victim is a woman.

**Section 67C of the IT Act:** Section 67C of the IT Act requires an 'intermediary' to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. The section further provides that any intermediary who intentionally or knowingly contravenes this requirement shall be punished with imprisonment for a term which may extend to 3 (three) years and also be liable to a fine. An 'intermediary' with respect to any particular electronic record, has been defined in the IT Act to mean any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and 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. There is no corresponding provision in the IPC.

**Cyber terrorism:** Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect critical information infrastructure, is guilty of 'cyber terrorism'. Whoever knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, is also guilty of 'cyber terrorism'.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

There is no provision in the IPC that mirrors section 66F of the IT Act, though section 121 of the IPC (waging, or attempting to wage war, or abetting waging of war, against the Government of India) does cover this offence partially.

## Whether Compoundable, Cognizable and Bailable

Section 77A of the IT Act provides that, subject to certain exceptions, all offences under the IT Act for which the punishment is imprisonment for a term of 3 (three) years or less, are compoundable. The provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 (“CrPC”) shall apply with respect to such compounding.

Section 77B of the IT Act provides that notwithstanding anything contained in the CrPC, all offences punishable with imprisonment of 3 (three) years and above under the IT Act shall be cognizable and all offences punishable with imprisonment of 3 (three) years or less shall be bailable.

Most of the cyber-crimes covered under the IT Act are punishable with imprisonment of 3 (three) years or less. The cyber-crimes which are punishable with imprisonment of more than 3 (three) years are:

- (a) publishing or transmitting obscene material in electronic form under section 67 of the IT Act;
- (b) publishing or transmitting of material containing sexually explicit act, etc., in electronic form under section 67A of the IT Act;
- (c) publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form under section 67B of the IT Act; and
- (d) cyber terrorism under section 66F of the IT Act.

All of the cyber-crimes under the IPC are bailable other than offences under section 420 (*cheating and dishonestly inducing delivery of property*), section 468 (*forgery for the purpose of cheating*), section 411 (*dishonestly receiving stolen property*), section 378 (*theft*) and section 409 (*criminal breach of trust by public servant, or by banker, merchant or agent*), which are non-bailable.

Offences under sections 463 and 465 (*forgery*), sections 425 and 426 (*mischief*), section 468 (*forgery for the purpose of cheating*), section 469 (*forgery for the purpose of harming reputation*) and section 292 (*sale, etc., of obscene books, etc.*) of the IPC are non-compoundable offences while offences under sections 378 and 379 (*theft*), 420 (*cheating and dishonestly inducing delivery of property*), sections 425 and 426 (*mischief when the only loss or damage caused is loss or damage to a private person*), section 509 (*word, gesture or act intended to insult the modesty of a woman*), section 411 (*Dishonestly receiving stolen property*) and section 419 (*Punishment for cheating by personation*) of the IPC are compoundable offences. Of these, offences under sections 420 and 509 can be compounded only with the permission of the court. Most of the cyber crimes under the IPC are cognizable other than the offences under sections 425 and 426 (*mischief*) and sections 463 and 465 (*forgery*) which are non-cognizable.

The overlap between the provisions of the IPC and the IT Act may sometimes lead to an anomalous situation wherein certain offences are bailable under the IPC and not under the IT Act and vice versa and certain offences are compoundable under the IPC and not under the IT Act and vice versa. For instance, in case of hacking and data theft, offences under sections 43 and 66 of the IT Act that are bailable and compoundable while offences under section 378 of the IPC are non-bailable and offences under section 425 of the IPC are non-compoundable. Further, in case of the offence of receipt of stolen property, the offence under section 66B of the IT Act is bailable while the offence under section 411 of the IPC is non-bailable. Similarly, in case of the offence of identity theft and cheating by personation, the offences under sections 66C and 66D of the IT Act are compoundable and bailable while the offences under sections 463, 465 and 468 of the IPC are non-compoundable and the offences under sections 468 and 420 of the IPC are non-bailable.

Finally, in case of obscenity, the offences under sections 67, 67A and 67B of the IT Act are non-bailable while the offences under section 292 and 294 of the IPC are bailable. This issue has been dealt with by the Bombay High Court in the case of *Gagan Harsh Sharma v. The State of Maharashtra*<sup>2</sup> (discussed below) wherein offences under sections 408 and 420 of the IPC that are non-bailable and cannot be compounded other than with the permission of the court were in conflict with offences under sections 43, 65 and 66 of the IT Act that are bailable and compoundable.

## Conflict between the IPC and the IT Act: Case Law

In the case of *Sharat Babu Digumarti v. Government of NCT of Delhi*<sup>3</sup>, the conflict between provisions of the IPC and the IT Act came to the fore. In this case, on November 27, 2004, an obscene video had been listed for sale on baazee.com ("Bazee"). The listing was intentionally made under the category 'Books and Magazines' and sub-category 'ebooks' in order to avoid its detection by the filters installed by Baazee. A few copies were sold before the listing was deactivated. Later Delhi police's crime branch charge-sheeted Avinash Bajaj, Bazee's managing director and Sharat Digumarti, Bazee's manager. The company Bazee was not arraigned as an accused and this helped Avinash Bajaj get off the hook since it was held that, vicarious liability could not be fastened on Avinash Bajaj under either section 292 of the IPC or section 67 of the IT Act when Avinash's employer Bazee itself was not an accused. Later changes under section 67 of the IT Act and section 294 of IPC against Sharat Digumarti were also dropped, but the charges under section 292 of the IPC were retained. The Supreme Court then considered if, after the charges under section 67 of the IT Act was dropped, a charge under section 292 of the IPC could be sustained. The Supreme Court quashed the proceedings against Sarat Digumarti and ruled that if an offence involves an electronic record, the IT Act alone would apply since such was the legislative intent. It is a settled principle of interpretation that special laws would prevail over general laws and latter laws would prevail over prior legislation. Further, section 81 of the IT Act states that the provisions of the IT Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

In the case of *Gagan Harsh Sharma v. The State of Maharashtra*<sup>4</sup>, certain individuals were accused of theft of data and software from their employer and charged under sections 408 and 420 of the IPC and also under sections 43, 65 and 66 of the IT Act. All of these sections, other than section 408 of the IPC, have been discussed above. Section 408 of the IPC deals with criminal breach of trust by clerk or servant and states that "*whoever, being a clerk or servant or employed as a clerk or servant, and being in any manner entrusted in such capacity with property, or with any dominion over property, commits criminal breach of trust in respect of that property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine*".

Offences under sections 408 and 420 of the IPC are non-bailable and cannot be compounded other than with the permission of the court. Offences under sections 43, 65 and 66 of the IT Act are bailable and compoundable. Therefore, the petitioners pleaded that the charges against them under the IPC be dropped and the charges against them under the IT Act be investigated and pursued. It was further argued that if the Supreme Court's ruling in *Sharat Babu Digumarti* were to be followed, the petitioners could only be charged under the IT Act and not under the IPC, for offences arising out of the same actions.

The Bombay High Court upheld the contentions of the petitioners and ruled that the charges against them under the IPC be dropped.

---

<sup>2</sup> 2019 CriLJ 1398

<sup>3</sup> AIR 2017 SC150

<sup>4</sup> 2019 CriLJ 1398

## A Suitable Home for Cyber Offences

We currently have a situation where a number of offences are penalised by both the IPC and the IT Act, even though the ingredients of both offences are the same. There are subtle differences in punishments under these statutes, especially in aspects like whether the offence is bailable or compoundable or cognizable. An offence such as obscenity may take place through different types of media, both online or offline. However, it could result in unfairness if 2 (two) different statutes apply to the same offence on the basis of the media used.

The sum and substance of the Supreme Court's ruling in the *Sharat Babu Digumarti* case is that no individual may be charged under the IPC for an offence arising out of certain acts or omissions if the IT Act could also be applied to the same acts or omissions. Though we are in full agreement with the Supreme Court's ruling, it is our contention that all cyber offences ought to be housed in the IPC and not in the IT Act. The "cyber" component of an offence is not sufficient reason for differential treatment of sub-categories of the offence. Even though the supreme court's ruling in the *Sharat Babu Digumarti* case has ensured that no individual may be charged under the IPC for an offence arising out of certain acts or omissions if the IT Act could also be applied to the same acts or omissions, it is a fact that offences such as theft and obscenity will be punished differently if they involve a 'cyber' element. Currently, an individual who distributes a hard copy book containing obscene materials will be punished under the IPC whilst an individual who distributes obscene materials through the internet will be punished under the IT Act, though the underlying offence is the same. A person who steals a car will be punished under the IPC whilst an individual who indulges in theft of online data will be punished under the IT Act.

Theft is theft, irrespective of whether the stolen property is digital or physical. Obscenity transmitted through the internet should be treated at par with obscenity which is transmitted offline.

### IPC's treatment of stalking

The legislature's treatment of the offence of "stalking", accomplished through the insertion of new section 354D in the IPC through the Criminal Law (Amendment) Act, 2013<sup>5</sup>, is a case in point. Section 354D penalises the offence of "stalking" whether it has a cyber component or not. If a man follows a woman and contacts, or attempts to contact, such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, it amounts to stalking. If a man monitors the use by a woman of the internet, email or any other form of electronic communication, it will also result in the offence of stalking. There are a few exemptions to this offence of stalking, and all the defences apply irrespective of whether the stalking is cyber stalking or not. The punishment prescribed for stalking by Section 354D of the IPC does not discriminate on the basis of the presence or absence of the "cyber" component.

### Amendments to the IPC to cover cyber-crimes

The Indian legislature has from time to time, made a number of amendments to the IPC, to specifically cover cyber-crimes. Some of the important amendments are as follows:

- (a) a new section 29A was created to define "electronic record" by linking it with the definition given in the IT Act<sup>6</sup>;
- (b) a new sub-section (3) was inserted in section 4 of the IPC (relating to the extension of the IPC to extra territorial offences) that states that the provisions of the IPC shall be applicable to any person in any place "*without and beyond India*", committing an offence targeting a computer resource located in India<sup>7</sup>;

---

<sup>5</sup> Inserted by the Criminal Law (Amendment) Act, 2013 (Act No. 13 of 2013) with effect from February 2013.

<sup>6</sup> Inserted by Act 21 of 2000, section 91 Schedule I, (with effect from October 17, 2000).

<sup>7</sup> Vide the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) which came into effect from October 27, 2009.

- (c) in sections 118 and 119 of the IPC (that deal with the concealment of a design to commit an offence punishable with death or imprisonment for life and a public servant concealing a design to commit an offence which it is his duty to prevent, respectively), the words “*voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design*” were inserted before the words “*to commit such offence or makes any representation which he knows to be false respecting such design*”<sup>8</sup>;
- (d) in section 464 of the IPC (which penalises the making of a false document), the phrase “digital signature” was replaced with the phrase “electronic signature” in all places. The section was also amended to include the making of false electronic records and affixing electronic signatures under its ambit and the phrase “affixing electronic signature” was given the same meaning as it has under the IT Act<sup>9</sup>;
- (e) “electronic record” was included within the ambit of sections 164, 172, 173, 175, 192, 204, 463, 466, 468, 469, 470, 471, 474 and 476 of the IPC that earlier only provided for “documents”, “books”, “paper”, “writing” or “records”, as the case may be;
- (f) in section 466 of the IPC (which deals with forgery of court records or of public registers), the term “register” was defined to include any list, data or record of any entries maintained in an “electronic form”, as defined in section 2(1) (r) of the IT Act<sup>10</sup>; and
- (g) a new section 354D was inserted in the IPC that introduces the offence of cyber stalking, which has been discussed above.

#### Bad and ill-thought out drafting

Article 14 of the Constitution of India, 1950 (“Constitution”) states that the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India. It is not our contention that the current state of affairs results in a per se violation of Article 14 of the Constitution even though it has created an unhappy state of affairs. The legislature does have the freedom to make specific laws for specific matters or situations. However, the docking of cyber-crimes in the IT Act does not appear to have been well thought through.

When the IT Act was enacted, its focus was on putting in place technology law fundamentals like digital signatures, providing legal recognition for electronic documents and the like. Its preamble stated that its objective was to “*provide legal recognition for 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 filing of documents with the Government agencies 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 matters connected therewith or incidental thereto.*”<sup>11</sup>

Even though the IT Act penalised cyber-crimes with a broad brush through sections 43, 66 and 67, it was only in 2008 that the IT Act was amended<sup>12</sup> and provisions were made for specific cyber-crimes such as sending offensive messages through communication servers, dishonestly receiving a stolen computer resource or communication device, identity theft, violation of privacy, cyber terrorism etc. through sections 66A to 66F and sections 67A to 67C. These amendments stick out like an unwieldy appendage.

---

<sup>8</sup> Vide the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) which came into effect from October 27, 2009

<sup>9</sup> Vide the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) which came into effect from October 27, 2009

<sup>10</sup> Inserted by Act 21 of 2000, section 91 Schedule I, (with effect from October 17, 2000).

<sup>11</sup> <http://meity.gov.in/content/preliminary>

<sup>12</sup> Vide the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) which came into effect from October 27, 2009

Therefore, it is submitted that all cyber offences in the IT Act ought to be repealed and the IPC be suitably modified (to cover all of the cyber-crimes, including those currently covered under the IT Act) at the earliest possible convenience of the legislature.

*This paper has been written by Vinod Joseph (Partner) and Deeya Ray (Associate).*

*The paper was presented at the National Seminar on Cyber Crime and Cyber Warfare at Symbiosis Law School, Hyderabad on February 1, 2020. It has also been submitted for publication by Symbiosis Law School, Hyderabad.*

## **DISCLAIMER**

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

**You can send us your comments at:  
[argusknowledgecentre@argus-p.com](mailto:argusknowledgecentre@argus-p.com)**

Mumbai | Delhi | Bengaluru | Kolkata

[www.argus-p.com](http://www.argus-p.com)