Cyber Cafe Case

Judicial Proceedings on Cyber Café Compliance: The State vs. Vishal Bhogade & Sandesh Dere

Case Details:

- **Case Number:** RCC No. 2095/2013
- **Court:** Judicial Magistrate First Class, Pune (Court No. 3), presided by S.R. Nimse
- **Complainant:** State of Maharashtra, through Bundgarden Police Station, Pune
- **Accused:**
    1. Vishal Hiraman Bhogade, Age 25, Service & Business, residing at Kharpudi Budruk, Pune.
    2. Sandesh Sopan Dere, Age 22, Service & Business, residing at Shiroli, Pune.
- **Charges:** Offences under Section 43(g), 66, and 67C(2) of the Information Technology Act, 2000, and Section 188 of the Indian Penal Code.

Prosecution Case Summary:

- On August 25, 2012, the Police Commissioner of Pune received an email with the subject "In Ganesh festival bomb blast," containing a threatening message: "Mission Ganesh attack. If you want to stop try but don't cry."
- The email was forwarded to the Cyber Crime Cell for investigation. Dr. Sanjay Tungar, the informant and a member of the Cyber Crime Cell, conducted a preliminary inquiry.
- Investigations revealed that the email was sent from Raje Computers, a cyber café in Rajgurunagar, Pune, using an internet connection registered to Vishal

Bhogade. The cyber café was operated by Sandesh Dere and was not registered as required by law. Necessary records, including user IDs, were not maintained.
- As a result, Dr. Tungar lodged an FIR against the accused under Cr. No. 191/2012, citing non-compliance with guidelines for cyber cafes.

Investigation and Evidence:

- During the investigation, police seized the cyber café's hard disk and conducted a spot panchanama (a form of written record used in Indian law).
- The prosecution presented Dr. Sanjay Tungar as a witness, who confirmed the receipt of the threatening email and the lack of compliance by the cyber café. He mentioned that the IP address traced back to Vishal Bhogade and that the café did not keep records of its customers, which hindered the investigation.

Charges and Defense:

- Initially, the accused were charged under Sections 43(g) and 66 of the IT Act and Section 188 of the IPC. Later, charges under Section 67C(2) were added.
- The accused denied all charges, stating that they did not wish to cross-examine any witnesses further after the additional charges were framed.
- The defense argued that the prosecution failed to prove their involvement in sending the email and highlighted the possibility of email spoofing, but did not provide evidence to support this claim.

Judgment Points:

1. **Section 43(g) and 66 of the IT Act:** The court concluded that these sections pertain to damages

to computers and systems and are not applicable in this case, as there was no damage reported.
2. **Section 188 of IPC:** Since the IT Act provides specific guidelines for cyber cafes, the court ruled that Section 188, related to disobeying public orders, was also not applicable.
3. **Section 67C(2) of IT Act:** The court found the accused guilty of contravening the IT (Guidelines for Cyber Café) Rules, 2011. These rules require cyber cafes to be registered, obtain ID proofs from users, and maintain a log register of users' activities.

Key Findings and Conclusions:

- The court acknowledged that the main culprit, who sent the threatening email, could not be traced due to the cyber café's non-compliance with statutory guidelines.
- The court emphasized the importance of compliance with these guidelines, especially given the threat of cyber crimes and cyber terrorism.
- The court found that the prosecution successfully proved that the accused failed to register the cyber café and maintain necessary records, as mandated by the IT Act.

Sentencing:

- Both Vishal Bhogade and Sandesh Dere were sentenced to 15 days of simple imprisonment and fined Rs. 10,000 each for violating Section 67C(2) of the IT Act. In default of payment of the fine, they would face an additional 15 days of imprisonment.
- The court acquitted the accused of charges under Sections 43(g), 66 of the IT Act, and Section 188 of the IPC due to insufficient evidence.

- The court ordered the preservation of seized property until the main culprit is identified and directed the concerned PSO to file a charge-sheet once the unknown accused is traced.

Final Order:

1. The accused are convicted under Section 67C(2) of the IT Act and sentenced as described above.
2. The accused are acquitted of charges under Sections 43(g), 66 of the IT Act, and Section 188 of the IPC.
3. The accused are required to surrender their bail bonds.
4. The preserved property will remain so until the main culprit is found.
5. A copy of the judgment is to be supplied to the accused free of charge.

Bazee.com Case (Avnish Bajaj vs. State): Section 67 and Section 85

• CEO of Bazee.com was arrested in December 2004 because a CD containing MMS of a DPS, R.K. Puram girl was being sold and hosted on the website.
• This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider.
• The burden rests on the accused that he was the Service Provider and not the Content Provider.
• It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.
• CEO was held liable by the Delhi High Court under Section 67 read with Section 85 of the IT Act recognizing the concept of an automatic criminal liability attaching to the director where the company is an accused.

Section 67B – Child Pornography

Lt. Colonel arrested for surfing Child Pornography

• A serving Indian Army officer of the rank of Lt. Colonel has been nabbed by the Mumbai Police.
• He was allegedly uploading, possessing & disseminating obscene pictures of foreign children between the ages of 3 & 10 on the Internet.
• The German Federal Bureau spotted the photos on a child pornography site and traced the pictures to India.
• The German agency alerted the Interpol which in turn passed the information to CBI which in turn tipped the

Mumbai Police.
• The Mumbai police has taken two hard drives from the Lt. Colonel's house as evidence against him.

State of Tamil Nadu Vs. Suhas Katti

• The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group.
• E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim.
• The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.
• Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC.
• Court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

Cases of 66A

• In September 2010, a freelance cartoonist Aseem Trivedi was arrested under Section 66A of the IT Act, Section 2 of Prevention of Insults to National Honour Act, 1971 and for sedition under the Section 124 of the Indian Penal Code. His cartoons depicting widespread corruption in India were considered offensive.
• On 30 October 2012, a Puducherry businessman Ravi Srinivasan was arrested under Section 66A. He had sent tweet accusing Karti Chidambaram, son of then Finance Minister P. Chidambaram, of corruption. Karti Chidambaram had complained to the police.
• On 19 November 2012, a 21-year-old girl was arrested

from Palghar for posting a message on Facebook criticizing the shutdown in Mumbai for the funeral of Bal Thackeray. Another 20-year-old girl was arrested for "liking" the post. They were initially charged under Section 66A.

• A group of Shiv Sena workers vandalized a hospital run by the uncle of one of girls. On 31 January 2013, a local court dropped all charges against the girls.

Mphasis BPO Fraud (2005):

Four employees at an Mphasis call center in India stole PIN codes from Citi Group customers and used this information to transfer money into fake accounts. They stole $426,000, but $230,000 was recovered when they were caught trying to withdraw the money. This case was prosecuted under Section 43(a) of the IT Act for unauthorized access.

Syed Asifuddin v. State of Andhra Pradesh:

Tata Indicom employees tampered with cell phones by changing their unique electronic numbers (ESN), which were meant for use only by Reliance Infocomm. The court found them guilty of altering the source code under Section 65 of the IT Act.

Kumar v. Whiteley:

A man named N.G. Arun Kumar hacked into a network and changed passwords to deny legitimate users access. He used the BSNL broadband connection to make illegal changes to user accounts, causing a financial loss. He was sentenced to one year in jail and fined under Section 66 of the IT Act and Section 420 of the IPC.

Fake Profile of President Pratibha Patil (2010):

Someone created fake Facebook profiles in the name of India's President Pratibha Patil. The profiles misled the public, and a complaint led to the imposter being charged under Section 66A of the IT Act and Section 469 of the IPC for forgery.

Bomb Hoax Email (2009):

A 15-year-old from Bangalore sent an email to a news channel, falsely claiming bombs were planted in Mumbai. The police tracked him down through the internet and arrested him under Section 66A of the IT Act.

Sandeep Vaghese v. State of Kerala:

A former employee created a fake website to defame his previous company, spreading false information about the company and its directors. He was charged with several offenses under Sections 65, 66A, 66C, and 66D of the IT Act.

Jawaharlal Nehru University MMS Scandal:

In this scandal, two students at JNU made a pornographic video on campus and shared it widely. When their attempt to extort money from the victim failed, they distributed the video through phones and online. The case was prosecuted under Section 66E of the IT Act for privacy violation.

Nagpur Congress Leader's Son MMS Scandal:

Two engineering students, including a Congress leader's son, filmed their sexual acts with a 16-year-old girl and shared the video online. They were arrested under privacy laws and the IT Act.

Mumbai Cyber Terrorism Threat:

A threatening email was sent to the Bombay Stock Exchange and National Stock Exchange, warning of a terror attack. The police traced the sender and made it

the first case of cyber terrorism under Section 66F of the IT Act.

First Conviction under Section 67 of the IT Act:

A man harassed a woman by creating a fake email account and posting obscene and defamatory messages about her online. He was convicted under Sections 469 and 509 of the IPC and Section 67 of the IT Act for publishing obscene material.

Lifelock CEO Identity Theft:

The CEO of an identity theft protection company, Todd Davis, had his social security number exposed on national television. This led to someone stealing his identity and taking out a $500 loan in his name, prosecuted under Section 66C of the IT Act.

Janhit Manch v. Union of India (2010):

An NGO filed a petition to block pornographic websites, arguing that they were harmful to youth. The case, which called for a ban on these sites, was pursued under Section 67B of the IT Act.