

By **AKSHAT KHETAN**

It is a known fact that growth in technology has changed the way social fabric has given rise to new challenges such as cyberbullying, cybercrime, cyber threats and digital harassment in India and worldwide. The internet was perceived as a safe-avenue for several, however leaving it unchecked without legal frameworks can damage individuals, citizens, enterprises, brands, institutions and even countries.

In recent years, the rising cases of cyberbullying has alarmed the legal fraternity. A 16-year old make-up artist died by suicide at the start of this year after receiving hateful comments. These comments ridiculed and disparaged the artist's gender. In Kerala, a month later, a young woman died from complications while undergoing treatment after a suicide attempt. The young lady in question was a victim of inflammatory comments on social media. According to NCERT, 35% of students in India had experienced cyber-bullying.

A WORRISOME BEGINNING AND TREND

Cyber harassment is the persistent and deliberate act of intimidating or threatening someone through electronic means. It often targets an individual's identity, safety, or dignity, and can include actions like stalking, blackmail, revenge pornography, or issuing death threats. Like cyberbullying, cyber harassment has severe emotional and psychological consequences for the victim.

India, with nearly 760 million internet users has witnessed a surge in cyberbullying. A 2020 study by the Indian Child Protection Fund (ICPF) revealed that one in four children in India were victims - girls and LGBTQ+ youth being disproportionately affected. The latest National Crime Records Bureau (NCRB) data has pointed to 50,000 cases of cyber-crime in FY21 - a 15% rise from the previous year.

In addition to the worrisome social impact, cyber-bullying and cybercrime have alarmed sectors such as banking, finance, lifestyle and entertainment. A report by Norton Cyber security, in 2021 found Indians having lost over \$6.5 billion to cyber fraud. Beyond economic loss, the country's national security is also at risk. Cyber-attacks on critical infrastructure, such as banking, healthcare, energy and corporate sectors, pose serious threats to the country's stability. Cyber-attacks on financial institutions serve as stark reminders of a nation's vulnerability and therefore it is pertinent that all kinds of digital arrests has led to the Indians lost over 1,200m rupees to "digital arrest" hoaxes between January and April this year, according to official figures.

Cyberbullying and harassment statistics may be grossly underreported around the world. Many victims fear further harassment, social stigma, and other issues in trusting authorities to take requisite action,

Among the general audience, there is a perception that online abuse can be turned off compared to physical abuse. Such a belief diminishes the urgency of implementing solutions.

LEGAL FRAMEWORK

India has several laws to address cybercrime, including the Information Technology Act of 2000 and its subsequent amendments. In 2015, the honourable Supreme Court struck down Section 66A of the IT act as a violation of free speech. However, identity theft (66C), transmission of obscene material (67) may be applied. Other legal provisions

reporting their cases. Awareness campaigns at schools and colleges will improve awareness among the young on the pitfalls of cyber-menace. A multi-faceted approach with NGOs, legal and social experts could educate individuals and workplaces on the legal remedies. Such awareness drives in legal departments and law-enforcement setups could help improve technological and legal expertise.

Often Indian courts are perceived as needing more time, in the case of Cyber-crime, cases can be expedited by empowering law enforcement. New digital infrastructure, software, and application of data and

CYBER-BULLYING

How can we legally protect ourselves?



Any cyber risk (bullying, harassment, and crime) needs to be dealt with utmost urgency. That, before the individuals and businesses get pushed into darkness.

include protection of children (POCSO), Defamation (499), criminal intimidation (503), and criminal intimidation by anonymous communication (507).

Despite laws and guidelines, victims may be disparaged owing to the complex nature of geographical boundaries, evolving nature of cybercrimes, which makes it challenging to seek legal recourse. The global nature of the internet makes it difficult to track and prosecute cybercriminals, especially when they operate from outside India. The cross-border nature of cyber-crime often leaves victims without clear avenues for justice, as laws differ between countries, and international cooperation on cybercrime is still limited. Factor of time consideration is crucial since courts may be overburdened and there may be a lack of technical expertise resulting in long delays in investigation and prosecution of cybercrimes.

3 CRUCIAL QUESTIONS

The three crucial questions that legal experts and the society should pose themselves are - ways to improve legal awareness, fast-tracking or expediting cases, and mechanisms to encourage victims from

analytical tools will improve the time to remediate such cases. Specialised cybercrime units, staffed with trained professionals, may also help in efficiently handling complaints. Besides, specialised cyber-crime tribunals could lead to faster resolution of cases. Solutions such as anonymous reporting mechanisms and access to medico-legal aid could empower victims.

The internet has become an undeniable platform to millions of Indians. The psychological effects of cyberbullying are profound. Victims often experience depression, anxiety, social withdrawal, and in extreme cases, suicidal thoughts. The anonymity that the internet provides makes it easier for bullies to continue their abuse without fear of immediate repercussions, leaving victims feeling powerless and isolated. Any cyber risk (bullying, harassment, and crime) needs to be dealt with utmost urgency. That, before the individuals and businesses get pushed into darkness.

(The author is Founder of AU Corporate and Legal Advisory Services Limited (AUCL))