IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

Cyber Crime - The Judicial Endeavors

Sandhya Rajawat
Prestige Institute of Management and Research, Indore, Madhya Pradesh, India

Abstract: *Cyber-crime primarily entails the use of the internet and computers to extract the private information of an individual, either directly or indirectly, and then disclose it on online platforms without the individual's consent or illegally, with the intent of degrading the reputation or causing mental or physical harm. With the development of technology, a sharp increase in cybercrimes has been observed. Internet-based offenses against women have increased along with women's increasing reliance on cyberspace. This is primarily due to the fact that more than half of online users are unaware of how online platforms operate, are oblivious of technological advancements, and have inadequate training and education. In order to safeguard women and children who are harassed and exploited for voyeuristic pleasures, cybercrime has become a formidable obstacle for the law enforcement agencies of various nations. Typically, cyberstalking, cyberpornography, impersonation, etc., target women. India is one of the few countries that has enacted the IT Act 2000 to deal with cyber-crime issues in order to protect women from exploitation by vicious predators. However, this act does not address some of the gravest threats to women's safety, and issues involving women are still growing exponentially.*

Keywords: Cyber-crime, women, IT Act, technology, online platforms, landmark Judgments

I. INTRODUCTION

For law enforcement agencies, the abundance of cybercrime cases in India has created new obstacles. The advancement of information technology has elevated sincere people beyond their financial capacity. It makes sense to suggest that each coin has a unique side. The rapidly emerging, modern, technologically advanced town offers both innumerable benefits and downsides.

The criminal justice system in India underwent growth over a period of more than 150 years and has earned recognition as one of the most effective legal systems in the world. The Parliament (administrators), the police (law masters), the investigators, the legal advisers, and the appointed authorities are among the key institutions concerned with the organization of criminal equity. While they value the many opportunities for use, the fact that their work is based on governing principles prevents them from encroaching on one another's territory and requires them to act in unison.

II. ISSUES FACED BY JUDICIARY

Since most of our activities, including trade, business, banking, currency exchange, data correspondence, legislative and non-administrative authority exchanges, scholarly pursuits, and so forth, take place online, online culture has grown to be an integral part of modern existence. According to current thinking, everybody can get whatever they need to know or see online. However, despite this more positive aspect of PC technology, there are undoubtedly some negative aspects that legitimately worry both legal functionaries and law-requirement agencies. The use of PC networks for illegal purposes has given rise to a number of online debates, comparisons, conversations, and other things thanks to the web culture that followed. Although debates relating to online exchanges are completely unique in their temperament, degree, and treatment, the goal of these digital-related questions has emerged as a true test for the official courtrooms due to the complexities associated with them, with which they are associated, questions as such are not new to human culture as they are known to have existed since the beginning of human civilization[1].

[1] Leon Radzinovicz , *The Growth of Crime*, 202 (Hamish Hamilton, 1977)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

The following factors prevent judicial condemnation in situations of cybercrime:

• The global nature of these crimes is so great that they are unaware of geographical or regional boundaries; Differences in the general sets of laws, laws, and methods of various nations with regard to the acceptability of digital-related cases; and o Uncertainty regarding the precise definition of cybercrime and activities that can be included within its ambit.

Due to its immaterial nature, cybercrime is not dependent on actual violence or the presence of victims where the crime was committed. Under these circumstances, the traditional adversarial arrangement of suit would hardly satisfy the requirements of equity in situations involving cybercrime.

In ***State of Punjab and Others v. M/s Amritsar Beverages Ltd. and Others,***[2] the Supreme Court of India made observations about the problems considered by the legal executive and the requirements organizations in addressing PC-related offences.

"Web and other data advances have brought with them problems that the law did not foresee. Additionally, it didn't consider the difficulties that might be encountered by officials who might lack scientific aptitude or sufficient knowledge to deal with the novel situation. Different new developments led to various unexpected violations, which quickly attracted the attention of our legislature. Although the Data Technology Act of 2000 was modified to include various cybercrimes and the appropriate punishments, it still doesn't cover all the issues that the Act's implementers are looking at.

III. SENTENCING BY THE COURT

The factors that affect legal sentencing generally in the Indian context, according to a cursory examination of the legal system, include the offender's age, sex, educational background, mental state, and stage of development. His reasoning, the circumstances in which the offense is committed, and its effects on the offender or the public all have a bearing on whether the denounced should be condemned. Young age, adolescence, and a prior clean record for the offender are typically excellent reasons for leniency in sentencing, but recidivism, an ongoing affiliation with hoodlums or the criminal underworld, as well as the seriousness or actuality of the crime, call for harsh punishment. However, they are only conjectures that in no way restrain judicial vigilance in denouncing the criminals. The Judges can hardly bear to ignore the entire impact of crime on society when they evaluate the discipline. In light of this, the court's decision assumes a crucial role in selecting a future strategy in comparable situations.

Despite the fact that there is undoubtedly less case law on cybercrime than there is for traditional crimes, this is changing as personal computers become more popular among people. The courts frequently have a tendency to view online criminals who commit planned crimes as expected risks to society, and as a result, they are reluctant to reduce the sentences of such guilty people.

expressing his views on judicial punishment According to Leon Radzinovicz[3], although it may be justified to impose a severe and unusually long term due to the severity of the crime or a reduced sentence in exchange for the guilty party's rehabilitation, a sentence that is too severe relative to the offense is objectionable.4 The general trend is to provide a strong discipline because cybercrimes are so detrimental. The main question in relation to cybercrime is whether the power in sentencing should come from society's security or the fight against crime. Whatever the case, the overall trend is by all accounts for anticipating and controlling cybercrime by adopting a harsh perspective in condemning digital wrongdoers, barring any specific measures in this regard. The case-law referred to in the pages that follow reflects the response of the legal system and how it dealt with digital issues by providing medical relief to those who had suffered such violations.

[2] AIR 2006 SC 2820.

[3] Leon Radzinovicz , *The Growth of Crime*, 202 (Hamish Hamilton, 1977)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

IV. INDIAN JUDICIAL TENDENCY

It should be noted that, until the Information Technology Act, 2000 was formed and enacted on October 17, 2000, there was almost no Indian case law on the subject of the legal authority of digital technology. The development of data innovation as a speedier and quicker way of communication in the new millennium has produced some unanticipated effects, resulting in cybercrimes being brought before the courts for mediation.

The problem of the court's jurisdiction was raised in the case of ***P.R. Transport Agency v. Union of India and others***[4]since the agreement between the parties living in better areas was reached via email. The offended party's (P.R. Transport organization) bid for 40000 metric tons loads of coal from Dobari colliery was accepted as part of an e-closeout for coal held by Bharat Cooking Coal Ltd. (BCCL) in response to this circumstance. On July 19, 2005, the BCCL forwarded the bid acknowledgment via email. As a result, the offended party wrote a check in the amount of 81.12 lakhs to BCCL, which accepted it and paid it but failed to deliver the coal to the offended party. Overall, it (BCCL) informed the offended party via email contact that the aforementioned e-closeout stands were canceled "for some specific and unavoidable reasons".

The offended party discovered that BCCL had withdrawn the e-closeout of the coal offer because another person had made a greater offer that had not previously been taken into account due to a flaw in the PC or its software or information handling procedures. The injured party (P.R. Transport) challenged the respondent's right to revoke their agreement before the High Court of Allahabad. The respondent (BCCL) objected to the court's regional ward on the grounds that the High Court of Allahabad did not have jurisdiction over the matter because it had not yet materialized in the province of Uttar Pradesh. The injured parties, on their part, argued that the matter fell within the jurisdiction of the Court because they received the email confirming receipt of the letter in Chandauli, Uttar Pradesh.

After hearing both sides, the High Court concluded that in the event of an email acknowledgment, the information sent from anywhere by the record holder goes to the memory of the "worker," which may be found anywhere and can be retrieved by the recipient account holder from anywhere in the world. Therefore, neither the point at which email is transmitted nor received is fixed. In accordance with Section 13(3) of the Information Technology Act of 2000, an electronic report is deemed to have been received at the recipient's place of business. The offended party (P.R. Transport) will regard the delicate to have been received in the location where it conducts business, for instance. The Allahabad High Court then had the option of choosing Varanasi or Chandauli, both in the state of Uttar Pradesh. Based on the circumstances, it could be assumed that the legal framework regarding the use of jurisdiction by courts in cybercrimes should conform to the standards of reasonable play and equity, which consistently depend upon the following considerations: a. The degree of intentional disruption or criminal operations influencing State's undertakings;

1. The degree of conflict with the State's influence;
2. The gathering of the State's advantage in arbitration of the question;
3.The legislation mandates that in order to assist the State's ward online, the site must be open as well as engage in communication with the subject in some way.

V. IMPORTANT DECISIONS

One such case is **SHREYA SINGHAL V. UOI,**[5]

Contextual Information

Two ladies were detained under Section 66A of the IT Act for allegedly making offensive Facebook posts about the city of Mumbai being shut down after the death of a political leader. Whoever, by the use of a computer resource or communication, transmits information that is offensive, false, or which causes discomfort, danger, irritation, insult, hostility, hurt, or ill will is punishable by imprisonment under Section 66A of the IT Act. The ladies claimed that Section 66A of the IT Act violated their right to free expression, so they filed a petition to have the provision struck down. Issue The Supreme Court heard arguments on whether or not Section 66A of the IT Act is constitutional.

[4]AIR 2006 All 2.
[5]AIR 2015 SC 1523.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

Decision

While rendering its verdict, the court elaborated on three ideas: discourse, advocacy, and incitement. Freedom of expression, according to the court, includes the ability to debate or advocate for any topic, regardless of how controversial it may be. The court ruled that Section 66A violates the right to free expression since it is unclear and includes harmless speech within its scope. It protected people' basic right to free expression in India and deleted an arbitrary clause from the IT Act, 2000. It reasoned that the Indian Penal Code, 1860 provisions prohibiting racist speech, any speech that outrages the modesty of a woman, or speech aimed at promoting enmity, abusive language, criminal intimidation, racism, etc. would still apply even if section 66A were to be struck down.

Mr. Rajendra Prasad Yadav and M/s Gujarat Petrosynthese Ltd v. The Union of India[6]

Contextual Information

Petitioners requested that Respondent appoint a Chairperson to the Cyber Appellate Tribunal (CAT) in order to guarantee the timely convening of CAT hearings. It was said in court documents that the agency will do whatever was required to fill the position. Every attempt shall be made to nominate a chairman within six months. It was also argued that the chairman should be selected before the deadline passed in the public interest. Issue If the Cyber Appellate Tribunal (CAT) is going to hold its hearings on a regular basis, as requested by the petitioners, this Court must issue a writ of mandamus requiring the respondent to designate a Chairperson to the CAT.

Decision

No more explanation is required. After more than two years, however, the respondent is required to act swiftly to fill the position of CAT Chairperson in accordance with Section 53 of the Information Technology Act, 2000. With these notations and this no-cost ruling, I must dismiss the petition.

Shamsher Singh Verma v. State of Haryana SCC Opinion[7]

Contextual Information

After the HC denied the defendant's request to present the CD he had submitted as part of his defense and have it verified by the Forensic Science Laboratory, the defendant appealed to the Supreme Court. Issue Is it necessary for the complainant or a witness to make a personal admission or denial of a document under Section 294 (1) of the CrPC if the document is on a compact disc?

Decision

According to the Supreme Court's interpretation of Section 294 (1) of the CrPC, a compact disc is a document with the same admissibility as any other document and does not need the personal admission or denial of the accused, complainant, or witness.

CBI vs. Arif Azim (Sony Sambandh)

NRIs may use the website www.sony-sambandh.com to order and pay for Sony items to be delivered to their Indian friends and family. A Sony Color TV and a cordless phone were ordered in May of 2002 by a user named "Barbara Campa" for a man named "Arif Azim" in the Noida area. Arif Azim received the shipment after she paid for it using a credit card. The credit card company warned the business, but the card's rightful owner refused to allow the transaction. The CBI received the complaint and opened an investigation under Sections 419, 418, and 420 of the Indian Penal Code (IPC), 1860. After conducting an investigation, it was determined that Arif Azim, while employed at the Noida Call Centre, fraudulently used Barbara Campa's credit card information. Issue When the IT Act falls short, is it possible to depend on the far more comprehensive IPC, 1860? Legal Ruling The court ruled Arif Azim guilty, although they were

[6] 2014 (1) Kar L J 121
[7] SC 1242 (2015)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

sympathetic toward him since he was a juvenile and this was his first offense. The offender was sentenced to a year of probation. When the court found that the IT Act was insufficient, it relied on the Indian Penal Code of 1860.

State of Tamil Nadu vs. SuhasKatti[8]

Contextual Information

The accused was a family friend of the victim's and had proposed marriage to her before she had married another guy. When she rejected the accused's proposal of marriage after their first divorce, he resorted to online harassment to get what he wanted. He created a fake email account in the victim's name and used it to send offensive, slanderous, and invasive messages. The suspects were charged with violating Section 67 of the IT Act as well as Sections 469 and 509 of the Indian Penal Code, 1860. Decision The Additional Chief Metropolitan Magistrate found the accused guilty under sections 469 and 509 of the Indian Penal Code, 1860, and section 67 of the IT Act. Under Section 469 of the IPC, he was sentenced to two years in prison and a fine of Rs. 500; under Section 509 of the IPC, he was sentenced to one year in prison and a fine of Rs. 500; and under Section 67 of the IT Act, he was sentenced to two years in prison and a fine of Rs. 4,000. This case is significant because it expedited the resolution of a cybercrime investigation, resulting in a conviction less than a year after the first police report was filed.

SMC Pneumatics (India) Pvt. Ltd. v. JogeshKwatra[9]***,***

Contextual Information

JogeshKwatra, the defendant, worked for the plaintiff. He began defaming the firm and its Managing Director by sending offensive and obscene emails to his employees and to the company's overseas branches. After looking into it, we discovered that the email was sent from a Cyber Cafe in New Delhi. During questioning, the defendant was recognized by the Cyber Cafe worker. The Defendant's employment was terminated on May 11, 2011.After that, he became vengeful and tried to settle scores by, among other things, writing emails designed to smear the names of plaintiffs 1 and 2. A lawsuit against the defendant has been launched because of this, and an injunction against further violations is being sought. Issue Should the court grant the plaintiffs' request for permanent injunctive relief? Is it true that the plaintiffs' hands were not clean when they entered the courtroom?

Decision

According to section 65B of the Indian Evidence Act, the court's ruling cannot be considered certified evidence, therefore the plaintiffs cannot get a permanent injunction. There was no hard proof linking the sender of these emails to a specific person or group. The court, on the other hand, ordered the defendant to refrain from making any defamatory statements against the plaintiffs in cyberspace.

Avnish Bajaj v. State (NCT) of Delhi[10]

Contextual Information

According to Section 67 of the Information Technology Act, Bazee.com's CEO Avnish Bajaj was detained in this case for allegedly screening cyber pornography. However, another user was peddling a CD with explicit content on it using the Bazee.com domain.

Decision

The court found that Mr. Bajaj was not responsible for the broadcast of obscene material. Bazee.com, which generates money from affiliate commissions and advertisements, would not allow such content to be seen on its site. The evidence shows that someone other than Bazee.com committed the cyber pornographic offense, the court notes. The CEO has approved bail, but it requires two Rs1 lakh sureties. The burden of proof is on the accused, who must

[8]Case No. 4680 of 2004:
[9]Case No. 33474 of 2016:
[10](2008) 150 DLT 769

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

demonstrate that he was only a conduit rather than a content producer. Pune History of Fraud at Citibank's Mphasis Call Center Three and a half million dollars were stolen in 2005 by hacking into four Citibank accounts in the United States and transferring the money to many fake accounts. The employees convinced the customers that they could help them through tough times, so they gave them their PINs. They weren't trying to crack encrypted programs or get through firewalls, but rather find vulnerabilities in the MphasiS infrastructure.

Decision

The court has determined that the defendants in this case are former workers of the MphasiS call center. Each employee is inspected each time they enter and leave the building. This indicates that the workers have the figures memorized. The funds were sent through SWIFT (Society for Worldwide Interbank Financial Telecommunication). The offense was committed through unauthorized access to customers' electronic accounts. This incident therefore constitutes a "Cyber Crime." All crimes committed with electronic documents may be prosecuted under the IT Act, while all crimes committed with paper documents can be prosecuted under the IPC. The court concluded that section 43(a) of the IT Act, 2000 applies due to the kind of unlawful access involved in executing transactions. In addition to the charges laid forth in sections 465, 467, and 471 of the Indian Penal Code, 1860, the defendants faced charges under sections 66 and 420 of the Information Technology Act, 2000.

Christian Louboutin SAS v. Nakul Bajaj &Ors.[11]

Contextual Information

An injunction was sought by a luxury shoe manufacturer against an online marketplace that allowed the sale of counterfeit shoes and thereby facilitated trademark infringement. Issue Can the plaintiff's logos, marks, and pictures (which are protected under Section 79 of the IT Act) be used by the defendant?

Decision

According to the Court, the defendant is more than just an intermediary since the website itself has full authority over the goods sold via its site. It acknowledges and encourages independent sellers to advertise their products. Further, the Court held that an e-commerce platform's active involvement would exclude it from the protections afforded to intermediaries under Section 79 of the IT Act.

Devidas Ramachandra Tuljapurkar v. State of Maharashtra,[12]

Contextual Information

The Indian Supreme Court considered whether publishing of a poem on historical individuals might result in charges under Section 292 of the Indian Penal Code. Debate Whether the poet who wrote "Gandhi Mala Bhetala" and distributed it to the All-India Bank Association Union breaks the law by doing so.

Decision

Since the poem had previously been performed and published by others, and since he had made an unreserved apology prior to the beginning of the proceedings after hearing the opinions of individual workers, the court invalidated the claims. According to the law, obscenity is determined by the "community standard test." Once it's established that anything is offensive, the question of whether the point of contention falls inside one of the exceptions in this section may emerge.

VI. CONCLUSION

"The law is not the be-all and end-all solution." In spite of a solid legal foundation and the victims' silence, victims continue to be denied justice. Cybercrime against women is merely a reflection of what is occurring in the real world.

[11] (2018) 253 DLT 728
[12] 6 S.C.R. 1 (2015)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

The distinctions between the online and offline worlds are blurring. Cybercrime occurs because of the perpetrators' belief that it is much simpler and carries less punishment. With millions of users, the complaint mechanisms of online platforms have also become ineffective. For example, in the recent boy's locker room case, a group of teenagers from Delhi shared photos of juvenile women and objectified them by posting derogatory remarks on Instagram and Snapchat group chats. When a female shared the chat screenshots, the group was discovered. Women across the nation elevated their voices, but it was evident that they were not surprised. The reason for this is that objectification of women has become a social norm. As new cases of objectification of women by men come to light daily, women have accepted this mentality. Despite the passage of time, women still fear venturing out into the actual world alone. In fact, the online world, which she could access from the comfort of her home, has become a dangerous place. It is the responsibility of women to take precautions such as using data security, not leaving a digital imprint, and keeping everything password-protected. However, these are all superficial means. In society, patriarchy and misogyny have always been the most significant problem. For this issue to be resolved, a long-term strategy must be implemented to combat cybercrime against women. With the advancement of information technology, it is imperative that societal and cultural norms evolve, and necessary measures must be taken to achieve this. Steps such as digital literacy, development of data security, providing women and girls with access to technology, and, most importantly, enactment of laws specifically on cybercrime in relation to women.