CYBER CRIMES AND BAIL: AN OVERVIEW

Dr.Sairam Patro
M.Com.,MBA(HRM), Ph.D(Law)
Lecturer/ Faculty, Lingaraj Law College
e-mail: drsairampatro @ gmail.com
Mob: 9861099455

A B S T R A C T

Cyber crimes are committed by persons, sitting far away from the victim and without having any direct physical access to the latter. Cyber Crime include Data Theft, Hacking, Computer Theft, Cyber Defamation, Social Media Abuse, Obscenity Matters, Pornography related matters, Online gambling, Denial of service, Software piracy, Copyright violation, Online Banking theft crimes, Cyber Frauds, Credit card frauds, Spreading of virus etc. to combat cyber crime in India has adopted the Information Technology Act, 2000. This act got drastically Amended in the year 2008.

Bail is an integral part of our criminal justice system and granted during the pendency of the trial or an appeal. The provisions for bail in case a person is arrested for a cybercrime are found in the Criminal Procedure Code, 1973 and the Information Technology Act,2000. The Criminal Procedure Code does not define the term 'bail' but contains provisions for grant of bail either by the police or courts. Section 77 B was introduced by the Information Technology Amendment, 2008 (Act 10 of 2009). Section 77B provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973 the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three year shall be bailable.

There is a great difference between the nature of cyber crime and ordinary crimes, as well as in investigation,. Hence it is essential to incorporate special provisions relating to arrest and bail in the case of cybercrimes in the IT Act. There is grave underreporting of cyber crime in the nation.

Key Word: Cyber Crime and Bail

Introduction

Cyber-crimes are committed by persons, sitting far away from the victim and without having any direct physical access to the latter. By touching the key

board of the computer with his fingers, the criminal can cause unimaginable harm to the victim and also steal more than what an ordinary robber could have done with gun. Cyber-crimes include Data Theft, Hacking, Computer Theft, Cyber Defamation, Social Media Abuse, Obscenity Matters, Pornography Related Matters, Online Gambling, Denial of Service, Software Piracy , Copyright Violation, Online Banking Theft crimes, Cyber frauds, Credit Card Frauds, Spreading of Virus etc.

To combat cybercrime India has adopted the Information Technology Act 2000. This act got drastically amended in year 2008. The Amended Information Technology Act is not only effective than the previous Act it is more powerful and stringent than the previous one. The purpose of this paper is to discuss bail in relations to cybercrimes.

Cyber Crimes

Cyber crime cannot be precisely defined but is attributable to any offence involving an internet device. These crimes are covered under the Information Technology Act, 2000[1], supplemented by the Indian Penal Code 1860.Crimes, like hacking, data theft, virus attacks, denial of service attacks, illegal tampering with source codes including ransom ware attacks could be prosecuted under Section.66 r/w Section.43 of the IT Act. In 2008 the IT Act was amended. Provisions were added to protect against identity theft (Section 66C) or cheating by impersonating online (Section 66D). Victims of revenge porn may register complaints for violation of their privacy under Section 66E as also under Section 67 and Section 67A IT Act in addition to IPC provisions. Section 67A and Section 67B also provide for prosecution of pornography and child pornography respectively. In case of the latter, the provisions of the Prevention of Children from Sexual Offences Act, 2012 (POCSO) may also be invoked. Cases of forging

[1]. The IT Act 2000 was amended in 2008

a credit or debit card or even cloning a mobile SIM with dishonest or fraudulent intent to cause wrongful loss or wrongful gain could be prosecuted under IPC provisions.

Bail Provisions under Criminal Procedure Code

The Criminal Procedure Code does not define the term 'bail' but contains provisions for grant of bail either by the police or courts. The Police Officer has power, to release a person on bail who has been accused of an offence and is in his custody. The Power to grant bail by police has been conferred upon them by the virtue of sections 42, 43, 56, 59, 71, 81, 169, 170, 436, 437 and Schedule I Column 5 of the Code.

Sections 436 to 439 deal with the provisions of bail. Bail is, generally, a kind of security which is given by the accused to the court that he will attend the proceedings against the accusations made upon him and include personal bond and bail bond. It is a mechanism used to ensure the attendance of accused at the trial before court.

Bail is an integral part of our criminal justice system and granted during the pendency of the trial or an appeal. Before bail is granted to the accused, a surety gives a guarantee to the Court that the accused will appear in the Court as and when required. Moreover, a sum of money is to be deposited to ensure his appearance before the Court, which otherwise stands forfeit

Offences are classified into "bailable" and "nonbailable" offences. Under Section 2(a) of the Criminal Procedure Code, "bailable offence" means an offence which is listed as bailable in the First Schedule or which is made bailable by any other law for the time being in force. Non-bailable offence' means any other offence. The CrPC has not provided any criteria to determine whether any

particular offence is bailable or non-bailable in the First Schedule. The gravity of the offences, namely, offences punishable with imprisonment for three years or more have been treated as non-bailable offences. But, this is not a hard and fast rule. There are exceptions to the same.

In case of bailable offences, under section 436 Cr.PC it is the right of accused to demand and be granted bail. The basic criteria for grant or denial of bail in case of non bailable offences has been laid down in section 437 Cr.PC. The criteria include the nature of offence, past criminal records, probability of guilt, and possibility of threatening witnesses or tampering with evidence.

Anticipatory bail is a bail that is applied for prior to one's arrest or detention by an authority, but in anticipation of the same. Section 438 of the Criminal Procedure Code prescribes that a person may apply to an appropriate High Court or Court of Sessions for anticipatory bail when he has reason to believe that he may be arrested on accusation of having committed a non-bailable offence. The filing of an FIR is not a mandatory pre-condition for the filing of an application for anticipatory bail. When directing the grant of anticipatory bail, the Court may set such conditions as it deems fit.

Bail Provisions or cyber offences

Section 77 B was introduced by the Information Technology (Amendment) Act 2008 (Act 10 of 2009). Section 77-B provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Case Law

An interesting case[2] relating to bail in cyber crimes came up before the High Court of Odisha in 2017. Obinna Nicodemus Enweka @ Obina Icodemus was the Petitioner and the State of Orissa was the opposite party.

Sukanti Mohanty filed an FIR at Cyber Crime Police Station of C.I.D., C.B., Cuttack stating that she had become a victim of organized cybercrime and had paid a sum of Rs.17,03,390/- to different persons through their bank accounts which were provided to her through e-mail/sms /whatsapp. She alleged against one person identifying himself as Frank Young on facebook had sent her a friend's request which she accepted. The accused informed the informant that he had sent her some gifts which were held up in Delhi from where she should collect the gifts. The informant was asked through a number of calls and e-mails for money on various pretexts i.e. remittance, foreign exchange, transfer etc. The phone calls and sms were received from different numbers and the people who identified themselves as Frank, Marc, security personnel, R.B.I. officials and Airport officials etc. advised and convinced the informant to deposit money in different bank accounts provided by them. The money was paid in four different bank accounts of four different persons by the informant totalling to Rs.17,03,390/-.

Basing on the first information report, C.I.D.C.B. Cyber Crime P.S. Case No.12 dated 26.08.2016 was registered under sections 419/420/468/471 of the Indian Penal Code and section 66-C/66-D of the Information Technology Act, 2000.

During course of investigation, the informant and other witnesses were examined. The documents relating to deposit of money, accounts statement of the

[2]. *Obinna Nicodemus Enweka @ Obina Icodemus vs.State of Orissa* Date of order 22.11.2017 ……..

informant's bank account as well as some other relevant documents were seized. Requisitions under section 91 of Cr.P.C. were sent to the concerned banks to provide A/c opening forms details along with up to date account statement and other necessary information for identification of the account holders. Immediate correspondence were also made with concerned mobile service providers to ascertain the subscriber information as well as call details to ascertain the identity and location of the cell phone numbers which were used in making contact with the informant. While conducting investigating at New Delhi, it was ascertained that large sum of money was deposited in the bank accounts of fraudsters and the same was immediately being transferred to many other bank accounts in smaller amounts by internet banking and soon after that the smaller amounts were withdrawn immediately through ATMs in no time leaving very little or no balance in the beneficiary accounts. The concerned branch managers were requested to debit freeze the beneficiary accounts. On 08.10.2016, the Inspector of Cyber Crime, Goa intimated the investigating officer by e-mail that two Nigerian nationals i.e. the petitioner and another have been arrested on 03.10.2016 by Goa police and during interrogation, it was ascertained that they are involved in a crime in Orissa by defrauding the informant by using two mobile numbers. During verification of the mobile numbers and call records received from the mobile service providers, it appeared that the two mobile numbers are common in Odisha Cyber Crime case and Goa Cyber Crime case. The investigating officer received CDR and CAF in respect of some of the mobile numbers and analyzed them. From the CDR of the mobile phones, it became evident that the fraudster had induced the informant by making telephone call and sms and the two mobile numbers which were used in two IMEIs were seized by the Cybercrime officials of Delhi and Goa. It was ascertained during course of investigation that the petitioner and another co-accused had become friends with the informant through e-mail/sms/whatsapp. Finding sufficient prima facie evidence against the petitioner, charge sheet was submitted on 27.02.2017 against

the petitioner and another co-accused under sections 419/420/468/471 of the Indian Penal Code and sections 66-C/66-D of the Information Technology Act keeping the further investigation open under section 173(8)of Cr.P.C.

The petitioner, a 21 year old boy moved an application for bail before the learned Addl. Sessions Judge, Bhubaneswar in Bail Application No.201/904 of 2017 which was rejected vide order dated 02.08.2017.

Justice S. K. Sahoo, commenting on the nature of the crime stated,: "The manner in which the crime has been committed shows the devilish master mindedness, cool thinking, tricks adopted, organised effort and timely execution of plan of the offenders. The intelligence and advanced type of knowledge on cyber seems to have been utilised in a wrong way. Sitting somewhere far from the victim and without having any direct physical access to her, the cybercriminal has caused unimaginable harm to her with touches of his fingers on the computer and stolen more than what an ordinary criminal could have done with gun. The victim of the organised crime appears to be an innocent lady fell into the trap of evil design. With the temptation of getting foreign gifts, she acted like a brainless toy in the hands of the criminals till she realised one day that she had been deceived on a mistaken impression."

Rejecting the bail application he held: "considering the nature and gravity of the accusation, the nature of supporting evidence, the manner in which the informant has been cheated with a huge amount, the severity of punishment in case of conviction, the reasonable apprehension of tampering with the evidence particularly when the further investigation is under progress and the criminal proclivity of the petitioner, I am not inclined to accept the prayer for bail of the petitioner."

Conclusion

Together with the advancement of technology, varieties of cybercrimes, such as email hacking, software piracy, cyber stalking and cyber terrorism are taking place. At present, cybercrimes committed by children with cameras and data on their mobile phones are increasing. Irrespective of the age of the accused, if the offence of circulating sexually explicit content or violating privacy through dissemination of images or videos of private parts is committed, the person is susceptible to prosecution.

There is a great difference between the nature of cybercrimes and ordinary crimes, as well as in investigation. Hence it is essential to incorporate special provisions relating to arrest and bail in the case of cybercrimes in the Information Technology Act. There is grave underreporting of cybercrimes in the nation.

Cyber Crime is committed every moment, but rarely reported. The cases of cybercrime that reach the Court of Law are therefore very few. There are practical difficulties in collecting, storing and appreciating Digital Evidence. Cybercrimes are stipulated under the IT Act as bailable offences, which may lead to people committing cybercrimes to be let out on bail and tamper with evidence.