

## Statics on Cyber Crimes and Cyber Laws in India: A Study

**Siddhartha Kaikini<sup>a</sup>, Kunal Agarwal<sup>b</sup>, Dr. Kiran Raj<sup>c</sup>, Dr. Sony Kulshrestha<sup>d\*</sup>**

a. LLM (Corporate & Commercial Law), SoL, Manipal University Jaipur

b. LLM (Corporate & Commercial Law), SoL, Manipal University Jaipur

c. Assistant Professor, School of Law, Manipal University Jaipur

d\*.Associate Professor, School of Law, Manipal University Jaipur,

[sonykulshrestha@gmail.com](mailto:sonykulshrestha@gmail.com) (Corresponding Author)\*

**Received:** 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10.

### **ABSTRACT**

In no legislation or regulation, the term “cybercrime” is defined. Anything having to do with computers, information technology, the internet, or virtual reality is referred to as “cyber”. As a consequence, “cyber-crimes” are now classified as crimes committed using computers, information technology, the internet, or virtual reality. The virtual environment of the internet is known as cyberspace, and the rules that govern it are known as cyber laws. Because they have a type of universal jurisdiction, these laws apply to all netizens of this area. “Cyber law is a discipline of law concerned with legal concerns that arise from the use of networked information technology. Cyber law, in a nutshell, rules computers and the internet. Cyber law is important because it touches almost all aspects of transactions and activities that occur on or involving the internet, the World Wide Web, and cyberspace. Every online activity and response has legal and cyber law consequences.” This paper will study the topic of cybercrime and cyber laws in India by analysing the statics of reported cyber- crime cases and by using major legislative provisions and case law.

**Keywords:** Internet, Cyber-crime, Computer, Hacking, Personal Data, Information.

### **INTRODUCTION**

“Cyber” is a prefix that denotes “someone, something, or an idea related to computers and the information age.” It is derived from the Greek word *kybernetes*, which means “steersman” or “governor,” and was first used in cybernetics, a term developed by Norbert Wiener and his associates.<sup>1</sup> The virtual environment of the internet is known as cyberspace, and the rules that govern it are known as cyber laws.<sup>1</sup>

There is a plethora of cybersecurity regulations that vary widely depending on the size of each country's territory. The severity of the sanctions varies based on

the nature of the offence, and may range from fines to imprisonment. “The first cyber legislation, the Computer Fraud and Abuse Act of 1986, was enacted. It prohibits both unauthorised access to computers and the abuse of digital information.”<sup>2</sup>

Cybercrime has evolved in lockstep with the internet's expansion. Identity theft, crypto jacking, child pornography, and cyber terrorism are all prevalent topics in today's headlines. Computers are used as either a tool or a target, or both, in cybercrime to carry out criminal operations.

Cybercrime is not defined under the Information Technology Act of 2000, the Information Technology Amendment Act of 2008, or any other Indian statute. That can't possibly be the case. The Indian Penal Code of 1860, as well as a number of other legislation, have expanded on offences and crimes, laying out particular actions and their penalties. As a consequence, cyber-crime might be defined as a mix of crime and technology. "Any transgression or crime involving the use of a computer is a cyber-crime," to put it another way. Even a simple crime such as stealing or pickpocketing might be classified as cyber-crime if the fundamental data or aid to the crime is a computer or information recorded on a computer utilised (or abused) by the fraudster.<sup>3</sup>

"Ransomware assaults, email and internet fraud, identity theft, and frauds involving bank accounts, credit cards, or any other form of payment card are all examples of profit-driven criminal acts that may be carried out as a consequence of cyber-crime. Theft and resale of personal and commercial data may be of interest to cybercriminals.

In India, cybercrime is covered under both the Information Technology Act of 2000 and the Indian Penal Code of 1860. Cybercrime and internet trade are addressed under the Information Technology Act of 2000. However, in 2008, the Act was updated to include a definition and penalty for cybercrime." The Indian Penal Code 1860 and the Reserve Bank of India Act were also amended.<sup>4</sup>

### **SIGNIFICANCE OF THE CYBER LAWS**

In today's technologically advanced culture, the globe is growing more digitally sophisticated, and so are the crimes. The Internet was established as a tool for research and information distribution, and it was initially unsupervised. "It became increasingly transactional over time with e-business, e-commerce, e-governance, and e-procurement. All legal concerns pertaining to digital crime are covered under cyber laws." The need for cyber laws and their execution develops in tandem with the number of individuals who use the internet.

"Cyber law affects practically everyone in today's highly digitalized environment. For example-<sup>5</sup>

- Almost all share transactions are done through a demat account.
- Almost all businesses rely heavily on their computer networks and store sensitive information in electronic form.
- Electronically filed government forms, such as income tax returns and company law forms, are becoming the norm.
- Credit cards are becoming more popular among shoppers.
- The majority of people communicate using email, cell phones, and SMS messages.
- Even in non-cyber-crime instances, such as divorce, murder, abduction, tax evasion, organised crime, terrorist operations, counterfeit currency, and so on, vital evidence is located in computers / cell phones.
- Online banking frauds, online stock trading frauds, source code theft, credit card fraud, tax evasion, virus assaults, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking,

pornography, and other cyber-crime instances are becoming more widespread.

- Digital signatures and e-contracts are quickly displacing traditional commercial techniques.”

#### **NCRB FIGURES ON CYBER CRIME**

According to official figures released on September 15, India registered 50,035 incidences of cybercrime in 2020, an increase of 11.8 percent over the previous year, and 578 incidents of “fake news on social media.”<sup>6</sup>

“According to statistics from the National Crime Records Bureau (NCRB), the country's rate of cybercrime (incidents per lakh people) increased from 3.3 percent in 2019 to 3.7 percent in 2020.

According to statistics from previous years, the Kingdom had 44,735 instances of cyber-crime in 2019, up from 27,248 in 2018.<sup>7</sup>

According to NCRB data, 4,047 incidences of internet banking fraud, 1,093 OTP frauds, and 1,194 credit/debit card fraud were recorded in 2020, while 2,160 cases of ATM fraud were reported.<sup>8</sup>

It also reported that there were 578 cases of false news on social media, 972 cases of cyber stalking or bullying of women and children, 149 cases of fraudulent profiles, and 98 cases of data theft.<sup>9</sup>

In terms of motivation, the NCRB, which is part of the Ministry of Home Affairs, claimed that fraud accounted for 60.2 percent of all cyber-crimes in 2020 (30,142 out of 50,035 instances).<sup>10</sup>

According to the data, sexual exploitation accounted for 6.6 percent (3,293 events) and extortion accounted for 4.9 percent (2,440 instances).<sup>11</sup>

According to the data, Uttar Pradesh has the highest cyber-crime instances with 11,097, followed by Karnataka (10,741), Maharashtra (5,496), Telangana (5,024), and Assam (3,530).<sup>12</sup>

According to the survey, Karnataka had the highest crime rate at 16.2 percent, followed by Telangana (13.4 percent), Assam (10.1 percent), Uttar Pradesh (4.8 percent), and Maharashtra (4.4 percent).<sup>13</sup> According to the NCRB, which is responsible for collecting and analysing crime data as mandated by the Indian Penal Code and special and local laws in the country, the national capital Delhi reported 168 such incidents throughout the year, with a crime rate of 0.8 percent.”<sup>14</sup>

#### **TYPES OF CYBER CRIME**

**Child pornography or child sexually abusive material (CSAM):** In its most basic form, kid sexual abuse materials (CSAMs) are any material that contains sexual imagery in any form, with both the exploited and abused child visible. “The publication or transfer of material depicting children in sexually explicit acts in an electronic form is criminal, according to Section 67(B) of the Information Technology Act.”<sup>15</sup>

**Cyber bullying:** A cyberbully is someone who uses electronic devices such as computers, cell phones, and laptops to harass or bully others. Bullying that takes place through the use of digital technology is referred to as cyberbullying. There may be a role for social media, messaging systems, gaming platforms, and mobile devices. Frequently, this entails a pattern of behaviour designed to frighten, enrage,

or disgrace individuals who are being targeted.

**Cyber stalking:** It is the act of harassing or stalking another person over the internet or through other technological means. Cyberstalking takes many forms, including texts, emails, social media posts, and other types of communication, and it is frequently relentless, methodical, and planned.<sup>16</sup>

**Online job fraud:** It entails deceiving people who are looking for work by offering them a better job with higher pay while also giving them false hope. The Reserve Bank of India (RBI) issued a warning on March 21, 2022, advising citizens not to fall for job scams. The RBI has described how online job fraud is committed, as well as the measures that the average person should take while applying for any job opportunity, whether in India or abroad.

**Phishing:** Phishing fraud occurs when a user receives an email that appears to be from a legitimate source but contains a malicious attachment designed to steal personal information from the user, such as their ID, IPIN, Card number, expiration date, CVV, and other information, and then sell it on the dark web.

**Vishing:** Vishing is a method of stealing private information from victims by utilising their phones. Cybercriminals employ sophisticated social engineering techniques to persuade victims to reveal personal information and log into accounts. Vishing, like phishing and smishing, successfully deceives victims

into thinking they are being kind by answering the phone.<sup>17</sup>

**Smishing:** As the name implies, smishing is a type of fraud that involves sending text messages to victims in order to deceive them into dialling a phoney phone number, accessing a fraudulent website, or downloading harmful software onto their computers.”<sup>18</sup>

**Credit card (or debit card) fraud:** It entails making unlawful transactions or withdrawals from another person's card in order to obtain access to their funds. Credit/debit card fraud occurs when illegal purchases or cash withdrawals are made from a customer's account. When a criminal obtains access to a cardholder's debit/credit card number or personal identification number, fraud occurs (PIN). Untrustworthy personnel or hackers may gain access to your personal information.<sup>19</sup>

#### **HISTORY OF CYBER LAW IN INDIA**

“The Information Technology Act is the consequence of a United Nations General Assembly decision enacted on January 30, 1997, which approved the Model Law on Electronic Commerce on International Trade Law. This resolution urged, among other things, that all states carefully evaluate the stated Model Law when modifying or adopting new legislation, so that consistency in the laws of the many cyber-nations controlling alternatives to paper-based communication and information storage may be respected.”<sup>20</sup>

The Department of Electronics (DoE) drafted the law in July 1998. However, when the new Ministry of Information Technology was constituted on December

16, 1999 (after a nearly one-and-a-half-year delay), it could only be tabled in the House on that day. The Commerce Ministry provided suggestions on e-commerce and topics pertaining to World Trade Organization (WTO) tariffs, which was a major move. The Ministry of Law and Company Affairs then reviewed the combined plan.<sup>21</sup>

After being presented in the House, the measure was sent to the 42-member Parliamentary Standing Committee on Members' Demands. Only suggestions that have received Ministry of Information Technology approval were considered. One possibility that was highly debated was for a cyber café owner to retain a registration of all visitors' names and addresses, as well as a list of the websites they viewed. Simultaneously, it was derided since it would invade a net surfer's privacy and be unprofitable. Finally, in the final draft, the IT Ministry abandoned this suggestion.<sup>22</sup>

The bill was agreed by the Union Cabinet on May 13, 2000, and the Information Technology Bill was enacted by both houses of the Indian Parliament on May 17, 2000. On June 9, 2000, President Clinton signed the measure, which became known as the Information Technology Act of 2000. On October 17, 2000, the Act goes into force.

With the growth of technology and the rise of new ways to conduct crime using the Internet and computers, the necessity to amend the IT Act, 2000 emerged in order to incorporate new forms of cyber offences and fix other loopholes that inhibited the IT Act's effective implementation. As a consequence, on October 27, 2009, the Information Technology (Amendment)

Act, 2008 was approved and became effective." The IT (Amendment) Act of 2008 made major changes to the IT Act of 2000 on a number of fronts.<sup>23</sup>

#### **PARALLEL PROVISIONS IN THE IT ACT AND IPC FOR CYBER CRIME**

Many of the cyber-crimes that are punishable under the IPC and the IT Act have similar elements and even names. Listed below are a few examples:

**Hacking and Data Theft:** "Hacking into a computer network, stealing data from a computer, introducing and spreading viruses through computer networks, damaging computers, computer networks, or computer programmes, disrupting any computer, computer system, or computer network, denying an authorised person access to a computer or computer network, and so on are all prohibited under Sections 43 and 66 of the IT Act. For the aforementioned offences, the maximum punishment is either 3 (three) years in jail or a fine of Rs. 5,00,000 (Rupees five lac), or both."<sup>24</sup>

Section 378 of the IPC, which deals with theft of movable property, will apply to the theft of any data, online or otherwise, because 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 attached to the earth." The maximum punishment for stealing is three years in jail, a fine, or both under section 378 of the IPC.

It could be claimed that the term "corporeal," which meaning "physical" or "material," excludes digital assets from the

scope of the IPC's section 378. The counter-argument is that the drafters intended to protect all types of property, excluding land and anything permanently fastened to anything attached to the soil.<sup>25</sup>

“Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or 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 for a term which may extend to two years, or with fine, or with both,” according to Section 424 of the IPC.

“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,” according to Section 425 of the IPC. “Damage to computer systems, as well as blocking access to a computer system, will come under the aforementioned section 425 of the IPC.” The maximum penalty for mischief under section 426 of the IPC is 3 (three) months in jail, a fine, or both.<sup>27</sup>

**Receiving stolen property:** “Dishonestly obtaining any stolen computer resource or communication equipment is penalised under Section 66B of the IT Act. According to this rule, the person who receives stolen goods must have done so dishonestly or had grounds to suspect it was stolen property. This crime is punished under Section 66B of the IT Act by imprisonment for up to three (three)

years or a fine of up to Rs. 1,00,000 (Rupees one lac), or both.

Dishonestly taking stolen goods is also punishable under section 411 of the IPC, which is virtually comparable to section 66B of the IT Act. Section 411 of the IPC carries a punishment of either imprisonment of any kind for up to 3 (three) years, a fine, or both. The IPC does not have a maximum fine limit, which is the fundamental difference between the proposed punishments.

Under Section 66C of the IT Act, anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other unique identification feature shall be punished with imprisonment of either description for a term that may extend to 3 (three) years, as well as a fine of up to Rs. 1,00,000. (Rupees one lac).<sup>28</sup>

“Any person who cheats by personation by using any communication device or computer resource,” according to Section 66D of the IT Act, “shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to a fine which may extend to Rs. 1,00,000.” (One lakh rupees).

“Section 419 of the IPC also specifies a punishment for 'cheating by personation,' saying that anybody who cheats by personation faces either imprisonment of any kind for a period of up to three years, a fine, or both. If a person cheats by pretending to be someone else, willfully substituting one person for another, or portraying oneself or herself as someone other than who he or she is, it is dubbed 'cheating by personation.

Sections 463, 465, and 468 of the Indian Penal Code, which deal with forgery and “forgery for the purpose of defrauding,” may also apply in cases of identity theft. Forgery with the intent to deceive is criminal under Section 468 of the Indian Penal Code, which carries a punishment of up to 7 (seven) years in jail and a fine. Forgery is defined in section 463 of the IPC as the creation 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 the intent to commit fraud or the possibility of fraud.<sup>28</sup>

In this case, section 420 of the IPC states that anyone who cheats and thus dishonestly induces the person deceived to deliver any property to anyone, or to make, alter, or destroy the whole or any part of a valuable security, or anything signed or sealed and capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term that may extend to 7 (seven) years.

The key distinction between the penalties imposed under sections 66C and 66D of the IT Act and those imposed under section 419 of the IPC is that the latter does not have a maximum monetary limit. The punishment under section 468, on the other hand, is even more severe, with a maximum term of 7 (seven) years in prison. Furthermore, the IPC uses the term 'or' to imply that the crime may be punished by either imprisonment or a fine, while the IT Act allows for both. In respect to the crime of identity theft, the most significant difference between the IPC and the IT Act is that the latter requires the

offence to be performed using a computer resource”.<sup>29</sup>

**Obscenity:** “Publishing or sending obscene content, material containing sexually explicit actions, and material portraying minors in sexually explicit acts in electronic form are all punishable under sections 67, 67A, and 67B of the IT Act, respectively. On the first conviction for an offence under section 67 of the IT Act, the punishment is imprisonment of either description for a term up to 3 (three) years, with a fine of up to Rs. 5,00,000 (Rupees five lac), and on the second or subsequent convictions, the punishment is imprisonment of either description for a term up to 5 (five) years, with a fine of up to Rs. 10,00,000 (Rupees ten lac) (Rupees ten lac). On the first conviction, imprisonment of either description for a term of up to 5 (five) years, with a fine of up to Rs. 10,00,000 (Rupees ten lac) (Rupees ten lac), and on the second or subsequent convictions, imprisonment of either description for a term of up to 7 (seven) years, with a fine of up to Rs. 10,00,000 (Rupees ten lac) (Rupees ten lac).

According to Section 292 of the Indian Penal Code, anyone who sells, distributes, publicly exhibits, or in any other way puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure, or any other obscene object shall be punished on a first conviction with imprisonment of either description for a term up to 2 (two) years, and a fine of up to Rs. 2,000 (Rupees two thousand) rupees.

Anyone who does any obscene act in a public place, or sings, recites, or utters any obscene song, ballad, or words in or near a public place, to the annoyance of others, shall be punished with imprisonment of either description for a term that may extend to 3 (three) months, or with fine, or both, according to Section 294 of the IPC.”<sup>30</sup>

#### **CONFLICT BETWEEN IPC AND IT ACT: CASE LAW**

In the case of Sharat Babu Digumarti v. Government of NCT of Delhi, the disparity between the IPC and the IT Act was underlined. “On November 27, 2004, an obscene video was offered for sale on baazee.com (‘Bazee’). The listing was put in the category ‘Books and Magazines’ and the sub-category ‘eBooks’ to avoid detection by Baazee’s filters. A few copies were sold before the listing was removed. The crime section of Delhi police eventually accused Avinash Bajaj, Bazee’s managing director, and Sharat Digumarti, Bazee’s manager. The court concluded that since Avinash Bajaj’s employer, Bazee, was not identified as a defendant, vicarious responsibility could not be imposed on him under either section 292 of the IPC or section 67 of the IT Act. The accusations against Sharat Digumarti under section 67 of the IT Act and section 294 of the IPC were later dropped, however the charges under section 292 of the IPC were upheld. After the charges under section 67 of the IT Act were dismissed, the Supreme Court considered whether a prosecution under section 292 of the IPC may be maintained. Special laws take priority over general laws, and subsequent laws take precedence over earlier legislation, according to a

well-established rule of interpretation. Furthermore, section 81 of the IT Act states that the IT Act’s provisions shall apply despite anything in any other legislation now in effect that is inconsistent with them.”<sup>31</sup>

In Gagan Harsh Sharma v. The State of Maharashtra, some individuals were accused of stealing data and software from their employer and were prosecuted under sections 408 and 420 of the IPC, as well as sections 43, 65, and 66 of the IT Act. All of these provisions have previously been examined, with the exception of section 408 of the IPC.

Only with the court’s permission may non-bailable offences under sections 408 and 420 of the IPC be compounded. The IT Act’s sections 43, 65, and 66 provide for bail and the compounding of offences. As a consequence, the petitioners asked for the IPC charges against them to be dropped and the IT Act allegations against them to be examined and prosecuted.” It was further argued that if the Supreme Court’s decision in Sharat Babu Digumarti was adopted, the petitioners could only be tried for the same conduct under the IT Act, not the IPC.

The petitioners’ arguments were supported by the Bombay High Court, which ordered the IPC charges against them to be quashed.

#### **CONCLUSION AND SUGGESTIONS**

As technology advances, frightening things are developing on the dark web. The Internet has evolved into a tool for evil activities, which intelligent individuals exploit for wicked intentions and occasionally financial benefit. As a result,

cyber laws are relevant at this time and are necessary for all citizens.

With the rising dependency of humans on technology in India and around the world, cyber laws must be constantly updated and refined to keep up. "As a result of the epidemic, there has been a considerable growth in the number of remote employees, which has raised the demand for application security. Legislators must take extra precautions to stay ahead of imposters so that they can take action against them as soon as they appear." If legislators, internet providers, banks, shopping websites, and other intercessors act together, it can be avoided.

## REFERENCES

1. Taxguru, *Overview of Cyber Laws in India*, Taxguru, <https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf>.
2. Rachit Garg, *Cyber Crime Laws in India*, I Pleadings (Apr. 28, 2022) <https://blog.ipleaders.in/cyber-crime-laws-in-india/#:~:text=The%20theft%20and%20re,sale%20of,cyber%20crimes%20and%20el,ectronic%20commerce>
3. Cyber Laws in India, Latest Laws, <https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf>.
4. *Supra* Note 1.
5. PTI, *India reported 11.8% rise in cyber-crime in 2020; 578 incidents of 'fake news on social media': Data*, The Hindu (Sept. 15 2021) <https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece>
6. Latest Report published by the NCRB <https://ncrb.gov.in/en/Crime-in-India-2020>.
7. PTI, *India reports 11.8% jumps in cyber-crime in 2020: NCRB data*, Bus. Today (Sept. 16, 2021) <https://www.businesstoday.in/latest/economy/story/india-reports-118-jumps-in-cyber-crime-in-2020-ncrb-data-306890-2021-09-16>
8. Chetan Chauhan, *Cyber-crimes registered 11.8% increase last year: NCRB*, Hindustan Times (Sept. 16, 2021) <https://www.hindustantimes.com/india-news/cyber-crimes-registered-11-8-increase-last-year-ncrb-101631731021285.html>.
9. India Spend, *India registered 136 Cyber-crime cases every day in 2020: NCRB data*, Bus. Standard (Feb. 21, 2022) [https://www.business-standard.com/article/current-affairs/india-registered-136-cybercrime-cases-every-day-in-2020-ncrb-data-122022100007\\_1.html](https://www.business-standard.com/article/current-affairs/india-registered-136-cybercrime-cases-every-day-in-2020-ncrb-data-122022100007_1.html).
10. *Supra* note 5.
11. *Supra* note 2.
12. *Supra* note 1.
13. Rohas Nagpal, *Introduction to Indian Cyber Law*, Asian School of Cyber Laws <http://osou.ac.in/eresources/introduction-to-indian-cyber-law.pdf>.
14. *History of Cyber Law in India*, Indian Cyber Security [http://www.indiancybersecurity.com/cyber\\_law\\_history\\_india.php](http://www.indiancybersecurity.com/cyber_law_history_india.php).
15. The Information Technology (Guidelines for Cyber Cafe) Rules, 2011. *Supra* note 13.
16. Matthew A. Machnitosh, *A Brief history and Development of Cyber Law*, Brewminate (Nov. 11, 2021)

17. Information Technology Act, No. 21 of 2000, §43 (Ind.).
18. Indian Penal Code, No. 45 of 1860, §22 (Ind.).
19. Indian Penal Code, No. 45 of 1860, §378 (Ind.).
20. Vinod Joseph, *Cyber Crimes in the IPC and IT Act: An Uneasy Co-existence*, Argus Partners (Feb. 6, 2020) [https://www.argus-p.com/papers-publications/thought-paper/cyber-crimes-in-the-ipc-and-it-act-an-uneasy-co-existence/?utm\\_source=Mondaq&utm\\_medium=syndication&utm\\_campaign=Linkedin-integration](https://www.argus-p.com/papers-publications/thought-paper/cyber-crimes-in-the-ipc-and-it-act-an-uneasy-co-existence/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=Linkedin-integration).
21. Indian Penal Code, No. 45 of 1860, §424 (Ind.).
22. Indian Penal Code, No. 45 of 1860, §425 (Ind.).
23. Indian Penal Code, No. 45 of 1860, §426 (Ind.).
24. Information Technology Act, No. 21 of 2000, §66(b) (Ind.).
25. Indian Penal Code, No. 45 of 1860, §411 (Ind.).
26. Information Technology Act, No. 21 of 2000, §66(c) (Ind.).
27. Information Technology Act, No. 21 of 2000, §66(d) (Ind.).
28. Indian Penal Code, No. 45 of 1860, §419 (Ind.).
29. Indian Penal Code, No. 45 of 1860, §420 (Ind.).
30. *Id.*