Section 66-A Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,–

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages

shall be punishable with imprisonment for a term which may extend to two three years and with fine.

Struck down of Section 66-A by the Hon'ble Supreme Court of India:–

It shall be noted that this **section 66– A IT Act was struck down by the Hon'ble Supreme Court of India** in the judgement dated March 24, 2015 in a batch of writ petitions filed before it for the reasons that the terminology "grossly offensive", "menacing" "annoyance," "inconvenience," or "obstruction" given in the section is vague, the **section is coming in the way of freedom of expression provided by** Constitution of India.

The back ground of the issue is that two girls were arrested by the Mumbai police in 2012 for expressing their displeasure, by posting their remarks over their facebook profiles at the bandh called in the wake of Shiv Sena chief Bal Thackery's death. The arrested women were released

later on and it was decided to close the criminal cases against them, yet the arrests attracted widespread public protest. It was felt that the police has misused its power by invoking section 66A inter alia contending that it violates the freedom of speech and expression. The apex court judgment came on a batch of petitions challenging the constitutional validity of Section 66A of the IT Act on the grounds of its vague and ambiguous and was being misused by the law enforcing authorities.

Struck down of Section 66–A – Effects, and alterative provisions:–

Thus, in view of the Apex Court's verdict the Police shall not register cases under section 66– A IT Act. Then the question comes, what to do if such cases are reported attracting the provisions given in 66–A IT Act. For instance a female approaching the police with a complaint that a fake facebook profile was created with her identities like photograph, her name, phone number or something objectionable content is posted against her in the social networking media, and such contents have caused her insult, annoyance or harassment. In these situations the police can look for other sections in IPC or in any other special act. For the contentions above relevant section IPC may be 354–D which can be invoked for causing stalking, harassment by online means through the use of computer resources and also physical harassment despite the victim resists. Further section 509 IPC can also be invoked. According to the situation 354 –A IPC sexual harassment (making sexually coloured remarks, shall be guilty of the offence of sexual harassment) may also be relevant.

It also be noted that hither to the Police used to invoke section 66 – A IT Act for communal sensitive remarks and degrading the gods or goddesses of the different religions under this provision. After this section is stuck down the Police may have to look for the provisions 153 –A and 505 (2)

that are relevant under Indian Penal Code as per the situation, the contents of the complaint and nature of the offence.

Social networking media refer to the mode of communication among people on the cyber space with use of Internet. These include social media networking sites (Facebook), micro blogging sites (Twitter), video sharing websites (Youtube), wikis I Wikipedia) etc.

The following different variants of offences may be reported with regard to the Facebook.

- Creating impersonating profiles with the identities like name, photographs of the victim.
- Sending and posting obscene content.
- Hacking of a profile.
- Sending obscene and derogatory content to a profile.
- Posting material which hurts the feelings and sentiments of a community.

Misuse of social networking media – standard operating procedure (SOP):–

The line of investigation shall be with an aim to trace the culprit and to gather sufficient electronic evidence to establish the case, and to that effect the standard operating procedure given below may be followed.

- The contents of web pages (facebook, youtube etc) along with the URL (universal resource locator) where the alleged contents are existing may be taken as computer prints, before independent mediators so that the authenticity of existence of web contents can be proved. With this the Investigating Officer will be in position to prove that the fake profile or web pages had in fact existed at the time of offence. Otherwise, the fake profile or web pages may be deactivated / deleted by the culprit or someone else fearing legal action. In case of the Facebook profile has been deleted or deactivated at the time of complaint and if at all the victim has taken prints while it had existed such prints may be collected.

  Further the people who have seen such web pages or people who have received friend requests from such fake facebook profiles may be examined and their statements are recorded towards corroborative evidence.

  If the harassment is through e-mails the prints of all such e-mails shall be collected towards documentary proof.

  Further, if the harassment is through SMS, MMS or WhatsApp chats then a mediator report may be drafted and the description of the alleged contents may be recorded. The messages can also be collected in the form of prints by connecting the mobile to the computer or with PC suite software e.g., Nokia PC Suite, Kies, Itunes. But care shall be taken that he contents are not deleted accidentally by the IO or by the victim. If the victim is ready to hand over the mobile phone then it can be recovered before mediators and can be forwarded to FSL for further analysis.

The IO can also collect the CDRs of the mobile numbers of the victim or the accused so that further corroboration for sending the messages (SMS, MMS or harassment phone calls) may be secured. Further the customer application forms (CAF) and associated address and ID proofs of the mobile numbers of the victim or the accused may also be collected from the mobile service providers so that the ownership and possession of them is established. If the mobile numbers (SIM) are not issued in the names of the victim ot the accused the person in whose name SIM were issued may be examined as witnesses.

- The next step in the course of investigation is securing all the relevant information including IP Addresses, mobile number if any, alternate e-mail account that are associated with alleged profile or web pages from the social networking service provider for example www.facebook.com .

  At this stage the service provider www.facebook.com, if the offence is through facebook profile or e-mail service provider like Gmail, shall be contacted by sending a letters / notices (PDF Documents) through e-mails and relevant information (registration information and IP address track shall be collected. To secure such information IOs can take the help of Cyber Crime Police. While contacting the Cyber Crime Police the IOs shall identify the web address / ID of the profile that may be traced. The web address / ID is uniform resource locator (url) of the profile to be traced. The example of the same is as given under.

  https://www.facebook.com/profile.php?id=100008532245343

  https://www.facebook.com/abcxyz

  The information that is furnished by the service provider may contain phone number that was given when the profile or E-mail ID

was created, secondary e-mail and IP logs which can be used to work out further leads and clues.

- During the course of further investigation the accused can be traced through the IP Addresses and other information that was obtained from the service provider and the computer or mobile phone or any other electronic device that was used in the offence can be identified.

- Thus by working out relevant leads, clues both electronic or circumstantial the offender can be identified. Then the culprit may be taken into to custody and on questioning his confession may be elicited. At the instance of the accused and in pursuance of the confession of the accused the tool of offence i.e., computer or mobile phone or any other electronic device may be recovered.

  After the accused is caught, and the tool of the offence is a mobile phone then ascertain the password, PIN or pattern if the phone is locked, recover the phone before the mediators at the instance in pursuance of the confession of the accused, record the navigation path of the alleged contents from the sent items etc

- The process of gathering of electronic evidence will not stop there. The tool of offence i.e., computer or mobile phone or any other electronic device shall be forwarded to Forensic Science Laboratory (FSL) along with correctly drafted Letter of Advise, basing on which the expert will analyse the materiel object and retrieve relevant electronic evidence i.e., contents of profiles, web contents etc and furnish report that can be furnished to the Court to establish the case.

- The statements of service providers (Nodal Officers) who furnished IP Address logs and user details of IP addresses may be recorded

and required certificate under section 65-B Indian Evidence Act may be collected.

- Therefore the point to be noted here is that though the offence is under the provisions of the IPC the evidence to be gathered can be oral, circumstantial, documentary and electronic.
- Further, these offences are usually committed by known people to the victim with personal grudge and therefore the oral or circumstantial evidence related to the personal rivalry between the victim and the accused may also be gathered, apart from the electronic evidences as narrated above and thus the motive is also established.

What is the URL?
URL stands for Uniform Resource Locator, and is used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files). URLs have the format: protocol://hostname/other_information.

Section 66 B: Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

This is provision is parallel to 411 IPC as per which receiving stolen movable property knowing that they have been stolen is an offence,

whereas as per section 66 – B receiving stolen computers or mobile phones knowing that they have stole is an offence.

However, it shall be kept in view that the section does not confined to the physical theft, even if the resource of the computer i.e., software is received by anyone with knowledge that it was stolen then also the section applies. Thus, this section has the relevance for violation of intellectual property rights.

***