Judicial Academy Jharkhand

READING MATERIAL

ON

CYBER CRIMES: INVESTIGATION AND TRIAL UNDER THE CURRENT LAW

Prepared by :
Judicial Academy Jharkhand

Judicial Academy Jharkhand

READING MATERIAL

on

CYBER CRIMES: INVESTIGATION AND TRIAL UNDER THE CURRENT LAW

Prepared by :

Judicial Academy Jharkhand

CONTENTS

1. Culpability under the Current Legal Regime 1

Computer related Offences - Identity Theft 1

What are the provisions of the Information Technology Act, 2000 which are applicable to "identity theft"? 2

What are the provisions of the Indian Penal Code which are applicable to "identity theft"? 4

Can the offender be charged with and tried for offences both under the IT Act and the IPC? 8

Can the offender be charged with and tried for offences both under the IT Act and the POCSO Act? 13

What is the procedure for trail of offences under the IT Act? 14

2. Procedure related to Investigation 16

Which Police Station shall have jurisdiction to investigate a case related to cyber crime? 18

3. Examination of Witness and Recording of the Statement 21

Can the statement of a witness be recorded by the Police using Audio-Video Electronic medium? 21

Can the Court record the statement of the witness by audio-video Electronic means? 22

Can the statement under Section 313 of the CrPC be taken through audio-video electronic means? 25

4. Electronic Evidence 27

Admissibility 27

When is the Certificate not Required? 29

What is the stage of filing the certificate? 30

Who is competent to issue the Certificate? 32

When can the objections related to the Electronic Evidence be raised? 32

5. Liability of Intermediary 33

Who is an intermediary? 33

What are his liabilities? 34

The Information Technology (Intermediaries Guidelines)Rules, 2011 34

What is the concept of Auto block of the unlawful content available on the website of the intermediary? 37

Blocking of Websites 40

The internet is primarily about communications and the networks that enable connectivity between computers on one side of the world with those on the other. So, the computers per se are not the sole object of concern rather it's the computers connected to other computers, the network computers .

A distinction is made between acts where the computer is the object of the crime, primarily addressing the theft of the hardware and software components, secondly, where the computer is the subject of the crime, for the purpose of breaching its confidentiality, integrity, an availability or the data it processes; thirdly, where the computer is the instrument of the crime encompassing both fraud and computer pornography offences.

1. Culpability under the Current Legal Regime

Computer related Offences - Identity Theft

On a daily basis, we are required to identify ourselves at numerous occasions, for example while accessing online banking services, we need to enter our password and username. However, if we fail to identify ourselves we may be denied access to our entitlements. On the other hand, if someone else is able to impersonate us, they may be able to gain access to that to which they are not entitled. One aspect of fraud which has received considerable notoriety over recent years has been the phenomenon of "identity theft", where a person's identification details are obtained through various surreptitious methods, for example by 'phishing', where emails are sent to individuals falsely claiming to originate from their as bank and asking them to re-register their account details at a replica website, or contain a virus which surreptitiously obtains and discloses an individual's confidential details.

In some cases, Social networking sites may be a fruitful source of personal information that can be used to create more plausible phishing messages targeted at specific individuals or organisations. For example, it might be possible to obtain information from a person's social networking sites profile that they are overseas. A fake message may then be sent to family and friends stating that the person has lost his wallet and needs funds to get home.

Another method utilised is 'pharming' which utilises the way in which internet domain names are resolved to direct unsuspecting users to the false website. For example, the domain name for the website may be a common misspelling of the legitimate website or a different domain (com instead of org) making it easy for users to stumble onto the fake website. A person who knows not to click on any suspicious links in emails, will still type legitimate URLs into their browser not suspecting it may lead to a phishing site.

The area of offences related to cyber crimes is an expanding and evolving one in the sense that either new types of offences come up again and again or new ways of committing them are developed by the perpetrators. Bank Accounts are one of the most common targets for cyber crimes by fraudulently and dishonestly procuring the ATM Pins or OTPs (One Time Passwords) from the Account Holders and misappropriating the money therefrom. Most of the times, when these misappropriated money were utilized by or deposited in the Bank Accounts of the perpetrators, the Police was able to trace them easily. To evade this, a new modus operandi has been developed. The money dishonestly taken away from the possession of the Account Holders from their Bank Accounts are now deposited by the perpetrators in the Bank Account of a third person. These persons whose accounts are used may either be innocent or may be the ones who enter into an agreement or conspiracy with the actual perpetrators and agree to let them use their Bank Accounts for the proceeds of the crime either for free or for some share in the proceeds.

Though it is an extremely difficult task, yet the Investigating Agencies and the Courts need to differentiate between these two categories. The first group of people involves the innocent Bank Account holders who are generally poor and illiterate and have their accounts in the Bank for Government benefit programs such as Jan Dhan Yojna. They are tricked into handing over the possession of their accounts to the perpetrators of cyber crimes, without any intention, knowledge or reasonable belief that their accounts will be misused for illegal purposes. In such situations, the Bank Officials must keep a strict check on the activities related to such Bank Accounts and must create awareness amongst the people.

The main problem before the Investigating Agencies and the Courts is with respect to the second group of people who voluntarily let their Bank Accounts be utilized for the purposes of receiving or transferring the proceeds of cyber crimes.

What are the provisions of the Information Technology Act, 2000 which are applicable to "identity theft"?

The provisions related to the offences of "identity theft" discussed above have been laid down in the provisions of Sections 66C and 66D of the IT Act. Section 66C of the IT Act reads as follows :-

> 66C. Punishment for identity theft.–Whoever, ***fraudulently or dishonestly make use of*** the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either

description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. **(emphasis supplied)**

Section 66D of the IT Act reads as follows :-

66D. Punishment for cheating by personation by using computer resource.– Whoever, ***by means of*** any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. **(emphasis supplied)**

The IT Act is a special Act, the object of which is as follows :-

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as —electronic commerce , which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

It is apparent from the object of the Act that it is not the intention of the Legislature to completely or exhaustively exclude the offences related to cyber or information technology from the purview of the provisions of the IPC. Wherever the Legislature intended to exclude the provisions of a General Law, the same has been done expressly, as evident from Section 81 of the IT Act which reads as follows :-

81. Act to have overriding effect.–The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).

The provisions of the IT Act shall have effect notwithstanding the fact that it may be ***"inconsistent"*** with the provisions of any other law. The connotation of this provision is not the exclusion of the provisions of all other General Laws. What the provisions of Section 81 does is that it validates the provisions of the IT Act even if it is inconsistent with the provisions of any other law. Therefore, in cases of "identity theft", there is no

provision in the IT Act or in the IPC which prohibits the application of the provisions of the IPC and the culpability thereunder.

Moreover, the probable Sections of the IPC under which the offence of "identity theft" can fall have been discussed in the following paragraphs and depending on the facts and circumstances of the case in a hypothetical case related to ATM Pins and Bank frauds discussed above, the probable Sections applicable are Sections 107, 109, 120A, 201, 378, 410 417 and 420 of the IPC. The offences under the IPC Act and those under Sections 66C and 66D are distinct offences and, therefore, the provisions of the IPC and the IT Act will be applicable. In light of this, the provisions of the IPC which may be applicable in cases of "identity theft" have been discussed below.

What are the provisions of the Indian Penal Code which are applicable to "identity theft"?

1. The person whose account is used for the transfer and deposit of the money which are the proceeds of a cyber crime is an abettor of the crime within the meaning of Section 107 of the Indian Penal Code. According to Section 107, a person abets the doing of a thing, who intentionally aids, by any act or illegal omission, the doing of that thing.

In this case, the person who voluntarily consents to let his account be used for the proceeds of the cyber crime intentionally aids in the crime by assisting the actual perpetrator in disposing of the proceeds of the crime through his Bank Account and is, therefore, culpable under Section 109 of the Indian Penal Code and can be charged and tried therefor.

2. If the commission of the crime prima facie shows that the involvement of the third person who has let his Bank Account to be used for the proceeds of the crime had entered into an agreement or the ingredients required for "criminal conspiracy" as required under Section 120A are satisfied, the person can be charged with and tried for the offence of "criminal conspiracy" punishable under Section 120B of the Indian Penal Code. The prima facie indication of the existence of an agreement to use the Bank Account of the third person for the proceeds of the cyber crime entails that the agreement is for the commission of an illegal act punishable under the provisions of the Indian Penal Code and the Information Technology Act and secondly, that an illegal act of cyber crime to attack the bank account of the victim which is an illegal act committed besides the agreement, thereby satisfying the ingredients required to attract the culpability under Section 120A, punishable under Section 120B of the

Indian Penal Code.

3. The provisions of the Indian Penal Code also recognize ex-post facto ¬aiding and abetting. Even in the absence of an agreement between the actual perpetrator and the third person who lets his bank account to be used for the purposes of depositing the proceeds of the cyber crime and thereby assisting in the concealment of the same, the third party can be charged with and tried for the offence under Section 201.

The purpose of Section 201 has been discussed by the Hon'ble Supreme Court in ***Sou. Vijaya @ Baby v. State of Maharashtra, (2003) 8 SCC 296***, wherein it was held that to make an accessory ex post facto it is in the first place requisite that he should know of the felony committed. In the next place, he must receive, relieve, comfort, or assist him. And, generally any assistance whatever given to a felon to hinder his being apprehended, tried or suffering punishment, makes the assister an accessory. What Section 201 requires is that the accused must have had the intention of screening the offender. To put it differently, the intention to screen the offender, must be the primary and sole object of the accused. The fact that the concealment was likely to have that effect is not sufficient, for Section 201 speaks of intention as distinct from a mere likelihood.

Section 201 punishes any person, who knowing that any offence has been committed, destroys the evidence of that offence or gives false information in order to screen the offender from legal punishment. Section 201 is designed to penalize "attempts to frustrate the course of justice", as held by the Hon'ble Supreme Court in S***tate of Karnataka v. Madesha and Ors., (2007) 7 SCC 35***.

The main purpose behind letting the perpetrator of the cyber crime use the Bank Account is to screen the offender from the Investigating Agency and the process of the Court and to mislead them from reaching the actual offender of the crime and such aiding and abetting after the commission of the crime has a substantial effect on the commission of the crime. Therefore, since the deposit of the proceeds of the cyber crime into the Bank Account of a person other than the offender and the victim is solely for the purpose of intentionally screening the offender and, therefore, the person whose Bank Account is used for the purpose can be charged with and tried for the offence under Section 201 of the Indian Penal Code, in which the existence of a prior agreement is not required to be proved.

4. The most common type of cyber crime is the one which involves the offender to impersonate as a Bank Manager or such official and then dishonestly induce the victim to disclose his ATM Pin or the OTP after which the offender takes away the money from the victim's Bank Account and then transfers the amount from the Account of the victim to the Account of some third person with the intention to avoid the investigation in the case and from the clutches of law. The offence has become very common and has affected several common people who have lost their hard-earned money through such fraudulent cyber offences.

In the case of the aforementioned offence and the modus operandi thereof, the offender dishonestly takes a movable property (money) from the Bank Account of the victim. As far as the question of victim's consent is concerned, though he gives his consent by sharing his ATM Pin or OTP with the offender but such a consent is taken under misconception of fact practiced by the offender by impersonating himself as the Bank Manager or such authoritative officials and, therefore, such a consent is not a consent within the meaning of Section 90 of the Indian Penal Code and for the purposes of Section 378. The consent for the purposes of the provisions of the IPC should be in consonance with Section 90 which reads as follows:-

90. Consent known to be given under fear or misconception.—A consent is not such a consent as it intended by any section of this Code, if the consent is given by a person under fear of injury, or under a misconception of fact, and if the person doing the act knows, or has reason to believe, that the consent was given in consequence of such fear or misconception; or Consent of insane person.—if the consent is given by a person who, from unsoundness of mind, or intoxication, is unable to understand the nature and consequence of that to which he gives his consent; or Consent of child.—unless the contrary appears from the context, if the consent is given by a person who is under twelve years of age.

Therefore, the offender, in this case, can be charged with and tried for the offence of theft under Section 378, punishable under Section 379 of the Indian Penal Code.

The third person who assists the actual offender in the crime by letting him use his Bank Account for the purpose of disposing of the proceeds of the crime procured through theft from the victim's Bank Account can also be held liable for the offence of theft. Such culpability can be attributed to the person by virtue of Section 34 of the Indian Penal Code which lays down the principle of constructive liability. According

to the Hon'ble Supreme Court in ***Pandurang v. State of Hyderabad, AIR 1955 SC 216,*** the essential part of Section 34 is that the common intention under the Section 34 presupposes prior concert. If that is established, then even if the person does not actually participate in the commission of the main offence, he can be held liable for the offence with the help of Section 34 of the IPC . In the present case, unless the case prima facie indicates that the Account Holder whose account has been used for the disposal and misappropriation of the money procured through theft from the victim's bank account, is innocent by virtue of his poverty, illiteracy and ignorance, the existence of a prior concert can be very well presumed between the Account Holder and the offender owing to the fact that the details of the Account and the credentials required for the transfer of money had been shared with the offender and also from the fact and in spite of the fact that such huge amounts of money or unaccounted money of any amount is transferred in the third person's account and he does not inform the Police or the Bank Officials.

5. As discussed above the offence involves the offence of theft which is committed by dishonestly taking a movable property (money) from the possession of the victim (Bank Account) without his consent as the consent (in the form of ATM Pin or OTP) is taken by the offender under misconception of fact as stipulated under Section 90 of the IPC. Since the money taken away from the victim's Bank Account has been transferred through theft, the same falls in the category of "stolen property" as defined under Section 410 of the IPC which reads as hereunder :-

410. Stolen property.—Property, the possession whereof has been transferred by theft, or by extortion, or by robbery, and proper¬ty which has been criminally misappropriated or in respect of which [***] criminal breach of trust has been committed, is designated as "stolen property", [whether the transfer has been made, or the misappropriation or breach of trust has been commit¬ted, within or without [India]]. But, if such property subse¬quently comes into the possession of a person legally entitled to the possession thereof, it then ceases to be stolen property.

As the third person who lets his Bank Account to be used for receiving the money procured through theft, he can be held liable for committing the offence of dishonestly receiving "stolen property" under Section 411 and for assisting in the concealment of "stolen property" under Section 414 of the Indian Penal Code and if the person is habitually involved in such an arrangement, he can also be held liable

for habitually dealing in "stolen property" under Section 413 of the IPC.

6. By virtue of the discussions made hereinabove related to the scope of "movable property", the offence discussed hereinabove would also fall under the provisions of Sections 415 and 420 which read as follows :-

415. Cheating.—Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any proper¬ty to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation.—A dishonest concealment of facts is a deception within the meaning of this section.

420. Cheating and dishonestly inducing delivery of property.—Whoever cheats and thereby dishonestly induces the person de¬ceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Can the offender be charged with and tried for offences both under the IT Act and the IPC?

The trial of an offence commences from the framing of the charge as provided under Chapter XVII of the CrPC. **Section 218** of the CrPC states that for every distinct offence of which any person is accused, there shall be a separate charge, and every such charge shall be tried separately. Two offences would be distinct if they are in no way interrelated. Sections 219-224 contain exceptions to the general rule contained in Section 218 and provide for the joinder of charges and of trials. However, there is no mandatory provision of the law laying down that, where separate trials can be held under the general rule, the Court must hold a joint trial, if the case falls under within one of the provisions that permit the holding of a joint trial.

Section 220 of the CrPC is one of the exceptions to the general rule contained in Section 218. It provides for the trial of more than one offences and the relevant provisions

related to the framing of charges and trial of an offence falling within two or more separate definitions of any law in force for the time being and reads as follows :-

220. Trial for more than one offence.

……

(3) If the acts alleged constitute an offence falling within two or more separate definitions of any law in force for the time being by which offences are defined or punished, the person accused of them may be charged with, and tried at one trial for, each of such offences.

…….

This provision contemplates offences falling under the definitions of separate provisions of the Indian Penal Code (IPC) or under the provisions of a Special Act or a Local Act or under the provisions of both IPC as well as a Special Act or a Local Act or both. Therefore, by virtue of Section 220(3) of the CrPC, the trial of an offence falling within two or more separate definitions of any law in force for the time being is permissible.

Under such circumstances, the question which arises is:-

Whether, after the joint trial for an act constituting an offence under a Special Act and also under the IPC, the accused person can be convicted and sentenced under both the enactments?

To answer this question, it is pertinent to look at the provisions contained in Section 26 of the General Clauses Act:

Section 26 of the General Clauses Act reads as follows:–

"26. Provision as to offences punishable under two or more enactments. Where an act or omission constitutes an offence under two or more enactments, then the offender shall be liable to be prosecuted and punished under either or any of those enactments, but shall not be liable to be punished twice for the same offence."

The only fair and proper construction of Section 26 is that an accused person should not be made to suffer punishment more than once for the ***"same offence"***

Punishment for separate but similaroffences under two separate Enactments:

As discussed earlier, the trial of an accused for **an offence** falling within two or more **separate definitions** of **any law** in force for the time being is permitted under Section

220(3) of the CrPC.

The separate definitions may result into two situations,

firstly, when the two offences under the separate definitions are distinct and

secondly, when the two offences under the separate enactments are separate but similar, like in the case of an offence under Section 4 of the POCSO and the offence under Section 376 of the IPC.

In the first case, Hon'ble Supreme Court has held in the case of ***State of Rajasthan v. Hat Singh and Others,(2003) 2 SCC 152***, that there can be joint trial, separate convictions and separate sentences which is evident from the principles enshrined in the provisions of the CrPC.

However, in the second situation, when the offences under two separate definitions under separate enactments are similar, Section 26 of the General Clauses Act and Section 71 of the IPC read with Section 31 of the CrPC come into play.

As far as the issue of punishment in the situation mentioned hereinabove is concerned, it is pertinent to discuss the provisions contained in Section 71 of the IPC along with the provisions of Section 26 of the General Clauses Act. Section 71 of the IPC reads as follows :-

The relevant portion of Section 71 of the IPC reads as follows :-

"71. Limit of punishment of offence made up of several offences.—

…….

Where anything is an offence falling within two or more separate definitions of any law in force for the time being by which offences are defined or punished, or

……..

the offender shall not be punished with a more severe punishment than the Court which tries him could award for any one of such offences."

Where an act or omission constitutes similar offences under two or more statutes, the person committing that act or omission, as the case may be, can be prosecuted under both the laws and can also be convicted for such offences. However, as per the restrictions under Section 26 of the General Clauses Act and Section 71 of the IPC, there can be only one sentence and not separate sentences.

The principle discussed in relation to the trial of two similar offences under separate

enactments vis-à-vis Section 71 of the IPC and Section 26 of the General Clauses Act has been discussed in the following cases:-

1. ***T.S. Baliah v. T.S. Ranghachari, AIR 1969 SC 701***

6…….. A plain reading of the section shows that there is no bar to the trial or conviction of the offender under both enactments but there is only a bar to the punishment of the offender twice for the same offence. In other words, the section provides that where an act or omission constitutes an offence under two enactments, the offender may be prosecuted and punished under either or both the enactments but shall not be liable to be punished twice for the same offence.

2. Ramanaya v. The State of Bihar, 1977 Cri LJ 467

5. ……. Section 71 of the Indian Penal Code as well as Section 26 of the Central General Clauses Act talk of punishment and not of conviction. From the language of Section 35 of the Code of Criminal Procedure, 1898 (equivalent to Section 31 of the Code of Criminal Procedure, 1973), it is manifest that punishment means sentence only and not conviction. It is also manifest from language of Section 235 of the Code of Criminal Procedure, 1898 , specially from the various illustrations given in that section. There are many decisions of the Supreme Court, which need not be referred to here, where convictions for two offences for the same act have been upheld. Of course on the question of punishment, i.e., the sentence, the provisions of Section 71 of the Indian Penal Code and Section 26 of the Central General Clauses Act are relevant. **It cannot, therefore, be held that the conviction of the petitioner for one of the offences must be held bad**. (emphasis supplied)

3. Municipal Corporation of Delhi v. Shiv Shankar, AIR 1971 SC 815.

9……. Even if they happen to some extent to overlap, Section 26 of the General Clauses Act fully protects the guilty parties against double jeopardy or double penalty. This section lays down that where an act or omission constitutes an offence under two or more enactments then the offender shall be liable to be prosecuted and punished under either or any of those enactments but shall not be liable to be punished twice for the same offence. **If, therefore, the provisions of the Adulteration Act and those of Fruit Order happen to constitute offences covering the same acts or omissions then it would be open to the prosecuting authorities to punish the offender under either of them subject to the only condition that a guilty person**

should not be punished twice over. (emphasis supplied)

4. Gaya Prasad Pal @ Mukesh v. State, 2016 SCC OnLine Del 6214.

"76. The learned trial judge also seems to have overlooked **the basic precept of criminal law that a person may not be punished twice over for the same set of acts of commission or omission which collectively constitute an offence covered by two different provisions of law. Though the law permits trial on alternative charge to be held for both the offences, the punishment may be awarded only for one of them, the one which is graver in nature.** Section 71 IPC, quoted earlier, concludes with the command that the offender shall not be punished with a more severe punishment than the court which tries him could award for any one of such offences. The charge under the corresponding provision of POCSO Act (Section 4) on which the appellant has been found guilty is in addition to his conviction for the offence under Section 376 IPC. Since the circumstances attendant on the acts committed by the appellant attract Section 376(2) IPC, the punishment under the corresponding (alternative) offence under Section 4 of POCSO Act 2002 would be rendered lesser in degree in as much as, unlike the latter provision, the former - 376(2) IPC - prescribes punishment which may extend to "imprisonment for life" which shall mean imprisonment for the remainder of such person's "natural life" and "shall also be liable to fine". In these facts and circumstances, Section 42 of POCSO Act would kick in and the court is duty bound to punish the offender for the offence under Section 376(2)(f)(i) and (k) of IPC; which is greater in degree in comparison to the offence under Section 4 of POCSO Act." (emphasis supplied)

From the discussions made hereinabove, it can be concluded that when the offences are not distinct, the provisions of Section 220 permit the framing of charges for both the offences and the trial therefor. However, the limitations specified under Section 26 of the General Clauses Act and Section 71 of the IPC would be imposed and the Court, in such cases, would be empowered to impose only one sentence for both the offences.

The principle of *"generali specialibus non derogant"* will not be applicable in penal laws and, therefore, an act or omission can fall under the definition of offences under the IT Act and also under the IPC. In such cases, the FIR must be registered for both the offences and if prima facie case is made out for both the offences, chargesheet shall also be submitted for both the offences.

- The Court trying the offence is empowered to take cognizance of offences falling within the definitions of the IT Act and the IPC. If the police fails to submit the

chargesheet under both the enactments even when prima facie there appears to be an offence under both the Act, the Court taking cognizance shall not be restricted to the chargesheet and, after applying its mind, can take cognizance for offences under both the Acts.

- In cases of offences which fall within the separate definitions of the IPC and also the IT Act and are distinct, there is no restriction on the trail, conviction and sentencing in such a case. But, where the offences falling under the two Acts are similar, the provisions of Section 71, IPC read with Section 26 of the General Clauses Act shall be applicable and, in such a case, there can be a trial and conviction for both the offences but the sentence that will be imposed will only be one.

Can the offender be charged with and tried for offences both under the IT Act and the POCSO Act?

As far as the offences under the POCSO Act are concerned such as the offence related to child pornography, the same can be tried under the POCSO Act as well as under the IPC or under any other Special law including the offences under the IT Act. This provision has been specially laid down under Section 28 of the POCSO Act which reads as follows :-

28. Designation of Special Courts

(1) For the purposes of providing a speedy trial, the State Government shall in consultation with the Chief Justice of the High Court, by notification in the Official Gazette, designate for each district, a Court of Session to be a Special Court to try the offences under the Act:

Provided that if a Court of Session is notified as a children's court under the Commissions for Protection of Child Rights Act, 2005 (4 of 2006) or a Special Court designated for similar purposes under any other law for the time being in force, then, such court shall be deemed to be a Special Court under this section.

(2) While trying an offence under this Act, a Special Court shall also try an offence other than the offence referred to in subsection (1), with which the accused may, under the Code of Criminal Procedure, 1973 (2 of 1974) be charged at the same trial.

(3) The Special Court constituted under this Act, notwithstanding anything in the Information Technology Act, 2000 (21 of 2000) shall have jurisdiction to try offences under section 67B of that Act in so far as it relates to publication

or transmission of sexually explicit material depicting children in any act, or conduct or manner or facilitates abuse of children online.

Therefore, the trial for offences under the IT Act as well as under the POCSO Act has been expressly made permissible under the POCSO Act based on the principle that one penal statute does not exclude the provisions of another penal statute. Apart from this, the POCSO Act also expressly states that the provisions of the Act are supplementary to and in derogation to any other law for the time being in force but in cases of inconsistencies, the POCSO Act shall prevail.

Therefore, unless there is an inconsistency between the provisions of the IT Act and the provisions of any other law including the IPC, an offender can be charged with, tried for and convicted of an offence falling under the separate definitions of the IT Act and any other law including the IPC. In case there is any inconsistency between a provision of the IT Act and another provision of the IPC, the principle of *"generali specialibus non derogant"* will be applicable and the provision of the IT Act will prevail.

What is the procedure for trail of offences under the IT Act?

The provisions for trail of offences under the IT Act are governed by the provisions of the CrPC except in the following cases:-

Compensation

> **77. Compensation, penalties or confiscation not to interfere with other punishment.–**No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

Compounding of Offences

> **77A. Compounding of offences.–**A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided, under this Act:
>
> Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:
>
> Provided further that the court shall not compound any offence where such

offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 (2 of 1974) shall apply.

Bailable Offences

77B. Offences with three years imprisonment to be bailable.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), 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.

Confiscation

76. Confiscation.– Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

Apart from the aforementioned provisions, the provisions of CrPC are applicable *mutatis mutandis* to the trial of offences under the IT Act.

2. Procedure related to Investigation

Generally the provisions of the Criminal Procedure Code (hereinafter referred to as the CrPC) prescribe the procedure for investigation and trial of the offences. Section 4 of the CrPC lays down the following and reads as follows:-

4. Trial of offences under the Indian Penal Code and other laws.

(1) All offences under the Indian Penal Code (45 of 1860) shall be investigated, inquired into, tried, and otherwise dealt with according to the provisions hereinafter contained.

(2) All offences under any other law shall be investigated, inquired into, tried, and otherwise dealt with according to the same provisions, but subject to any enactment for the time being in force regulating the manner or place of investigating, inquiring into, trying or otherwise dealing with such offences.

Section 4(1) of the CrPC provides that offences under the IPC are to be investigated, inquired into and tried in accordance with the provisions of the CrPC. According to the provisions of Section 4(2) of the CrPC, offences under *any other law*, which includes the offences under the Information Technology Act, 2000 (*hereinafter referred* to as the IT Act), shall also be investigated, inquired into and tried or otherwise dealt with according to the CrPC, *subject to any special provision applicable under the special law. Thus the provisions of the CrPC govern the investigation, trial etc of offences under the IT Act with a few exceptions provided under the Act.* The exceptions have been contained under Section 78 and Section 80 of the IT Act. These Sections read with Section 81 of the IT Act prevail over the provisions of the CrPC.

Section 78

Section 78 of the IT Act reads as follows :-

78. Power to investigate offences.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of 1 [Inspector] shall investigate any offence under this Act.

According to the provisions of this Section, the offences under the IT Act can be investigated only by a police officer ***not below the rank of an Inspector.***

Section 80

80. Power of police officer and other officers to enter, search, etc.–

(1) Notwithstanding anything contained in the Code of Criminal Procedure,

1973 (2 of 1974), any police officer, not below the rank of a Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.–For the purposes of this sub-section, the expression —public place includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

According to this section, any police officer, not below the rank of an inspector, may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. Under the IPC, only preparation to commit dacoity and preparation to wage war against the Government are offences. In the cases of offences under the IT Act, the search and arrest is applicable even in cases where the offence under the Act is *about to be committed*. However, it is important to note here that the Section is applicable only to "public places" and not to private places.

Apart from these two exceptions given under Section 78 and Section 80, investigation, trial etc. for an offence punishable under the IT Act is to be conducted according to the CrPC. These two exceptions are however, supplementary to the provisions of the CrPC, and both the Acts are applicable unless the provisions of the CrPC are inconsistent with the provisions of the IT Act, in which case the procedure shall be governed by Section 78 and Section 80.

The police station under whose jurisdiction, the offence has been committed has the jurisdiction to investigate into the offence. Therefore, normally, the information (FIR) regarding a cognizable offence is lodged in the police station within whose jurisdiction,

the offence was committed. However, according to the Hon'ble Supreme Court in ***State of Andhra Pradesh v. Punati Ramulu*** if for some reason, the information of the cognizable offence is given to another police station, then the police should record it (known as **"Zero FIR"**) and forward it to the police station within whose jurisdiction, the offence or part of it appears to have been committed. This is more important in cases of offences related to cyber crimes especially Bank Frauds and identity theft, where time is of great importance and essence.

Which Police Station shall have jurisdiction to investigate a case related to cyber crime?

Jurisdiction of Police station in registering FIR related to cybercrime:

1. The concerned police station will have the jurisdiction to register an FIR under section 156 (1) read with section 177 of the Code of Procedure and conduct the investigation of the victim's account from which the money is withdrawn illegally.

2. In cases of economic offenses where it is not certain in which area the crime has been committed or if the crime has been committed under more than one locality or is of a consistent tendency (continuous offenses) Section 178 read with section 156 (1) Code of Criminal Procedure, can be registered in any related police station and investigation can be conducted.

Example - Money is withdrawn from the account of a person who is located in Ranchi by a criminal sitting in Jamtara and it is transferred to more than one account. There will be jurisdiction in all the places from where money has been transferred.

3. In cases where the offense has been committed in the jurisdiction of one police station and its effect will be in the jurisdiction of any other police station then the offence can be registered in either of the two police stations under the provisions of Section 156 (1) of Code of Criminal Procedure.

Example- In offences related to social media, if the objectionable post has been made the jurisdiction of a police station, and it is uploaded on the social media through the Internet, and it is seen in other jurisdictions.

4. In case the offence is a result of a criminal conspiracy. Here, where the crime has been committed or where criminal conspiracy has been done, both places can be investigated by registering the case under the provisions of Section 180 read with Section 156(1) Code of Criminal Procedure.

Example - In cases where the illegal withdrawal of funds through cyber crime has been done on more than one victim, and that amount has been transferred to a bank account of some other jurisdiction and the beneficiary is found accomplice under S. 120 IPC, then in this case the offence can be registered either in the jurisdiction of the bank account of the victim or the beneficiary and the investigation and the trial can be conducted.

5. In cases where economic communication or social media communication is done through telecommunication like internet, mobile etc., the place where the communication was made, or where it was received, the jurisdiction of the concerned police station, will be Section 182 read with Section 156(1) under the Code of Criminal Procedure.

Example: If the OTP of an account holder is obtained by criminals sitting in the jurisdiction of any other police station through mobile or telecom and internet, then both the police stations will have jurisdiction.

Necessary steps to be taken by the researcher after the registration of cases related to the cyber crime:

5. To inform the bank to stop withdrawals from the concerned account of the victim

- by phone
- by Internet, or.
- By personally visiting the nearest branch.

6. To obtain account details of the accounts from which illegal/unauthorized withdrawals have been made and the accounts in which funds have been transferred.

7. Similarly, to obtain details of the mobile or IP address using which crime has been committed such as CDR, CAF etc. from the internet service provider.

8. In this regard the following actions are required by I. O.-

(a) Obtaining attested copy of account under Section 4 of the Bankers Book Evidence Act, 1891 from the branch manager of the concerned bank.

(b) In case of non-acceptance, the above details should be sought through the concerned Court of competent jurisdiction under Section 91 of the Code of Criminal Procedure.

(c) And in such special circumstances, when the above-mentioned details is not

made available to the I.O. in due time, the concerned court can take legal action against the branch manager under Section 175 of the Indian Penal Code, 1860 by filing a separate case and then taking cognizance on it.

(d) Or

(e) For taking separate cognizance in money matters by the I.O., a complaint can also be filed under Section 195(1) (a) of the Code of Criminal Procedure, 1973 and requesting to take cognizance under Section 175 of the Indian Penal Code, 1860.

(f) If the account statement is received without verification in the order of concurrence, the prescribed verification certificate may also be obtained and presented to the court under the provisions of Section 4 of Bankers Book Evidence Act, 1891.

(g) With whom can the account statement be verified and obtained?

(h) Every branch manager or Chief Accountant is a competent officer in accordance with the provisions of Section 2(8) of the Bankers Book Evidence Act, 1891 for issuing an attested copy of the account statement.

(i) In the light of the Section 4 of the Bankers Book Evidence Act, 1891 the attested copy of the account details shall be admissible in the court of law and the bank officer issuing the same will not be required to be presented in the court as a witness. In circumstances where the account statement is obtained by computer printout it will also be mandatory to take a certificate separately under the Section 65B (4) the Indian Evidence Act, 1872.

(j) Under Section 65B (4) of the Evidence Act, 1872 the certificate must be obtained from the service provider and be filed in the Court and the prescribed procedure of Section 91 Criminal Procedure Code, 1973 must be followed to obtain the said certificate.

(k) Under Section 65B (4) of the Evidence Act, 1872 the officer issuing the certificate will not be required to be presented as a witness. The said certificate will be admissible only by identification of the investigation officer as recipient in the court.

(l) The certificate under Section 65B (4) Evidence Act, 1872 will be presented with the said CDR or electronic record as far as possible. But in the event of non-

receipt of prescribed certificate, it will be admissible by the court even during the trial.

(m) The aforesaid procedure will also be followed to obtain CCTV footage. Also, to identify the accused from CCTV footage, obtain his still photo and after getting the certified photo of the accused from jail, he can be sent to the expert for identification.

(n) Under Section 65B (4) of Evidence Act, 1872 prescribed certificates can be issued under the provisions of Section 3 of I.T. Act by putting digital signatures or signatures and seals.

(o) Where the money of the victim has been withdrawn through an account which is not verified as per KYC bank rules, then the bank officials opening the concerned account can also be charged under Section 120B of the Indian Penal Code, 1860 and where the involvement of the bank worker is found in the said crime, then the same bank worker can also be prosecuted.

(p) The persons who give their bank account and ATM for the use of cyber crime can be charged under Section 413 of Indian Penal Code, 1860 along with other sections.

(q) In cases where the victim or witness resides in any other police station area, there may be undue delay in filing their statement; in that case the investigation officer can record the statement of witness with the help of the Audio Video Electronic instrument under Section 161 of Code of Criminal Procedure, 1973. The investigation officer will mention the said statement in case diary and the will also attach the audio and video of the said statement in the case diary.

- Generally, in a case related to the illegal withdrawal of money from bank account, the case will be registered and investigated as per the provisions contained in section 156(1) read with section 177of the CrPC.

3. Examination of Witness and Recording of the Statement

Can the statement of a witness be recorded by the Police using Audio-Video Electronic medium?

Usually in cases related to cyber crimes especially those related to Bank Frauds and Identity Theft, it is a common situation that the place of occurrence, the location of the offender, the location of the witness may be at different locations. In such cases to

facilitate the process of examination of witnesses by the Police the proviso Section 161 of the CrPC permits such examination and provides as follows :-

> **161. Examination of witnesses by police.—**(1) Any police officer making an investigation under this Chapter, or any police officer not below such rank as the State Government may, by general or special order, prescribe in this behalf, acting on the requisition of such officer, may examine orally any person supposed to be acquainted with the facts and circumstances of the case.
>
> (2) Such person shall be bound to answer truly all questions relating to such case put to him by such officer, other than questions the answers to which would have a tendency to expose him to a criminal charge or to a penalty or forfeiture.
>
> (3) The police officer may reduce into writing any statement made to him in the course of an examination under this section; and if he does so, he shall make a separate and true record of the statement of each such person whose statement he records:
>
> *Provided that statement made under this sub-section may also be recorded by audio-video electronic means.*
>
> Provided further that the statement of a woman against whom an offence under Section 354, Section 354-A, Section 354-B, Section 354-C, Section 354-D, Section 376, Section 376-A, Section 376-AB, Section 376-B, Section 376-C, Section 376-D, Section 376-DA, Section 376-DB, Section 376-E or Section 509 of the Indian Penal Code (45 of 1860) is alleged to have been committed or attempted shall be recorded, by a woman police officer or any woman officer.
>
> (emphasis supplied)

Can the Court record the statement of the witness by audio-video Electronic means?

Section 273 of the CrPC requires the Court to take all the evidences in the course of trial or other proceeding in the presence of the accused and reads as follows :-

> **273. Evidence to be taken in presence of accused.—**Except as otherwise expressly provided, all evidence taken in the course of the trial or other proceeding shall be taken in the presence of the accused, or, when his personal attendance is dispensed with, in the presence of his pleader.

Provided that where the evidence of a woman below the age of eighteen years who is alleged to have been subjected to rape or any other sexual offence, is to be recorded, the court may take appropriate measures to ensure that such woman is not confronted by the accused while at the same time ensuring the right of cross-examination of the accused.

Explanation.—In this section, "accused" includes a person in relation to whom any proceeding under Chapter VIII has been commenced under this Code.

Effect of Section 3 of Jharkhand Act 2 of 2016

The Amendment proposes to amend the provision of Section 273 of the CrPC as follows :-

In its application to the State of Jharkhand, in Section 273—

(i) After the words "All evidence taken in the course of the trial or other proceeding shall be taken in the presence of the accused," the word "either in person or through the medium of electronic video linkage" shall be inserted.

The effective date for the Amendment has not been notified yet and, therefore, the provision related to the recording of evidence through Audio-Video Electronic means will be governed by the judgment of the Hon'ble Supreme Court in ***State of Maharashtra v. Dr. Prafulla B. Desai***, wherein the Court examined the question whether in a criminal trial, evidence can be recorded by video conferencing and answering the question in the affirmative, it held as follows :-

19……Thus it is clear that so long as the accused and/or his pleader are present when evidence is recorded by video-conferencing that evidence is being recorded in the "presence" of the accused and would thus fully meet the requirements of Section 273 of the Criminal Procedure Code. Recording of such evidence would be as per "procedure established by law".

20. Recording of evidence by video-conferencing also satisfies the object of providing, in Section 273, that evidence be recorded in the presence of the accused. The accused and his pleader can see the witness as clearly as if the witness was actually sitting before them. In fact the accused may be able to see the witness better than he may have been able to if he was sitting in the dock in a crowded courtroom. They can observe his or her demeanour. In fact the facility to playback would enable better observation of demeanour. They can hear and rehear the deposition of the witness. The accused would be able

to instruct his pleader immediately and thus cross-examination of the witness is as effective, if not better. The facility of playback would give an added advantage whilst cross-examining the witness. The witness can be confronted with documents or other material or statement in the same manner as if he/she was in court. All these objects would be fully met when evidence is recorded by video-conferencing. Thus no prejudice, of whatsoever nature, is caused to the accused. Of course, as set out hereinafter, evidence by video-conferencing has to be on some conditions.

21. Reliance was then placed on Sections 274 and 275 of the Criminal Procedure Code which require that evidence be taken down in writing by the Magistrate himself or by his dictation in open court. It was submitted that video-conferencing would have to take place in the studio of VSNL. It was submitted that this would violate the right of the accused to have the evidence recorded by the Magistrate or under his dictation in open court. The advancement of science and technology is such that now it is possible to set up video-conferencing equipment in the court itself. In that case evidence would be recorded by the Magistrate or under his dictation in open court. If that is done then the requirements of these sections would be fully met. To this method there is, however, a drawback. As the witness is now in court there may be difficulties if he commits contempt of court or perjures himself and it is immediately noticed that he has perjured himself. Therefore as a matter of prudence, evidence by video-conferencing in open court should be only if the witness is in a country which has an extradition treaty with India and under whose laws contempt of court and perjury are also punishable.

22. However, even if the equipment cannot be set up in court, the Criminal Procedure Code contains provisions for examination of witnesses on commissions. Sections 284 to 289 deal with examination of witnesses on commissions.

…….

Thus in cases where the witness is necessary for the ends of justice and the attendance of such witness cannot be procured without an amount of delay, expense or inconvenience which, under the circumstances of the case would be unreasonable, the court may dispense with such attendance and issue a commission for examination of the witness.

.....

> Normally a commission would involve recording evidence at the place where the witness is. However, advancement in science and technology has now made it possible to record such evidence by way of video-conferencing in the town/city where the court is. Thus in cases where the attendance of a witness cannot be procured without an amount of delay, expense or inconvenience, the court could consider issuing a commission to record the evidence by way of video-conferencing.

Therefore, in light of the decision of the Hon'ble Supreme Court, the mandate of Section 273 does not require the actual physical presence of the witnesses in the Courtroom and, therefore, the evidence of the witnesses can be taken by audio-video electronic means if the principles of Sections 273, 274 and 275 are satisfied in accordance with the judgment of the Hon'ble Court.

Can the statement under Section 313 of the CrPC be taken through audio-video electronic means?

The Hon'ble Supreme Court in ***Basavaraj R. Patil v. State of Karnataka*** considered the question - is it necessary that in all cases the accused must answer by personally remaining present in court and answered the same in the negative and hold as follows :-

> 21. But the situation to be considered now is whether, with the revolutionary change in technology of communication and transmission and the marked improvement in facilities for legal aid in the country, is it necessary that in all cases the accused must answer by personally remaining present in court. We clarify that this is the requirement and would be the general rule. However, if remaining present involves undue hardship and large expense, could the court not alleviate the difficulties. If the court holds the view that the situation in which he made such a plea is genuine, should the court say that he has no escape but he must undergo all the tribulations and hardships and answer such questions personally presenting himself in court. If there are other accused in the same case, and the court has already completed their questioning, should they too wait for long without their case reaching finality, or without registering further progress of their trial until their co-accused is able to attend the court personally and answer the court questions? Why should a criminal court be rendered helpless in such a situation?

******

23. Section 243(1) of the Code enables the accused, who is involved in the trial of warrant case instituted on police report, to put in any written statement. When any such statement is filed the court is obliged to make it part of the record of the case. Even if such case is not instituted on police report the accused has the same right (vide Section 247). Even the accused involved in offences exclusively triable by the Court of Session can also exercise such a right to put in written statements (Section 233(2) of the Code). It is common knowledge that most of such written statements, if not all, are prepared by the counsel of the accused. If such written statements can be treated as statements directly emanating from the accused, hook, line and sinker, why not the answers given by him in the manner set out hereinafter, in special contingencies, be afforded the same worth.

24. We think that a pragmatic and humanistic approach is warranted in regard to such special exigencies. The word "shall" in clause (b) to Section 313(1) of the Code is to be interpreted as obligatory on the court and it should be complied with when it is for the benefit of the accused. But if it works to his great prejudice and disadvantage the court should, in appropriate cases, e.g., if the accused satisfies the court that he is unable to reach the venue of the court, except by bearing huge expenditure or that he is unable to travel the long journey due to physical incapacity or some such other hardship, relieve him of such hardship and at the same time adopt a measure to comply with the requirements in Section 313 of the Code in a substantial manner. How could this be achieved?

25. If the accused (who is already exempted from personally appearing in the court) makes an application to the court praying that he may be allowed to answer the questions without making his physical presence in court on account of justifying exigency the court can pass appropriate orders thereon, provided such application is accompanied by an affidavit sworn to by the accused himself containing the following matters:

(a) A narration of facts to satisfy the court of his real difficulties to be physically present in court for giving such answers.

(b) An assurance that no prejudice would be caused to him, in any manner, by dispensing with his personal presence during such questioning.

(c) An undertaking that he would not raise any grievance on that score at any stage of the case.

26. If the court is satisfied of the genuineness of the statements made by the accused in the said application and affidavit it is open to the court to supply the questionnaire to his advocate (containing the questions which the court might put to him under Section 313 of the Code) and fix the time within which the same has to be returned duly answered by the accused together with a properly authenticated affidavit that those answers were given by the accused himself. He should affix his signature on all the sheets of the answered questionnaire. However, if he does not wish to give any answer to any of the questions he is free to indicate that fact at the appropriate place in the questionnaire (as a matter of precaution the court may keep photocopy or carbon copy of the questionnaire before it is supplied to the accused for an answer). If the accused fails to return the questionnaire duly answered as aforesaid within the time or extended time granted by the court, he shall forfeit his right to seek personal exemption from court during such questioning.

27. In our opinion, if the above course is adopted in exceptional exigency it would not violate the legislative intent envisaged in Section 313 of the Code.

4. Electronic Evidence

Admissibility

The Hon'ble Supreme Court, through 3-Judges Bench, in ***Anvar P.V. v. P.K. Basheer and Others***, discussed the issue of the admissibility of electronic evidence and placing reliance on the non obstante clause in section 65B of the Evidence Act, the court overruled its Judgment in ***State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru***, and held that special provision under section 65A and 65B will prevail over the general law on secondary evidence under sections 63 and 65 of the Indian Evidence Act, 1872). Therefore, for an electronic record to be admissible as secondary evidence in the absence of the primary, the mandatory requirement of section 65B certification is required to be complied with. The relevant portion of the judgment is extracted below:-

"22. The evidence relating to electronic record, as noted hereinbefore, being a special provision, the general law on secondary evidence under Section 63 read with Section 65 of the Evidence Act shall yield to the same. Generalia specialibus non derogant, special law will always prevail over the general law.

It appears, the court omitted to take note of Sections 59 and 65-A dealing with the admissibility of electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65-A and 65-B. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this Court in Navjot Sandhu case [State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 : 2005 SCC (Cri) 1715] , does not lay down the correct legal position. It requires to be overruled and we do so. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65-B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65-B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

* * *

24. The situation would have been different had the appellant adduced primary evidence, by making available in evidence, the CDs used for announcement and songs. Had those CDs used for objectionable songs or announcements been duly got seized through the police or Election Commission and had the same been used as primary evidence, the High Court could have played the same in court to see whether the allegations were true. That is not the situation in this case. The speeches, songs and announcements were recorded using other instruments and by feeding them into a computer, CDs were made therefrom which were produced in court, without due certification. Those CDs cannot be admitted in evidence since the mandatory requirements of Section 65-B of the Evidence Act are not satisfied. It is clarified that notwithstanding what we have stated herein in the preceding paragraphs on the secondary evidence of electronic record with reference to Sections 59, 65-A and 65-B of the Evidence Act, if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, the same is admissible in evidence, without compliance with the conditions in Section 65-B of the Evidence Act."

At present, the Hon'ble Supreme Court in ***Arjun Panditrao Khotkar V. Kailash Kushanrao Gorantyal and Others***, has referred the issue of the admissibility of electronic evidence and the requirement of the certificate under Section 65B of the Indian Evidence Act to a larger bench for laying down a settled principle of law. The Hon'ble Court observed

as follows :-

> 3. We are of the considered opinion that in view of ***Anvar P.V.*** (supra), the pronouncement of this Court in ***Shafhi Mohammad*** (supra) needs reconsideration. With the passage of time, reliance on electronic records during investigation is bound to increase. The law therefore needs to be laid down in this regard with certainty. We, therefore, consider it appropriate to refer this matter to a larger Bench. Needless to say that there is an element of urgency in the matter.

When is the Certificate not Required?

It was held by the Hon'ble Supreme Court in ***Shafhi Mohammad v. State of H.P.*** that the requirement of the certificate under Section 65B of the Evidence Act as per the judgment of Anvar (supra) is not required in the following two cases :-

- A party who is not in possession of device from which the document is produced cannot be required to produce certificate under Section 65-B(4) of the Evidence Act
- The applicability of requirement of certificate being procedural can be relaxed by the court wherever interest of justice so justifies.

The relevant portion of the judgment has been extracted below:-

> 26. Sections 65-A and 65-B of the Evidence Act, 1872 cannot be held to be a complete code on the subject. In Anvar P.V. [Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 : (2015) 1 SCC (Civ) 27 : (2015) 1 SCC (Cri) 24 : (2015) 1 SCC (L&S) 108] , this Court in para 24 clarified that primary evidence of electronic record was not covered under Sections 65-A and 65-B of the Evidence Act. Primary evidence is the document produced before the Court and the expression "document" is defined in Section 3 of the Evidence Act to mean any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.
>
> * * *
>
> 29. The applicability of procedural requirement under Section 65-B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce

such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In such case, procedure under the said sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in the absence of certificate under Section 65-B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate under Section 65-B(4) is not always mandatory.

30. Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65-B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by the court wherever interest of justice so justifies. (emphasis supplied)

What is the stage of filing the certificate?

Generally the certificate under Section 65B, wherever applicable must be filed alongwith the chargesheet. However, the Hon'ble Supreme Court recently in ***State by Karnataka Lokayukta, Police Station, Bengaluru v. M.R. Hiremath***, held that the failure to produce the certificate under Section 65B of the Evidence Act at the stage of filing the charge-sheet is not fatal to the prosecution and observed as follows :-

14. The provisions of Section 65-B came up for interpretation before a three-Judge Bench of this Court in Anvar P.V. v. P.K. Basheer [Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 : (2015) 1 SCC (Civ) 27 : (2015) 1 SCC (Cri) 24 : (2015) 1 SCC (L&S) 108] . Interpreting the provision, this Court held: (SCC p. 483, para 14)

> "14. Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65-A, can be proved only in accordance with the procedure prescribed under Section 65-B. Section 65-B deals with the admissibility of the electronic record. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer."

15. Section 65-B(4) is attracted in any proceedings "where it is desired to give a

statement in evidence by virtue of this section". Emphasising this facet of sub-section (4) the decision in Anvar [Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 : (2015) 1 SCC (Civ) 27 : (2015) 1 SCC (Cri) 24 : (2015) 1 SCC (L&S) 108] holds that the requirement of producing a certificate arises when the electronic record is sought to be used as evidence. This is clarified in the following extract from the judgment: (Anvar P.V. case [Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 : (2015) 1 SCC (Civ) 27 : (2015) 1 SCC (Cri) 24 : (2015) 1 SCC (L&S) 108] , SCC p. 484, para 16)

> *"16. … Most importantly, such a certificate must accompany the electronic record like computer printout, compact disc (CD), video compact disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic record sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc., without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice."* (emphasis supplied)

16. The same view has been reiterated by a two-Judge Bench of this Court in Union of India v. Ravindra V. Desai [Union of India v. Ravindra V. Desai, (2018) 16 SCC 273 : (2019) 1 SCC (L&S) 225] . The Court emphasised that non-production of a certificate under Section 65-B on an earlier occasion is a curable defect. The Court relied upon the earlier decision in Sonu v. State of Haryana [Sonu v. State of Haryana, (2017) 8 SCC 570 : (2017) 3 SCC (Cri) 663] , in which it was held: (Sonu case [Sonu v. State of Haryana, (2017) 8 SCC 570 : (2017) 3 SCC (Cri) 663] , SCC p. 584, para 32)

> "32. … The crucial test, as affirmed by this Court, is whether the defect could have been cured at the stage of marking the document. Applying this test to the present case, if an objection was taken to the CDRs being marked without a certificate, the court could have given the prosecution an opportunity to rectify the deficiency." (emphasis supplied)

17. Having regard to the above principle of law, the High Court erred in coming to the conclusion that the failure to produce a certificate under Section 65-B(4) of the Evidence Act at the stage when the charge-sheet was filed was fatal

to the prosecution. The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise.

Who is competent to issue the Certificate?

According to the provision of Section 65B 94) of the Indian Evidence Act, ***"a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities"*** is competent to issue the certificate. However, the ambit regarding the position on the persons having the authority and capacity to issue the certificate has not been settled by the Hon'ble Supreme Court. The Hon'ble Delhi High Court in ***Kundan Singh v. The State***, held that the provision refers to a person primarily responsible for the management or the use, upkeep or operations of such device which is evident from the following paragraph of the judgment:-

> 44. Sub-clause (b) to sub-section (5) is rather ambiguously uses the expression "any official" without explaining what is meant by the said term. However, when we read sub-section (4) to Section 65B, the meaning to be given to the expression "any official" emerges. Sub-clause (b) applies when information is supplied to "any official" in the course of activities carried on by him, i.e., in the course of "official" activities with a view that the said information shall be stored and processed for the purpose of the activities carried on by that officer or official. It is also elucidated that the information could be beyond or otherwise in the course of the said activities. Even in such cases the information is treated as supplied in the course of the activities of the official. We clarify that the word "official", as used in clause (b) of sub-section (5) of Section 65B, is not intended to mean or be restricted to a person holding an office or employed in public capacity. It connotes, as exemplified by the use of the same expression (albeit in its adjective form) in sub-section (4), a person primarily responsible for the management or the use, upkeep or operations of such device. It would, thus, cover a computer device containing electronic records in the hands or control of a private individual or entity.

When can the objections related to the Electronic Evidence be raised?

According to the Hon'ble Supreme Court in ***Sonu alias Amar v. State of Haryana,*** the challenge on the ground of electronic evidence can be realted to its inadmissibility or its mode of proof. In the former case, the objection can be raised at any stage. However,

in the latter case, the objection cannot be raised at Appellate stage, if the same was not raised at the time of trial. Since, the non-production of certificate under Section 65B falls under the category of "mode of proof", therefore, the same cannot be raised at the Appellate stage, if the same had not been raised at the trial stage. The relevant paragraph has been reproduced below:-

> 32. It is nobody's case that CDRs which are a form of electronic record are not inherently admissible in evidence. The objection is that they were marked before the trial court without a certificate as required by Section 65-B(4). It is clear from the judgments referred to supra that an objection relating to the mode or method of proof has to be raised at the time of marking of the document as an exhibit and not later. The crucial test, as affirmed by this Court, is whether the defect could have been cured at the stage of marking the document. Applying this test to the present case, if an objection was taken to the CDRs being marked without a certificate, the Court could have given the prosecution an opportunity to rectify the deficiency. It is also clear from the above judgments that objections regarding admissibility of documents which are per se inadmissible can be taken even at the appellate stage. Admissibility of a document which is inherently inadmissible is an issue which can be taken up at the appellate stage because it is a fundamental issue. The mode or method of proof is procedural and objections, if not taken at the trial, cannot be permitted at the appellate stage. If the objections to the mode of proof are permitted to be taken at the appellate stage by a party, the other side does not have an opportunity of rectifying the deficiencies. The learned Senior Counsel for the State referred to statements under Section 161 CrPC, 1973 as an example of documents falling under the said category of inherently inadmissible evidence. CDRs do not fall in the said category of documents. We are satisfied that an objection that CDRs are unreliable due to violation of the procedure prescribed in Section 65-B(4) cannot be permitted to be raised at this stage as the objection relates to the mode or method of proof.

5. Liability of Intermediary

Who is an intermediary?

According to Section 2 (w) of the IT Act, the term "intermediary" has been defined as follows:-

(w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;

What are his liabilities?

Under section 79 of the Information Technology Act, the intermediary is required to comply with "due diligence" standards prescribed by the Government. The Information Technology (Intermediaries Guidelines) Rules, 2011 elaborates the due diligence to be observed by the intermediary. The intermediary is required to place a privacy policy and user agreement before allowing access to its platform to any person for disseminating information. The intermediaries are also under an obligation to take down the unlawful content hosted within 36 hours of receiving 'actual knowledge'. In ***Shreya Singhal v. Union of India, (2015) 5 SCC 1***, the Apex court read down section 79(3)(b) with the effect that actual knowledge is to mean receipt of a court order/notification directing intermediaries to remove or disable access to content expeditiously. The Apex court held:

122. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject-matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

The relevant extracts of The Information Technology (Intermediaries Guidelines) Rules, 2011 are as under:

The Information Technology (Intermediaries Guidelines)Rules, 2011

3. Due diligence to be observed by intermediary — The intermediary shall observe following due diligence while discharging his duties, namely : —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation

(3) The intermediary shall not knowingly host or publish any information

or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule: (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource; (b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide

information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

What is the concept of Auto block of the unlawful content available on the website of the intermediary?

In ***Sabu Mathew George v. Union of India***, the case related to the advertisement of pre conception and pre natal determination of sex and sex selection on the internet which was against section 22 of the PCPNDT Act,1994. The writ petition was filed by the petitioner, a public-spirited person, for issue of necessary directions for the effective implementation of the provisions of the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 (for brevity "the 1994 Act"). Section 22 of the 1994 Act that occurs in Chapter VII which deals with "Offences and Penalties" reads thus:

> ***"22. Prohibition of advertisement relating to pre-conception and pre-natal determination of sex and punishment for contravention.—***(1) No person, organisation, genetic counselling centre, genetic laboratory or genetic clinic including clinic, laboratory or centre having ultrasound machine or imaging machine or scanner or any other technology capable of undertaking determination of sex of the foetus or sex selection shall issue, publish, distribute, communicate or cause to be issued, published, distributed or communicated any advertisement, in any form, including internet, regarding facilities of pre-natal determination of sex or sex selection before conception available at such centre, laboratory, clinic or at any other place.
>
> (2) No person or organisation including Genetic Counselling Centre, Genetic Laboratory or Genetic Clinic shall issue, publish, distribute, communicate or cause to be issued, published, distributed or communicated any advertisement in any manner regarding pre-natal determination or pre-conception selection of sex by any means whatsoever, scientific or otherwise.
>
> (3) Any person who contravenes the provisions of sub-section (1) or sub-section (2) shall be punishable with imprisonment for a term which may extend to three years and with fine which may extend to ten thousand rupees.
>
> *Explanation.*—For the purposes of this section, "advertisement" includes any notice, circular, label, wrapper or any other document including advertisement through internet or any other media in electronic or print form and also includes any visible representation made by means of any hoarding.

The Apex court referred to its order in Sabu Mathew George v. Union of India . The relevant extract of the order are as follows:

7. Explaining the same, it is submitted by the learned Solicitor General that all

the three Companies are bound to develop a technique so that, the moment any advertisement or search is introduced into the system, that will not be projected or seen by adopting the method of "auto block". To clarify, if any person tries to avail the corridors of these companies, this devise shall be adopted so that no one can enter/see the said advertisement or message or anything that is prohibited under the Pre-Conception and Prenatal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 (for short "the Act"), specifically under Section 22 of the said Act.

8. Mr Sanjay Parikh, learned counsel for the petitioner would contend that the Union of India should have taken further steps to see that the law of the country is totally obeyed by these three Companies, inasmuch as the commitment given by them or the steps taken by the Union of India are not adequate. He has pointed out from the affidavit filed by the petitioner that there are agencies which are still publishing advertisements from which it can be deciphered about the gender of the foetus. The learned counsel would submit that Section 22 of the Act has to be read along with the other provisions of the Act and it should be conferred an expansive meaning and should not be narrowly construed as has been done by the respondents.

****

10. At this juncture, Mr C.A. Sundaram, Mr K.V. Vishwanathan, learned Senior Counsel, Mr Anupam Lal Das, learned counsel appearing for Google India, Microsoft Corporation (I) Pvt. Ltd. and Yahoo India, respectively, have submitted that apart from the aforesaid words, if anyone, taking recourse to any kind of ingenuity, feeds certain words and something that is prohibited under the Act comes into existence, the "principle of auto block" shall be immediately applied and it shall not be shown. The learned counsel appearing for the search engines/intermediaries have submitted that they can only do this when it is brought to their notice. In our considered opinion, they are under obligation to see that the "doctrine of auto block" is applied within a reasonable period of time. It is difficult to accept the submission that once it is brought to their notice, they will do the needful. It need not be overemphasised that it has to be an in-house procedure/method to be introduced by the Companies, and we do so direct.

Thus, the Apex court adopted the approach of auto block mechanism and directed

the respondents to establish an ín house procedure to take down content punishable under section 22 of the PCPNDT Act.

Blocking of Websites

The constitutional validity of section 69A of the IT Act which deals with blocking of contents of a website was challenged in Shreya Singhal wherein the Apex court upheld its validity. The Apex court said:

> 121. It must first be appreciated that Section 79 is an exemption provision. Being an exemption provision, it is closely related to provisions which provide for offences including Section 69-A. We have seen how under Section 69-A blocking can take place only by a reasoned order after complying with several procedural safeguards including a hearing to the originator and intermediary. We have also seen how there are only two ways in which a blocking order can be passed—one by the Designated Officer after complying with the 2009 Rules and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69-A read with the 2009 Rules.

In the matter of ***Videos of Sexual Violence and Recommendations, In re***, the Apex Court received a letter bringing its attention to the existence and circulation of videos of sexual violence depicting rape, gangrape and child pornography. The Apex court directed that guidelines, standard operating procedures, as well as technology for auto-deletion of content be put in place to deal with videos, imagery, sites and other similar content in relation to child pornography (CP), rape and gangrape (RGR).

The relevant paragraph is reproduced below:

> 103. The proposals and the recommendations made on which there is consensus read as follows:

		Proposal	Recommendations
1.	(a)	The search engines expand the list of key words which may possibly be used by a user to search for CP content.	Government of India may work with the represented companies as well as civil society organisations to suggest expansion of the list of key words for showing CP warning ads/ public service message on search.

	(b)	These key words should also be in Indian languages and vernacular search.	The same may be gradually expanded to other Indian languages where applicable.
	(c)	These key words should be expanded to cover RGR content.	For RGR, the Government of India may work with the represented companies as well as civil society organisations to suggest the list of key words for RGR warning ads/ public service message.
2.		Creating an administrative mechanism for reporting and maintenance of data in India.	
	(a)	Either within the CBI, or under the aegis of the MHA, a cell must be set up to deal with these crimes.	The Committee agrees that there is a need to create a Central Reporting Mechanism (India's hotline portal), as has been done in other countries, like in the U.S. with NCMEC. Further there is a need to strengthen law enforcement in this area. Any person/organisation should be able to report any CP and RGR content in India with ease with provision for anonymous reporting. This portal may go for INHOPE membership, as an Indian Hotline.
	(b)	A hash bank for RGR content be created (under the charge and control of Ministry of Home Affairs, GoI or through authorities or NGOs authorised by it).	The Committee also agreed that there is a need to develop a centralised agency to maintain and verify the hashes of all known CP and RGR imagery.
	(c)	GoI to formulate specific parameters for identifying RGR content to ensure expeditious identification and removal;	Government may look into these for appropriate action expeditiously.
	(d)	The hashes so generated must be under the custody of the centralised cell as stated hereinabove who will take to prosecute, as per the law.	

	(e)	A reporting mechanism must be created at a Central level, preferably with the CBI (in view of their role and special access) to also receive information of any CP/RGR content being circulated in the social media or any other platform over the internet.	
	(f)	The cell would regularly engage with represented Companies and the NCMEC for updation of technology, technical support etc.	
	(g)	Technology similar to Project Arachind crawler technology be availed of, for identifying India – based CP and also to adapt the same for identifying RGR content online.	
	(h)	Content hosting platforms (CHPs), Search Engines and GoI to work together in formulating process for proactively verifying, identifying and initiating take down of all CP/RGR content.	
3.		Project CCPWC being a general project to alleviate crimes against women and children, a special focus sub-project to be created within the same for eliminating CP\RGR to undertake the following.	
	(a)	The Online Portal proposed to provide for anonymous reporting of identified CP/RGR.	Government may take action, as appropriate expeditiously.
	(b)	A separate hotline to be established for reporting (with the option for caller to remain anonymous) of identified CP/RGR content.	
	(c)	GoI to identify and authorise specific authority/ entity for receiving complaints of CP/RGR online and for initiating action thereon within specified timelines; such authority to have immunity and permission to verify CP/RGR content and to initiate take downs: authority to also have specified processes for immediately intimating respective police stations for registration of FIR and for initiation of prosecutions.	
	(d)	A team to be set up for immediately verifying such tips and to issue directions to the service providers/ intermediaries for immediate removal of such identified content.	

	(e)	Government of India team/authority to also immediately send communications to police stations concerned for registration of FIR and initiation of prosecutions. In view of the CBI's willingness to take this responsibility it is recommended that matter be handled by CBI and not by local police.	
	(f)	Government of India to create tipper list of NGOs. Tips from such sources to be acted upon immediately by GoI authority for take down and initiation of prosecution without delay.	
4.		Creation of infrastructure/training/awareness building:	
	(a)	Government of India to form regulations for reporting of identified CP/RGR imagery online.	Internet companies should provide technical support and assist in capacity building to the relevant agencies in India including law enforcement and NGOs through a series of trainings on online crime investigations, and trainings on using relevant internet tools.
	(b)	Government of India to ensure that search engines other than those already implementing URL blocks for identified CP/RGR content to initiate similar processes.	Internet companies should consider providing support to Indian NGOs to help bring awareness of these issues.
	(c)	Government of India or its designated authority/ NGOs to be extended permission/immunity for human intervention to identify CP/RGR content.	Government of India may also conduct regular training programme as well as relevant Government training infrastructure to have the latest technology on the subject-matter.
	(d)	Government of India to allocate funds for training, verification, continuous monitoring and review of personnel involved in such human intervention process for identifying CP/RGR content, in line with those adapted by NCMEC/IWF.	Government of India may also partner with civil society organisations, research institutes to conduct programme as mentioned in (c) above. Premier research institutes like IISc must be encouraged and supported to have dedicated research programme to undertake these studies.

	(e)	GoI/CHPs/search engines to involve in creation of awareness amongst users and sensitisation programs and capacity building initiatives for judiciary, prosecutors and law enforcement authorities, to mitigate the menace of CP/RGR dissemination.	
	(f)	GoI to set up processes for expeditious initiation of prosecution against users for identified CP/RGR content reported by CHPs.	
5.		The solution lies in proactively identifying rogue sites by an independent agency which can identify sites that contains CP and	The members of the Committee were of the opinion that this could be a process that could be considered for suitable implementation in India.
		RGR content and blocking these sites. To prevent the circulation of subject imagery, Government can block any additional sites/applications if they do not remove such contents of their own. MHA/ designated LEA can be empowered to directly order Indian ISPs through DoT.	
6.		The Government, through an appropriate agency setup a VPN to receive the NCMEC reports for uploading of CP from India. As conveyed by NCMEC, there were more than one hundred thousand reports belonging to India. Law enforcement agencies should initiate legal action against uploaders.	The Committee agreed that this should be looked into expeditiously.
7.		*Removal of known CP/RGR imagery:* When imagery is detected as CP/RGR, in addition to preventing subsequent uploads, content hosting platforms (CHP) voluntarily identify, remove and prevent distribution of previously existing content on their platforms.	The Committee agreed to the said proposal.

8.		There is need for greater thrust and emphasis on research & development of Artificial Intelligence (AI)/Deep Learning (DL)/Machine Learning (ML) based techniques for identifying CP/RGR content at the stage of uploading to enable real time filtering. Some specific suggestion in this regard may include as follows.	The Committee recognised the technologies developed by represented companies including PhotoDNA, Video hashing and other techniques for Imagery. However Committee also recognises the need for much greater collaborative work in the subject area amongst all stakeholders.
	(a)	Traditional DL/ML techniques, including feature engineering based techniques and other Image processing techniques to be developed for identifying CP/RGR content at the stage of uploading.	The Committee also feels that video hashing technique should also mature as has been done for hashing techniques for images. Represented companies should further voluntarily collaborate with NCMEC to establish a shared database of CP video hashes similar to the image hashes database that is already used by the industry.
	(b)	CHPs to review existing architecture to screen/ verify uploads for CP/RGR content using such AI/DL/ ML tools after suitable technologies are developed.	
	(c)	AI/DL/ML tools to be tested real time (i.e. upon each upload).	The committee suggested that suitable research be initiated for further development of technologies for identifying CP/RGR imagery.
	(d)	Research into above alternatives to be initiated in a time-bound manner.	
	(e)	CHPs to consider using NCMEC for creating deep learning/machine learning tools, subject to applicable laws, for CP (to avail of the huge data sets repository of NCMEC).	
	(f)	Government of India, along with CHPs to engage services of suitable experts for developing deep learning/machine learning tools for identifying RGR content.	
9.		*User authentication:* Create a mechanism where users who seek to upload an image/video, falling within the subject content, using the pre-identified key words, are put to a more rigorous verification process which would have them believe that they would be traced.	The Committee decided to drop this proposal by consensus.

10.		Content removal processes/URL de-indexing process for identified RGR imagery should be as expeditious as removal of CP imagery.	The represented companies stated that they are continuously working on improving processes for review of content including RGR that is reported to them. The Committee noted the same.
11.		Content hosting platforms, social media platforms and search engines will provide links for reporting CP/RGR imagery, as a specific category and the same to be more prominently displayed on their pages.	The represented companies stated that they are continuously working on improving processes for reporting content including CP and RGR that violates their policies or applicable laws. The Committee noted the same.
12.	(a)	Create a mechanism to ensure that when CP imagery is identified, the CHPs shall preserve and retain such information of the uploader including the identified content to assist law enforcement.	The represented companies are already taking action in this regard. The Committee agrees to Part (a) of proposal.
18.		WhatsApp should make further improvement in their reporting process which would enable easier reporting of contents in the App while maintaining the integrity of the contents and metadata available on phone at the time of reporting.	There was consensus in the Committee. The Committee recommends that these efforts be taken up at the earliest.
19.		Compute the PhotoDNA has, VideoHash at WhatsApp Client on Mobile Handset level, and transmit them to central WhatsApp server for matching with CP/ RGR Hashes database.	The Committee agreed not to pursue this proposal.

104. We expect the parties including the Government of India to abide by the recommendations on which there is consensus and to try and implement them at the earliest.

❑❑❑

JUDICIAL ACADEMY

LEARNING

ENDURING JUSTICE

Judicial Academy Jharkhand

JUDICIAL ACADEMY JHARKHAND

Near Dhurwa Dam, Dhurwa, Ranchi-834004

Phone : 0651-2902833, 2902831, 2902834,

Fax : 0651-2902834, 2902831

Email Id : judicialacademyjharkhand@yahoo.co.in

Website : www.jajharkhand.nic.in