NUJS ONLINE LECTURE SERIES IN COLLABORATION WITH THE SOCIETY FOR ADVANCEMENT OF CRIMINAL JUSTICE

Date: 27.05.2020

Speaker: Dr. A. Nagarathna

Topic: Regulating Illegal Online Content

Rapporteur: Apoorv Shukla (Rapporteur)

OPENING REMARKS FOR THE SESSION:

The speaker started with terming the expression 'illegal online content' as vast and wide. She said that she will be limiting her address to some forms of online content-based offences. Especially, those which are considered illegal because of some law criminalising it or it being considered as a civil offence under some law. She said that her focus would be on criminalised versions of online content. She would try to briefly touch upon the regulation of online content through substantive and procedural law.

FUNDAMENTAL ISSUES/CHALLENGES:

- Content affecting State/Affairs of State.
    i. Online content affecting state's sovereignty, integrity and security.
    ii. Online content leading imminent threat to law and order or criminal violence like mob lynching.
- Individuals getting victimised by online contents.
    i. Women as victim.
    ii. Children as victim.
    iii. Defamatory content against an individual.
- False news affecting effective regulation of COVID-19, lack of provisions directly addressing false information about the epidemic in Epidemic Diseases Act.
- Copyright infringement.
- Deceptive advertisements.

- Liability holder for illegal online content.
- Tracing the author of illegal online content given the anonymity that technology provides.
- Sharing of illegal content inadvertently, negligently or knowingly.
- Liability of platforms on which such content is shared.
- Immediate removal of women and children related abusive content.
- Filtering of online contents by the intermediaries, allowing them to act as adjudicators.
- Intermediary guidelines continuing with the wider law framework.
- Large dependency on ISPs which are not based in India.
- Child pornography.
- Less number of convictions under Cyber Law.

VIABLE RECOMMENDATIONS/SOLUTIONS:

- Content based crimes affecting state's sovereignty get tackled under IPC, state specific organised crimes act, anti-terror law.
- Online content-based crimes leading imminent threat to law and order get covered under IPC. In states like Maharashtra, it gets covered under Maharashtra Organised Crimes Act.
- Abusive content targeting women gets dealt under Indecent Representation of Women's Act, IPC and Workplace Harassment Act. This all is in addition to the provisions of IT Act.
- Abusive content targeting children gets dealt under IPC, IT Act and POCSO Act.
- False information regarding the epidemic can be dealt under S.54 of Disaster Management Act, ordinances passed by the states which address the issue and reading S. 188 of IPC along with.
- Copyright infringement can be dealt under Copyright Act and IT Act.
- Deceptive advertisements can be dealt under IPC, IT Act and Consumer Protection Act.
- One who authors illegal online content can be subjected to criminal liability provided he can be traced.
- Depending upon nature of content shared and kind of mens rea involved, different offences can be made out.

- Remedies to get from Internet Service Providers:
    i. Directly approach the platform.
    ii. Illegal content can be brought down by presenting the court's/government agency's order.
- In case of copyright infringement, the actual owner can issue a notice to the intermediary (online platform). It has to respond to the notice within 36 hours and block the content. But, within 21 days, the owner needs to come up with a court order only then further blocking will continue.
- The court has given directions to ISPs to come up with nodal/grievance officers so that enforcement agencies can approach them to get things blocked immediately.
- When sexually abusive content relating to a child is released then there should be mandatory and anonymous reporting.
- Hashing mechanism, where the content shared on different URLs is matched.

CONCLUSION:

In India, we require better law framework with regards to sexually abusive content. At the same time, we see that there is an abuse of process in charges like sedition. On one hand, there is an abuse of legal process and on other hand the actual victim even now continues to suffer. The suffering of the victim continues because most often this happens on platforms which are not based in India. To procure convictions in such cases, evidence is required apart from getting the content blocked. Collecting data or evidence from such platforms is a difficult task. So, unless they cooperate, one would not be able to collect the evidence against these offences. As a result, number of convictions under the cyber laws in India are very low. Many a time it is difficult to get the evidence on time. Otherwise, the presence of several techno-legal challenges renders it as inadmissible. Therefore, unless we get access to the data or unless a mechanism is set in to get the information on time, regulation of such kind of content-based crime is difficult.

QUESTIONS:

The following questions were raised by the participants to which the speaker responded:

- Who should be in the role of the regulator of the online content?

  Content based crimes should be properly classified and accordingly regulatory mechanism can be made out. There should be an involvement of State in serious offences and a mechanism should be setup balances the public concerns and social media's responsibility.

- Data localisation may help the investigating agencies but it has an additional threat of trampling upon the rights of the netizens. What are your views about the same?

  To help the law enforcement agencies and to further prevent the commission of offence, an alternative to data localisation should be looked out for. Becoming a party to the regional conventions where the parties get a lot of information regarding the abusive content can be a good option.

- What happens if the content is posted not on a social media platform or a big platform but rather on a random website which is hosted in a different country?

  Any website/online platform can come under the definition of 'intermediary' in the IT Act. To make out an offence, the content needs to be 'published' on a 'public platform' even if only a single person reads it.

  The challenge arises if the platform is based in another country. You can send a notice through online mechanism but for collecting evidence, the procedure is an outdated one. The procedure is complicated and time consuming. However, the Computer Emergency Response Team (CERT) of India can help in this some of these cases. They have signed MoUs with CERTs of other countries. Sometimes, through them you may get the required information.