
Cyber Crime Against Women In India

*Bhagyashri V. Neware, Maharashtra National Law University, Aurangabad.**

Abstract

In the digital age, Information and communication Technology (ICT) is benefiting billions across the world by bridging certain gaps and multiplying human potential in every walk of life. Digital services provision that is being developed for our society has enormous positive potential. The internet has revolutionized the way businesses approach and conduct work. In the social media platforms as a major cause of increasing cyber-crimes against women in the Indian society. the legal remedies available under various piece of legislations dealing with the menace of cybercrime have been focused upon. The role of government in the current legal scenario and the accountability of the government is also discussed in detail. The paper concludes by considering the loopholes in the system, that neither the provisions of the Indian Penal Code, 1860 nor the Information Technology Act, 2000 satisfactorily deal with such offences and fail to provide adequate safety measures to curb the same.

***Keywords** :- Cybercrimes, Information Technology, Legal Remedies, India, women.*

* She is pursuing LLM. from Maharashtra National Law University, Aurangabad.

I. Introduction:

“Cybercrime is as any activity that uses the internet to commit a crime”

- *Milhorn*

India is developing rapidly and one of the major factors contributing to its own growth is the technological advancement. The idea of a modern India has had a strong focus on science and technology for its all-inclusive development. Cyber Crime is a global phenomenon. ‘Cyber’ is a prefix used as to describe a person, thing or idea as part of the computer and information age. In the Greek word “Kybernetes” for ‘steersman’ or ‘governor,’ it was first used in cybernetics, a word coined by the Norbert Wiener and his colleagues.

The virtual world of internet is known as the cyberspace and laws governing this area are known as cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter networked information technology. In short, cyber law is the governing computers and the internet. The day-to-day life, cybercrime is increasing rapidly. In the cybercrime with the help of internet, e-mail, chatting, online gambling etc. they are various ways to performing a cybercrime.

Cybercrime in broader sense means any illegal behavior by means of, or in relation to a computer system or network including such crimes as illegal possession and offering or distributing information by means of computer system. As the Tenth United Nations Congress on the prevention of Crime and treatment of offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

- a. ***Cybercrime in a narrow sense(Computer Crime):*** any illegal behavior directed by means of electronic operations that target the security of computer system and data processed by them.
- b. ***Cybercrime in a broader sense (Computer- related Crime):*** any illegal behavior committed by means of, or in relation to, a computer system or network including

such crimes as illegal possession [and] offering or distributing information by means of computer system or network.

The OECD Recommendation of 1986 included a working definition as a basis for the study:- computer- related crime is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data.

In the year of 1820, they found firstly in the cybercrime, that is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 BC. In India, Japan, China. The time of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph Jacquard, a textile manufacturer in France, produced the loom. This allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cybercrime.

II. Cyber Crime Against Women

In the recent time, the cybercrime of women is familiar. In India, the women are trapped by cybercrime in every second victimization through the internet. Technology is the resource used by some criminal who target to defame women by sending obscene emails, What's app messages, stalking women by using websites, chatting, dating app, and worst all by the developing pornographic videos, mostly without any consent they make clips and viral on internet sites. In an cybercriminal use computer technology to access personal information and use internet for harassment, blackmailing, extortion, etc. in cybercrime mostly in the social media like what's app messenger, Facebook, twitter, Instagram causing harmful for women, as though they mostly blackmailing, threatening, cheating with these platforms. In the cybercrime is malafide intension to take some men are revenge for women they are used for insulting them. In the cyber world is very humanoids in nature.

III. Various Kinds Of Cyber Crime Against Women

Amongst the various cybercrimes committed against individuals and society at large, crimes that are specially targeting women are as follows,

- i. Cyber stalking
- ii. Cyber bullying
- iii. Cyber defamation
- iv. Harassment via e-mail
- v. Email spoofing
- vi. Morphing
- vii. Cyber pornography
- viii. Online Trolling
- ix. Voyeurism
- x. Cyber flirting
- xi. Privacy Infringement

A. **Cyber Stalking** : In the cybercrime is found mostly is the cyber stalking. In the cyber stalker with the help of social sites. Stalking in the internet happens when the perpetrator follows the victim continuously by leaving unwanted messages. The stalker disturbs through private emails as well as public message also. The stalkers are :-

- Sexual harassment
- Obsession for love,
- Revenge and hate,
- Ego and power tips.

B. **Cyber Bullying** : Cyber bullying which means to that the use of electronic communication to bully person, typically sending messages of an intimidating or threatening in nature¹. The main aim and object behind the such crimes may be to defame the target of an anger, revenge, hatred

¹ According to Oxford Dictionary.

or frustration takes place. In the *United States Vs. Lori Drew (2006)* is one of the example of cyber bullying. In this case a 13year old girl got a message on Internet, “the world would be better off without you” and took it her heart. She had not met the person who sent this message but only after twenty minutes she hung herself. The story turned to b more terrific when it found that the person was just a creation of some Lori drew, who was arrested in 2008 for violating the fraud and abuse act but unfortunately was acquitted in 2009. The social network like Orkut, Facebook can be considered the main source of cyber bullying.

C. **Cyber Defamation** : Cybercrime that includes defamation is another common internet crime against women. Even though It can happen to both genders but specially women are suffered mostly. In the cyber defamation generally takes place when someone publishes defamatory information or sends defamatory messages or emails about someone with the help of computer or the internet publicly. Unfortunately, cyber defamation is not defined by the IT act, 2000 and it is treated by the criminal justice system under the same provisions of cyber pornography or publication of obscene materials in the internet.

D. **Harassment via mail**: Harassment via email is form of harassment, which includes blackmailing, threatening and constant sending and love letters in anonymous names or regular sending of embarrassing mails to one’s mail box. Indian Penal Code, Criminal Procedure Code and Information of Technology act deal with the protection of cybercrime. After the Amendment of 2008 new sections are inserted as Section 67A to 67C , Section 67A and Section 67B insert penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 67C deals with the obligation of any intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central as the Central Government may prescribe. These provisions do not mention anything about e-mail harassment of different type but in general they are used to book the perpetrators along with Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under section 509 of the IPC for uttering any words or making any gesture intended to insult the modesty of women. In such cases the victim goes to the police station to report the crime of harassment and thereby it is regulated as per the general laws and not by the provisions of cyber laws. The issues related to publication or transmission of obscene

information in electronic form under section 67 of IT act, 2000 may be looked from the perspective of 'extra- territorial' jurisdiction. With the advancement of technology that obscene is no longer a local phenomenon. It is now global and dynamic in nature and thus needs strict interpretation of statutes.

E. E-mail Spoofing : E- mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appeared as through email originated from a different source. By changing certain properties of the email, such as the form, return path and reply- to fields, ill-intentioned user can make the email appear to be from someone other than actual sender. Email spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow an authentication mechanism. One of the best examples of Cyber Spoofing is Gujrat Ambuja's Executive Case, in this case the perpetrator pretended to be a girl for cheating and blackmailing the Abu Dhabi based NRI.

F. Morphing: When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads then after editing is known as morphing. It was observed that the female's pictures are more downloaded by the fake users and reposted after editing. This crime is done for the purpose of blackmailing or cheating the victim's online intended to take revenge or defame them.

G. Cyber Pornography : Internet may be considered the facilitator of crimes like cyber pornography, women and children are becoming the main victim of this flip side of technology. cyber pornography is another threat to the female netizens. This includes pornographic websites containing porn photos and porn videos and their transmission. Internet has provided a platform for the facilitation of crimes like pornography. About 50% of the websites shows pornographic and obscene material today. Females of the society are being threatened on the name of pornographic sites to get sexual favours or to take revenge from them. These offences mainly include morphing of photos with nude photographs and uploading them to pornographic sites. The easy availability and access to these sites has led to more serious offenses in the cyber world. Recently, the *Air Force Bal Bharati School Case (Delhi)*² is a recent case comes under

² Air Force Bal Bharti School & Anr. V. Delhi School Tribunal & Ors. On 16 January, 2013.

this category where a student of the school was teased by all his classmates for having a pocked face. He, who is tired of the cruel jokes, decided to get back at his tormentors and scanned photograph of his classmates and teachers, morphed them with nude photographs and put them upon a website that he uploaded on to a free web hosting service. The father of the class girl featured on the website came to know about this and lodged a complaint with the police.

- H. Online Trolling* : Trolling means posting a proactive or off- topic messages in online community such as newspaper, blogs, social media(Twitter, Facebook, Instagram) which mainly targets the females intending to emotionally upset them. It is done by the trolls who are professional abusers who create a scene of cold war by creating fake ids and using them for this purpose.
- I. Voyeurism* : The cybercrime voyeurism is committed when any man watches or captures the image of a women engaged in private act in circumstances where she has the belief of not being observed either by the perpetrator or any other person but those images used to be disseminated.
- J. Cyber Flirting* : Generally cyber flirting may be considered very minimal petty offence that starts when perpetrator force the victim to hear obscene songs, messages and it may consequently result in cyber sexual defamation and breach of thrust. Again, this can be treated as the flip side of IT act that except section 72 which deals with the breach of confidentiality and privacy there is no other supports that can be offered by the act to the victim.
- K. Privacy Infringement* : Privacy infringement generally means the violation of privacy of any individual. It means taking photographs, making videos, records, private pictures and publishing them or sending them electronically to anyone without the consent of the individual. Any violation of the privacy is punishable and legal action can be taken against of it.

IV. Relevant Case Laws :

A. Ritu Kohli Case

In the case of Ritu Kohli Vs. Rajesh Kohli³ on 1 August, 2018. It was the first reported by cybersex crime in India. It was Reported on Sunday, June,18,2000 in Delhi. In this case a 30year-old- software engineer, Manish Kathuria arrested by officials of the crime branch of the Delhi Police for harassing a women by chatting on the internet. Manish reportedly used to chat on a website under the name of Mrs. Ritu Kohli he used obscene languages while chatting and also gave her residential telephone number for further chatting. As a result, Mrs. Kohli started from obscene calls at her residence. Due to the disturbances, Mrs. Kohli lodged a complaint after the enquiries the Delhi police traced the culprit started criminal proceeding against him under section 67 of the IT act with Section 509 of IPC for outraging Ritu Kohli's modesty.

B. *State Of Tamil Nadu Vs. Suhas Katti*

This is the case related to the posting of obscene, defamatory and annoying messages about the divorcee women in the yahoo message group. Emails were forwarded to the victim by the accused through a false email account opened by him in her name. the posting of the messages related in online harassment to the victim as annoying phone calls stated coming to her in the belief that she was soliciting. Therefore, she lodged a complaint in the Egmore court in February 2004. Based on the complaint, the Chennai police cyber cell traced and arrested the accused. Further the accused found guilty of offences under section 469/509 of IPC and section 67 of the IT Act, 2000 and convicted⁴.

³ Ritu Kohli V. Rajesh Kohli on 1st August, 2018.

⁴ State of Tamil nadu V. Suhas Katti, C.No. 4680 of 2004.

C. Puri Cyber Pornography Case

This was the first pornographic case in Odisha. The accused Jayant Kumar Das, RTI activist created a fake e-mail account and fake profile of the wife of the complainant Biswajit Patnaik, a journalist to take revenge on him. He linked the fake profile to an America based porn website and posted vulgar remarks. He also posted the victim's phone number on the porn portal. Later, the journalist lodged on FIR against Das at Baselisahi Police station in Puri in July 2012 after getting obscene messages and phone calls. The cyber cell of the crime branch took over the investigation in August 2012 and arrested Das on September 18, 2012. The Puri Sub-Divisional Magistrate Court convicted RTI campaigner Das in a Cyber Pornography case to 6 year's imprisonment under the section 292 (obscenity), 465(forgery), 469(forgery for the purpose of harming reputation) and 500 (punishment for defamation) of the IPC and 66C/67/67A of the Information Technology Act, 2000.

D. Karan Girotra V. State & Anr⁵

This case was reported on 8th may 2012 on cyber stalking when the petitioner filed an application to grant anticipatory bail. This case dealt with a women, Shivani Saxena, whose marriage could not be consummated and she filed a divorce with mutual consent. In between, she came across Karan Girotra while chatting on the internet, who told her that he loved her and wanted to marry her. Girotra invited Saxena over to his house to introduce her to his family where he intoxicated her and sexually assaulted her. He started assuring her that he would marry her and began sending her obscene pictures of her assaultation. He also threatened her to circulate the pictures if she would not marry him. As a result, an engagement ceremony was performed after which he continued to assault her and called off his engagement to her.

⁵ Karan Girotra V. State & Anr. On 8 May, 2012

Frustrated out of this, Saxena filed a complaint under section 66A of the IT Act. Although the court rejected the plea of anticipatory bail but did not give serious custodial interrogation.

E. Dr. Prakash Vs. State Of Tamil Nadu⁶

It is the first case to be prosecuted under IT Act in the state of Tamil nadu. The case is a big scandal, involving sex, pornography, the internet and a mastermind, allegedly a medical doctor. Doctor was involved in the offences of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to 23 countries, spoiling life of many young girls, who was then kept to detention. The story revealed when the city police received a complaint from Ganesh who claimed to be a victim of the doctor. Two cases got lodged against the doctor; one under Information Technology act and the other under Arms act. As per section 67 of the IT Act, that deals with obscenity, the sentence can be of 5 years imprisonment with a fine of Rs. 1000 on the first conviction and penalty may extend up to 10 years imprisonment with a fine of Rs. 2 lakhs on the second conviction. Presently, six terms of police are working day and night to gather more information related to it⁷.

V. Law Enforcement

In the various laws have been protected to the women's protection of crime they have some laws are there:- Information Technology Act, 2000(amendment act 2013) and Indian Penal Code, 1860.

⁶ Dr. Prakash Vs. State of Tamil Nadu AIR 2002 SC 3533

⁷ P. Oppili, first case to be prosecuted under IT Act, THE HINDU (Jan 05, 2002), www.thehindu.com

I. INFORMATION TECHNOLOGY ACT, 2000

- a. Section 66A :- Any person who sends offensive messages through communication services that causes annoyance, inconvenience, danger etc. through an electronic device to mislead or deceive the recipient about the origin of such messages is liable for the punishment of imprisonment up to 3 years with fine.
- b. Section 66C :- Any person dishonestly makes use of the electronic identity such as signature or password of any other person, is liable for the punishment of imprisonment which may extend to 3 years with fine which may extend to rupees 1 Lakh.
- c. Section 66D :- Any person who by means of any communication device or computer resource cheats by personation is liable for the punishment of imprisonment which may extend to 3 years with fine which may extend to rupees 1 Lakh.
- d. Section 66E:- Any person who intentionally or knowingly captures, publishes or transmitters the image of private area of any person without his or her consent is liable for the punishment of imprisonment which may extend to 3 years or 2 Lakh fine or with both.
- e. Section 67 :- Any person who publishes or transmits any obscene material in the electronic form is liable for the punishment which may extend to 3 years and with fine which may extend to 5 lakh rupees or first conviction and imprisonment which may extend to 5 years and with fine which may extend to 10 Lakh rupees on second conviction.
- f. Section 67A :- Any person who publishes or transmits any material which contains sexually explicit act in electronic form is liable for the punishment which may extend to 10 Lakh rupees on first conviction and imprisonment which may extend to 7 years and fine which may extend to 10 Lakh rupees on second conviction.
- g. Section 72 :- Any person who illegally discloses any electronic information or other material which contains personal information of that person without the consent of that person to any other person is liable for the punishment of imprisonment which may extend to 3 years or with fine which may extend to 5 lakh rupees or with both.

II. INDIAN PENAL CODE, 1860

- a. Section 354 : Assault or criminal force to women with intent to outrage her modesty :- Whoever assaults or uses criminal force to any women, intending to outrage or knowing it to be likely that he will thereby outrage her modesty, [shall be punished with imprisonment of either description for a term which shall not be less than one year but which may extend to 5 years, and shall also be liable to fine.]⁸
- b. Section 354 C : Voyeurism :- Any man watches, or captures the image of a women engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.
- c. Section 354D : Stalking :- (1) Any man who-
- d. Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- e. Monitors the use by a women of the internet, email or any other form of electronic communication,
- f. commits the offence of stalking:
- g. Provided that such conduct shall not amount to stalking if the man who pursued it proves that-
- h. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state; or
- i. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
- j. (2) whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to 3 years, and shall also be

⁸ Subs. By act 13 of 2013, sec.6, for “shall be punished with imprisonment of either description for a term which may extend to 2 years, or with fine, or with both”

liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

- k. Section 463 : Forgery :- [whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.
- l. Section 471 :-Using as a genuine a forged [document or electronic record] :- whoever fraudulently or dishonestly uses as a genuine any [document or electronic record] which he knows or has reason to believe to be a forged [document or electronic record] , shall be punished in the same manner as if he had forged such [document or electronic record].
- m. Section 499 : Defamation :- Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected to defame that person.
- n. Section 500 : Punishment for Defamation :- Whoever defames another shall be punished with single imprisonment for a term which may extend to two years, or with fine, or with both.

VI. Reasons For The Growth Of Cyber Crime Against Women In India

The expansion of the technology is a positive aspect that can be regarded as an essential factor for the development of any country but simultaneously it is becoming the platform to escalate the crime rate with the advancement of technology against the weaker section of the society. the main victim of these crimes uses to be women. The reasons for the increasing rates of these crimes are as follows:-

- Most of the cybercrimes remains unreported due to the unwillingness and risk of the social embarrassment and social stigma.
- They do not take any ingenuity to report such crimes because of the terror of defamation of the victim and her family.
- The Patriarchal society existing in India, that inspires the victims to compromise to maintain peace and keep away the further conflicts in the family.

- There are no such specific laws conscious for the offences committed in the cyberworld against women.
- There is a lack of awareness among the females of the society as to where to report such crimes.
- Lack of vigilance from the part of the owners of the websites to observe what is going on their sites.
- The judicial system of India is painfully slow, which is a major threat to the society as it does not provide justice at the proper time.
- The National Crime Record Bureau (NCRB) does not maintain any separate records of the cybercrimes committed against females.

VII. Motives Behind Cybercrime Against Women

The motive behind any of the cybercrimes committed is the malafide intention of the cyber criminals who take use of the technology carry out their plans. Some of the motives behind the cybercrimes against women are as follows :-

- Financial Profit :- Alike so many offline crimes, the main motive of cybercrimes is to gain monetary profit. The cyber criminals usually demand money by threatening or blackmailing the victim to post their private pictures or videos captured by them with the use of different online identities.
- Sexual Motives :- The weird sexual behaviour is illicit and it is considered harmful. Lots of people watch porn sites to fulfill their wrong desires and lust which impulses the cyber criminals to post on pornographic sites subsequently increasing cyber pornography.
- Entertainment Purpose :- unlike cybercrimes, cybercrimes against women are done for the purpose of fun and entertainment by the use of internet.
- Emotional Motives :-Internet is also misused by the cyber criminals outraged of anger because of love failure or someone who feels cheated to take revenge as the chance of their plans and tricks being caught often gets reduced.

VIII. How To Register A Complaint Using The National Cyber Crime Reporting Portal?

Most women, at some point in time, have been victims of cybercrimes. But, they often do not file a complaint against the crime due to fear of social retribution or lack of awareness. The government has initiated a National Cyber Crime Online Portal to file a complaints against criminals. Such complaints may also be filed anonymously. The government initiated this portal to create awareness about cybercrimes and also give complaint without any fear.

IX. National Cyber Crime Reporting Portal

Government commissions and schemes that create awareness about the cybercrimes against women and children are as follows :

- National Commission for Women,
- Cyber Crime Prevention against Women and Children

X. Suggestions

- Don't share passwords with your trusted friends or partner as it is riskier to share passwords which may cause harm. Keep passwords secret and complex.
- Don't share intimate messages or pictures to anyone, no matter how much trustworthy that person is. Be cautious as it may be unsafe and sometimes can be used to harass you.
- Never go to meet the friend, you met online alone as it can be risky and may cause change. Make sure to meet that person in a very populous place.
- Never accept friend requests from unknown person and don't feel weird in rejecting those friend requests on any of the social media.
- Block the people with the whom you don't want to interact as safety comes first. In any point of time if you feel something fishy just block them immediately.
- If there is any cybercrime, go and report it instantly as the procedure for reporting of any other offences.

- The law enforcement systems in India should be well equipped to deal with cybercrimes against women.
- The Indecent Representation of Women Prohibition Act, 1986 is the only gender specific act mentioned in the legislation. Some more gender specific act should be amended under the IT Act, 2000 to prohibit cybercrimes against women.
- The National Crime Record Bureau should maintain a separate record of the cybercrimes registered against women.

XI. Conclusion

India is considered as one of the very few countries to enact IT Act, 2000 to combat cybercrimes; This act is widely covered commercial and economic crimes which is clear from the preamble of the IT act but it is observed that there is no specific provision to protect security of women and children. Cybercrime against women in India is at its developing stage and growing at a large level very quickly. The chief problem of cybercrime lies in the modus operandi and the persistence of the cybercriminals. The judiciary along with the police department and the investigative agencies should be boosted up with the modern web-based applications in order to be a step ahead from such perpetrators. It is the job of the legal system and regulatory agencies to keep pace with the technological developments and ensure that newer technologies do not become tools of exploitation and harassment.

Governments can take legislative measures that ensure human rights; especially women's rights are protected online just as they are physical spaces. Legislations should not just protect users; however, it should also educate and inform all groups on how to exercise their communication rights. Moreover, individuals should be more aware online as well as offline with regards to the precautionary measures in the cyber space and the remedies available if their right is violated. Though there used to be several difficulties in dealing with cybercrimes such as loss of evidence and lack of cyber army but with the Criminal Law Amendment Bill (2013) most of these problems have been taken care.

However, several changes are still needed such as cyber savvy judges. It can be stated that proper implementation of laws along with public awareness and education of women concerning their rights and legal remedies can play a crucial role in eradicating cybercrimes from our society. Enacting of laws cannot be the only recourse available to curb such crimes. Also, only looking from the angle of protection of the social mores would also not suffice. The digital technology has grown faster than the laws governing the technology. Hence the existing laws fall short to tackle the situation. The menace of cyber-crime extends not only to India, but is widespread across the planet. Hence, there is a need for coordinated and integrated effort on part of the world community. Additionally, grievance redressal mechanisms and institutions should be vitalized and popularized, with the ease of lodging complaints and minimizing delay in investigation and prosecution as major objectives.