STATE OF MAHARASHTRA V. VISHAL HIRAMAN BHOGADE

COURT: JUDICIAL MAGISTRATE FIRST CLASS (COURT NO-3), PUNE

CITATION: R C. C. No.- 2095/2013

DATE OF PRESENTING: 25 APRIL 2013

DATE OF REGISTRATION: 25 APRIL 2013

DATE OF JUDGEMENT: 31 JULY 2015

BENCH: Honorable Justice S.R. NIMSE

PARTIES:

STATE OF MAHARASHTRA……..……COMPLAINANT

VERSUS

1. VISHAL HIRAMAN BHOGADE…….……...……. ACCUSED 1
2. SANDESH SOPAN DERE……. ACCUSED 2

FACTS OF THE CASE:

A mail was received on the mail ID of the Police commissioner of Pune on 25th August 2012. The subject of the mail stated "In Ganesh festival bomb blast" and the content of the mail also was a threat to the Police regarding a bomb blast on Ganesh Puja and further challenging the police to stop the attack. The mail as a result of being objectionable was sent for investigation to the Cyber Crime Cell, Pune. A prior investigation was conducted by the informant Dr. Sanjay Tungar. The inquiry revealed that the mail was sent from Raje Computers, Rajgurunagar, Pune. The cafe was run by Accused 2 Sandesh Dere and the internet connection was registered in the name of Accused 1 Vishal Hiraman Bhogade. Further, the cafe was not a registered one. The police failed to reach the criminal as the cafe did not maintain records of the visitors neither procured the mail IDs of the users. The informant registered FIR against the accused.

ISSUE RAISED:

The issue raised in this case was whether an intermediary could be arrested/convicted before the actual commission of the cyber-crime.

RULE APPLIED:

The accused were initially charged under Section 43(g) and Section 66 of the Information Technology Act, 2000, and also under Section 188 of the Indian Penal Code. Subsequently, there were charged under Section 67C (2) of the Information Technology Act, 2000.

Taking into consideration the investigation of the case and the statements of the accused that were recorded under Section 313 of Code of Criminal Procedure and further, hearing the arguments presented by both the parties the Court deduced that there was no adducing of evidence by the accused.

A. It was presented before the honorable Court that the prosecution had failed to prove the charge that was filed under Section 43(g)[1] against the accused. The accused had not provided help to the preparator at his Cyber Café assisting him in violating the provision and the rules.
B. The charges filed under Section 66[2] of the I.T Act were also held invalid by the prosecution. The accused had not fraudulently or dishonestly aided the main culprit in accessing the computer network thereby violating the law.
C. Further, the charges under Section 188[3] of the IPC were also held invalid. The accused on the day of the commission of the crime had not disobeyed the law and order implemented by the public servant.

[1]any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder

[2]If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

[3]Disobedience to order duly promulgated by public servant.—Whoever, knowing that, by an order promulgated by a public servant lawfully empowered to promulgate such order, he is directed to abstain from a certain act, or to take certain order with certain property in his possession or under his management, disobeys such direction, shall, if such disobedience causes or tends to cause obstruction, annoyance or injury, or risk of obstruction, annoyance or injury, to any person lawfully employed, be punished with simple imprisonment for a term which may extend to one month or with fine which may extend to two hundred rupees, or with both; and if such disobedience causes or trends to cause danger to human life, health or safety, or causes or tends to cause a riot or affray, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

D. But the prosecution proved the charges under Section 67 C (2)[4] valid. The accused had violated the guidelines of the Information Technology Rules, 2011.

Moreover, complying with Section 43(g), the accused had neither dishonestly nor fraudulently aided the culprit in the commission of the crime. The accused were naïve to the mail that was sent by the preparator.

ANALYSIS OF THE JUDGEMENT:

The court highlighted the facts that as per Section 3 of the above-stated guidelines, a Cyber Café needs to be compulsorily registered. Further, under Section 4 of the guidelines, procuring the ID proofs of the users is mandatory on the part of the Cybercafe.

Moreover, complying with Section 5, the log registration is requisite. And the guidelines under Section 4 and 5 further mentions that the information procured from the users should be preserved for a span of a minimum of 1 year. In the present case, there was no registration of the Cyber Café and the ID proofs were also not obtained by the users. The café also did not maintain records.

Section 67C (1) states that preservation and retention of data and information by the intermediary are mandatory. And on the breach of subsection 1 of Section 67 C, it is a punishable offense under Section 67 C (2) of the IT Act. Since the prosecution could not prove liability under Section 43(g) and Section 66 of the IT Act as well as under Section 188 of the IPC. They were charged under Section 67C (2) in the offense of violation of Section 67 C (1). The IP address was assigned to accused 1 Vishal Bhogade and the café being run by Accused 2 Sandesh Dere. The court held that the Café did not comply with the rules of the Information Technology (Guidelines for Cyber Café) Rules 2011.

The café owner in this case had no “malicious intention” behind his carelessness. It was negligence on his part to not maintain the records and information of the users as well as of not registering the café. Violation of law under section 67 C (2) requires "intention" and "knowing". The café owners had neither intention nor any knowledge regarding any such threatening mail that was sent to the Pune Police on the stated date.

[4]Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to three years and also be liable to fine.

Further, the Court held that the privilege of Section 360 of the Code of Criminal Procedure[5] could not be provided to the accused as due to the negligence on the part of the accused non-maintenance of recorded the main suspect could not be traced by the police.

A similar incident occurred in December 2004 in Chennai when a man influenced by the movie "Ramana" sent a threatening email of a bomb blast to some secretaries. The culprit was charged under the Indian Penal Code since there was no IT Act and hence there was the absence of Section 66A and Section 66F.

Concluding, both the accused were acquitted for the offense actionable under Section 42(g) and Section 66 of the Information Technology Act, 2000 and also under Section 188 of the IPC vide Section 248(1) of the CrPC. The court held Accused 1 Vishal Hiraman Bhogade and Accused 2 Sandesh Sopan Dere liable for the offense under Section 67C (2) of the Information Technology Act, 2000 vide Section 248(2)[6] of the Cr.P.C. The Court sentenced them imprisonment of 15 days and imposed a fine of Rs. 10,000 on each of the accused. Further, the court declared that on the failure of payment of the amount the imprisonment will be extended for another 15 days. The main preparator could not be traced due to lack of sufficient evidence. The investigation further proved that the mail ID was created solely for the purpose of sending the mail because no other activities were recorded from the mail ID. Moreover, the investigation revealed that the café owners had installed banned foreign software and as a result of which it was difficult on the part of the police to trace the culprit.

The sentence for the offense charged against the accused extended up to a term of 3 years. But the court is impressed with the behavior of both the accused and witnessing there regular presence in the courts had considered giving a decrease in their sentence.

The Pune Court could have focused on the role of the State Government in the formation of a regulatory authority for the regulations of cyber Cafe. This could have been a new direction for other Cyber Café's that remained unregistered and that still did not comply with the guidelines of the Information Technology Rules, 2011. The court should have devoted its attention to the part of the government in improving compliance. Though there are several software available

[5] Order to release on probation of good conduct or after admonition.
[6]Where, in any case under this Chapter, the Magistrate finds the accused guilty, but does not proceed following the provisions of section 325 or section 360, he shall, after hearing the accused on the question of sentence, pass sentence upon him according to law.

to cyber cafes to manage ITA 2008 compliance some of which have been even recommended by Police in several States, the State Governments have not created the back end systems to receive data created from these software and therefore the use of such software has not gained popularity.[7]

CONCLUSION:

The penalty imposed upon the café owners were adequate owing to the fact that there was no malicious intent on the part of the owners. So, the owners had not aided the culprit in the commission of the crime. But the owners have failed to maintain the café with a par to the guidelines. Had the café owners successfully maintained proper records of the users, then the culprit would have been caught and the owners would not have been accused of negligence on their part of maintaining the café. It is mandatory for the cafe owners to maintain the information of the users like it as an easy place for the commission of cyber-crimes and without proper evidence, the culprit might get away with such act. This case sets an example for all cafe owners who do not maintain proper records of the users and also neglect in obtaining and verifying the ID proofs of the users. The police in this case arrived at the conclusion that the owners should install CCTVs at the cafes and also should restrain the installing of anti-forensic software.

This case is an important precedent for cases where the intermediary could be arrested before the actual commission of the crime. This gives the police right to catch the culprit to avoid the commission of any crime. It is interesting to note that for the first time in this case Section 67 C was invoked for a conviction.

The police could have further added charges for "Threat via email" under Section 66A[8] as this Section was functional at that time when the crime was committed. It would have been interesting to note how the court would have dealt with the charges under Section 66A. Although this Section was subsequently quashed down by the Supreme Court.

[7]Vijayashankar Na, Conviction of an Intermediary is possible even before the real cyber criminal is traced, Naavi (5 August , 2015), https://www.naavi.org/wp/conviction-of-an-intermediary-is-possible-even-before-the-real-cyber-criminal-is-traced/#:~:text=Conviction%20of%20an%20Intermediary%20is%20possible%20even,real%20cyber%20criminal%20is%20traced.&text=Accused%20Vishal%20Hiraman%20Bhogade%2C%20Sandesh,and%20Section%20188%20of%20IPC

[8] Section 66A of the IT Act defines the punishment for sending "offensive" messages through a computer or any other communication device like a mobile phone or a tablet. A conviction can fetch a maximum of three years in jail and a fine.

CASE ANALYSIS

Cyber-crime is a burning threat in the 21st century. There are rules and laws for the protection against such crimes. But there needs to be the maintenance of proper records for the tracking of the culprit. In the present case, the email was sent from a cybercafé and the information about the users was not recorded, as a result of which the informant failed to trace the culprit.