

Comparative Analysis of Cybercrime against Women in India, UK and USA

Pooja Pandey
Research Scholar,
Faculty of Law
University of Allahabad.

Abstract

The internet has made the world a smaller place. But with everyone being on the internet, the crimes that were prevalent in physical reality have now also become possible in the cyber space. One of these problems being harassment and stalking of women; with the advent of technology, a person sitting thousands of miles away is still able to monitor the activities of an individual and harass them. The problem that is posed to the judiciary in this situation is how one would deal with a problem that could potentially be international with perpetrators and victims being several countries apart from each other. This paper focuses on legislations regarding cyber-laws for protection of women in three countries, namely, U.K, U.S.A and India. The objective is to engage in a discussion regarding how these three countries define and punish cyber-crime in specific regard to women.

1. Introduction

Deviance from the commonly followed principles of society is not an uncommon occurrence. Society has had instances of social deviancy for as long as it has lived; When the social rules were not codified in forms of laws, acts of deviancies tended to elicit responses of disapproval, with the more serious acts of deviancy resulting in the perpetrator being ostracized or the victim being allowed some form of payback. The laws in place today are essentially codification of the same principles universally followed and the acts of deviancy from those laws are labeled as 'crimes'. So if the crimes are acts which are deleterious to the society by way of deviation from universally acknowledged rules of the land. Cybercrimes are the same crimes perpetrated on a cyber space with the addition of crimes which are also unique to the cyberspace, such as hacking, publication of obscene material etc.

This paper would not be dealing with the entire field of cyber law since the concept, while nascent, is still extensive to be dealt in the scope of one paper; instead, it will be dealing with the Cybercrime perpetrated against the women.

Working to halt online abuse, an online organization working to combat cyberspace abuse, receives from 50-75 cases every week, based on that they made a cumulative paper on the cases reported from the year 2000-2013 and percentage of each gender who were the victim. Out of the 4043 reported cases worldwide, 70% of the victims were women.¹The European Institute for Gender Equality states that one in ten women have already experience some form of cyber violence since the age of 15.²

There is a famous argument that men are the majority victims in other kinds of crime such as robbery, theft, murders. Now, while that argument does factually hold true, one needs to look beyond the numbers as well. In the other crimes, the men are victims for a number of reasons; reasons ranging from their economic status to being at the wrong place at the wrong time, but when you look at the crimes of rape, harassment or abuse being perpetrated against the women, most of these crimes originate from the same mens rea: the intent to claim power over the women who have long been considered the disadvantaged groups of society. Since the advent of settlement in humanity, women have been considered to be the less abled gender of the society, and therefore have mostly been treated more as property than human beings. In the medieval times, men actually raped women from affluent families to be able to marry them and then get some of the fortune the family carried.³

While physical crimes are kept in check due to the extensive substantive laws prohibiting not only the commission of those crimes but also even the manifestation of the intention to commit those crimes, the cyberspace, being a new advent of socialization, is largely left untouched with few authorities acting as watchdogs for crimes perpetrated on it. One of the most affected groups due to this lack of legal jurisprudence, are women; laws are well established to protect a women from physical harassment in any form, but protection of them from the same harassment

¹ Comparison Statistics 2000-2013, available at: <http://www.haltabuse.org/resources/stats/Cumulative2000-2013.pdf>(Last visited on December 8th, 2019)

² Cyber Violence against Women and Girls, available: <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls> (Last Visited on December 20th2020.)

³Larry J. Siegel, *Criminology: Theories, patterns and typologies* (Cengage Learning, Boston MA, 2013).

perpetrated through the cyberspace is quite flimsy, for example, in India, there is no law punishing a foreign national from distributing pornographic distorted pictures of women.

This paper aims to look at the methods of dealing with cybercrimes against women in three countries, namely UK, U.S.A and India. While India is a developing country with the Internet coming into the country at around 1995, USA and UK are developed countries. This paper will study the laws in these two countries and compare it with India's jurisprudence to hopefully come to a conclusion regarding what can be changed in our jurisprudence to better protect the women of our country.

1.2 Major forms of cyber harassment against women

There are namely two kinds of crimes perpetrated against women in the cyber space:

Cyber Harassment:

The European institute for gender equality defines 'cyber harassment' as *any form of harassment by the means of email, text (or online) messages or the internet.*⁴ It further states that the such harassment can take the form of unwanted sexually explicit messages, inappropriate advances on social networking websites, threats of physical or sexual violence through these social media websites and hate speeches or messages target the victim's identity (usually women end up being the victims) and other traits such as sexual orientation.⁵ In India, even though cyber-harassment laws have been in existence since 2000 with the Information technology act, cyber space crimes are rarely reported.⁶ In fact, one of the first cases of cyber-harassment laws being used are from 2001 where the alleged perpetrator was arrested due to impersonation of the victim and disclosing her number along with publishing obscene material under her name resulting in calls being received by her from strangers asking her to perform obscene acts.⁷ The case initially hit a hurdle when the accused was charged under section 509 of the Indian Penal Code; it was

⁴Cyber Harassment, available at: <https://eige.europa.eu/thesaurus/terms/1486> (Last visited on December 21st 2019)

⁵Supra.

⁶ Why Online Harassment Goes Unpunished in India, available at: <https://www.bbc.com/news/world-asia-india-33532706> (Last Visited on December 22nd 2019)

⁷ V.M Eshwar and Aswathy Ranjan, "A Critical Analysis in Relation to Cyber-Law- An Indian Perspective", Volume 119, *International Journal of Pure and Applied Mathematics*, p.no.: 1489-1501 (2018)

found that since section 509 only dealt with physical outrage of modesty, the contents of the sections could not be applied to the case at hand. The case eventually fizzled out when the victim chose to leave the country out of sheer frustration.⁸ The case did alarm the central government to such an extent that they introduced section 66 to the Information Act, 2000 which made it a punishable offence for any person to:

send, 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 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,"

This section was, however, declared ultra vires of the constitution and was struck down by the Supreme Court,⁹ due to the provisions of the sections being outside the purview of reasonable restrictions that could be placed on freedom of expression enumerated in Article 19 of the India Constitution.

Cyber Stalking:

Section 354D of the India Penal Code,¹⁰ inserted in 2013,¹¹ defines stalking as:

“Any man who-

- (i) 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*

⁸ Supra No. 6

⁹ *Shreya Singhal v. Union of India*, W.P (CrI.) No. 167 of 2012

¹⁰ Indian Penal Code, (Act 45 of 1860)

¹¹ Inserted by Act of 2013, s. 7 (W.R.E.F. 3-2-2013)

- (ii) *Monitors the use by a woman of the internet, email or any other form of electronic communication.”*

This section was added as a preventive measure to the Ritu Kohli case and to bring the crime of stalking done over cyber space within the ambit of the stalking which was legally always punished as a physically perpetrated offence.

Apart from these two forms of cyber-crime, there exist many more, such as cyber pornography or trolling, but they essentially are a subset of cyber harassment and are therefore covered under cyber-harassment.

The three countries focused in this paper deal in various ways. While all three countries have enacted legislation to govern activity in the cyber space, all three countries are legally structured different from each other and therefore deal with crimes also in a different way.

2. U.K legislations for cyber-crime against women

The cyber law in U.K is governed by the provisions of several laws with some offences being punishable under the ambit of several laws. Apart from the laws, one thing the UK also legally excels in is the presence of a protocol in case of sensitive situations of harassment and stalking. In case of stalking, there is a proper protocol the Crown Prosecution Service and NPCC (National Police Chiefs' Council) follows to ensure that along with serving justice upon the true perpetrator, the victim is also given support and referred to support organization in case of any trauma from the crime.¹²

Section 1(2) of Protection from Harassment Act 1997 defines harassment in the contextual understanding of the victim in the case, it reads; *“For the purposes of this section or section 2A (2)(c), the person whose course of conduct is in question ought to know that it amounts to or involves harassment of another if a reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other.”*

¹²Stalking and Harassment, available at: <https://www.cps.gov.uk/legal-guidance/stalking-and-harassment> (Last Visited on December 26th2019).

So UK does not follow any particular definition of harassment and depends on the reasonable person test to declare a particular act an act of harassment. This helps the law to adapt to the changing times, so while this law was made in 2005, the internet had not yet become an everyday part of the society's life, but now in 2019 the law still protects all the online victims of harassment since the definition of harassment is not tied to any particular act to be committed but on the reasonable individual of the society to believe that it was harassment. The law therefore binds itself to the conscious of the current society and not to tally of whether the acts stipulated were committed or not.

Similarly, stalking is covered under the provisions of Protection of Harassment Act, 1997. While the act does not adopt any explicit definition for what defines as stalking, section 2A(2) of the Act reads:

“For the purposes of subsection (1) (b) (and section 4A (1) (a)) a person's course of conduct amounts to stalking of another person if—

(a) it amounts to harassment of that person,

(b) the acts or omissions involved are ones associated with stalking, and

(c) the person whose course of conduct it is knows or ought to know that the course of conduct amounts to harassment of the other person.”

The law, much like the law dealing with harassment, is not bound by the boundary of any particular act that has to be committed for the provisions of stalking to be attracted, it instead relies on the social conscious at the period of time. *“The acts or omissions involved are ones which are associated with stalking”*¹³; the statute relies on subjective interpretation of the provisions and their applications on allegations are made on case-to-case basis. Apart from the definition, section 2A(3) also lists out examples of acts that can be associated with stalking, the list is no way exhaustive of the list and merely lists out the possible examples of the same. Now juxtapose that with sec 354D of the IPC which defines stalking and you'd understand why it had to be added by an amendment and will also continue to be amended as the UK stalking law will continue to adapt to the changing social conscious; there are two acts mentioned in section 354D and at least one of them is required to be met for the act to be considered a crime of stalking. The restrictive boundary around section 354D results in the need for its constant amendment as the state of technology constantly changes the way humans communicate to each other. Section 2A

¹³S.2A (2), Protection from Harassment Act, 1997.

of the Protection from Harassment Act on the other hand doesn't need to be constantly amended as the wording of the provisions attaches itself to the socially prevalent definition of stalking.

Apart from cyber harassment and stalking, UK laws also punish Cyber Pornography. Revenge pornography is a broad term but usually involves an individual, often an adult ex-partner, uploading sexually intimate images of their partner on to the internet to cause the victim humiliation or embarrassment.¹⁴The offence is covered under the provisions of the section 33(1) of the *Criminal Justice and Courts Act, 2015*. In the section it is stated that "it is an offence to disclose private sexual photographs or film". But just mere disclosure does not make it an offence as, the disclosure has to be "i) Without the consent of the individual in the frame and ii) to cause distress".

Section 34(2) of the Act also defines what disclosure means: "A person 'discloses' something to a person if, by any means, he or she gives or shows it to the person or makes it available to the person."

So, relying on the provision, the moment the disclosure is made to any third individual outside of the person who was in the frame and the person to whom it was sent to, it is considered a disclosure.

But mere disclosure does not constitute an offence under section 33 of the Act; the disclosure must have been with the intent to cause distress. So for example, forwarding a sexually intimate video received would not amount to an offence under the section. The video must have been sent specifically to cause distress. The English court's jurisprudence is a little shaky on this facet of the law, a fact which is apparent from the case of Mr. Christopher Green. Mr. Green had found a video of his former partner on the internet and sent it to her and her best friend to warn them about the presence of the video on the internet and even sent it to the police to have it taken down. But, Mr. Green was also brought before the court and given a sentence, albeit a much lenient one compared to the actual perpetrator Mr. Aiden Farrelly.¹⁵

Although the Act imposed no liability on third parties hosting the images, websites were swift to see the reputational benefit in being seen to be proactive in helping the victims, many setting up specific forms for users to report revenge porn. In just one example, Microsoft responded to the

¹⁴Revenge Pornography- guidelines on prosecuting the offence of disclosing private sexual photographs and films, available at: <https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual> (Last visited on December 27th, 2019)

¹⁵Advertising salesman, 34, is hauled before the courts for 'sending revenge porn', available at: <https://www.dailymail.co.uk/news/article-3706525/Advertising-salesmen-34-hauled-courts-sending-revenge-porn-tipping-ex-boyfriends-sent-sex-tape-her.html>(Last visited on December 29th,2019)

new law by establishing a specific content removal request form for “non-consensual pornography” from its Bing search engine. The company has since reported that between January to June 2016 it received 406 removal requests, of which it accepted 251 (62%).¹⁶

The United Kingdom has three legislations in place to protect from cyber trolling: The Malicious Communication Act, 1988 which deals with comment that causes ‘anxiety and distresses and the Communications Act, 2003 which covers threats.¹⁷ Now the only distinction between the two acts is that while one covers England and Wales, one covers the entirety of United Kingdom. The two acts in fact overlap too when it comes to application of them.

The Malicious Communication Act, 1988 was used to prosecute Sean Duffy, who was jailed under the act for 18 weeks because he had made grossly offensive comments about children who had killed themselves in 2011.¹⁸ The Communication Act 2003, on the other hand, was used to jail Colm Coss, who was also jailed for 18 weeks for posting offensive messages on the memorial site to John Paul Massey, a boy who was mauled to death by a dog.¹⁹

2.1 Jurisdiction of courts

The question of jurisdiction of the courts in cases of cyber-crimes has also been pondered upon by the English courts in the case of *R v. Smith(Wallace Duncan)*,²⁰ where in it was said:

“The English Courts ... seek ... to apply the English criminal law where a substantial measure of the activities constituting the crime take place in England, and restricts its application in such circumstances solely to cases where it can be seriously be argued on a reasonable view that these activities should on the basis of international comity not be dealt with by another country.”

The same principle was also in the case of *R v Sheppard and Whittle*,²¹ where in the accused posted racially inflammatory messages in a website which was registered in California, once the message reached the server in California, it was posted online for everyone to see including

¹⁶ Agate Jennifer, “Revenge Porn” and Section 33: The Story So Far, *Entertainment Law Review*, Volume 28(2), p.no. : 40-42 (2017).

¹⁷ Who, What, Why: What laws currently cover trolling?, available at: <https://www.bbc.com/news/blogs-magazine-monitor-29686865>(Last visited on December 25th2019)

¹⁸ Supra

¹⁹ Jade Goody website “troll” jailed, available at: <https://www.bbc.com/news/uk-england-manchester-11650593> (Last visited on December 25th2019)

²⁰(no.4) (2004) 2 Cr App R 17

²¹(2010) EWCA Crim 65

people of England and Wales, the court applying the principle in the case of R v. Smith, declared the jurisdiction to be in England since the accused and the people reading it were based in England and only the server was in California.

2.2 International Co-operation

With the very inherent nature of cyber space being an international forum, it is likely that crimes will be perpetrated by individuals outside the jurisdiction of the English courts, but there are safeguards to be able to prosecute those individuals as well. The UK has a system of procuring evidence from other countries in case of a crime perpetrated against an individual of the nation.

In case of a crime happening which is outside the immediate jurisdiction of the English executive and the courts, UK has several *Joint Investigating Teams* with jurisdiction spanning over two or more countries to conduct investigation into the matter. A Joint Investigation Team (JIT) is an international cooperation tool based on an agreement between competent authorities – both judicial (judges, prosecutors, investigative judges) and law enforcement – of two or more States, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the involved States. JITs constitute an efficient and effective cooperation tool that facilitates the coordination of investigations and prosecutions conducted in parallel in several States or in cases with a cross-border dimension.²² JIT's are provided for in Article 12 of the 2000 MLA Convention.

There is also the provision for requesting mutual legal assistance from another country when it seems imperative to enlist international help. Section 7 of Crime (International Cooperation) Act 2003 permits for obtaining evidence regarding a crime, while communication through police to police channels is encouraged, the Crown Prosecutors are designated under the Act to request evidence for a particular crime if they believe or have reasons to believe that a crime has taken place.²³ While there are several Mutual Legal Assistance (MLA) treaties the UK has with several countries, the courts can still send a request to a country where there doesn't exist any treaty, but as a thumb rule, it is taken that the request has much more chance of being granted in a country with whom there exists a treaty.

²²General Background, available at: <http://www.eurojust.europa.eu/Practitioners/JITs/Pages/historical-background.aspx> (Last visited on December 25th 2019)

²³ International Enquiries, available at: <https://www.cps.gov.uk/legal-guidance/international-enquiries> (Last Visited on December 25th 2019)

3. Cyber-laws in USA for protection of women

There is no national law for protection of cyber-crimes perpetrated against women; the states themselves have enacted laws to punish such offences with 46 states of the 60 have enacted some form of law to prevent un-consensual distribution of sexually intimate images of partners. But since it's a state made law, the punishment for, for example non-consensual imagery, ranges from simple misdemeanor in Alaska to Class C felony in the state of Alabama.²⁴ While most of the states classify distribution of sexually intimate images of a partner as a misdemeanor, some states such as Alabama, Connecticut, and Georgia classify a second occurrence of the crime as a felony, with Alabama awarding a sentence possibly up to 10 years.

In U.S, cyber-stalking and cyber-bullying are mostly similar concepts, divided only on the basis of the age of the victim; so, adults being involved makes it cyber-stalking while when the victims are children, it is referred to as cyber-bullying.

Federally, U.S.A has very little legislation to deal with cyber harassment and cyber-stalking. Violence against Women Act, 2000 was one where the country federally made cyber-stalking a part of their inter-state stalking statute.

Because of cyber-crime being mostly a state devised legislation, the jurisprudence regarding the crime also differs widely. In the case of the State of New Jersey v. Dharun Ravi,²⁵ the perpetrator was sentenced to 30 days in jail and three years in probation; the judge believed that the perpetrator acted in "colossal insensitivity and not hatred".

When it comes to cyber trolling though, U.S falls short when it comes to legislation to combat that. Unlike, its neighbor across the pond who has two legislations in place to protect offensive messages sent over social media, and even unlike India which, even though it gives the citizens of its country the fundamental right to free speech, still places a reasonable restriction of it not being against public order, decency or morality, The US law keeps nothing above the protection of first amendment which protects against abridging the freedom of speech. So for a troll to be

²⁴ 46 States +DC+ One territory now have revenge porn laws, available at:
<https://www.cybercivilrights.org/revenge-porn-laws/> (Last visited on December 30th, 2019)

²⁵ 2016 Westlaw 4710195

punished it has to be a direct threat to a victim or else they are legally acting under the protection of first amendment.²⁶

4. Cyber laws in India for protection of women

In India there are three legislations in place which prohibit cyber-crimes against women, The Indian Penal Code, 1860 which protects women from sexual harassment in the online space and cyber-stalking.

Section 354A, states that:

1) Any man committing any of the following acts:

- i) Physical contact and advances involving unwelcome and explicit sexual overtures; or*
- ii) A demand or request for sexual favours; or*
- iii) Showing pornography against the will of a woman; or*
- iv) Making sexually coloured remarks, shall be guilty of the offence of sexual harassment.*

While Indian Penal Code covers crimes of the land, the wording of this particular section shows that the medium of communication is not the important bench mark but the acts that are committed by the perpetrator. The act, contrary to UK legislation, lists out specific acts which constitute the crime of harassment, but has made them applicable both over the cyber space and physical reality.

Section 354C also prohibits voyeurism, essentially making it a criminal offence for a person to capture video or picture of women engaged in a private act in a situation where the women will not be expecting observation. Dissemination of such videos and photos becomes punishable under the provisions of the section.

Section 354D of the same act (mentioned above in the article) covers stalking. The Act specifically lists out the acts need to be committed by the accused for the provisions of the

²⁶Art. 19(2), The Constitution of India, 1949

sections to be attracted. The provision also specifically mentions the acts committed over cyber space which will be considered as stalking.

While IPC deals directly with the offenses of harassment and stalking, the country also has enacted other legislations to deal with the offences indirectly. The Information Technology Act, 2000, is one such legislation. Sections 67 and 67A punish the publication of obscene material, and sexually explicit material respectively in an electronic form.²⁷ While they don't directly deal with crime against women, any act of voyeurism punishable under section 354C of IPC will also be punished under section 67A of the Information Technology Act.

There also used to be another section which more directly dealt with the harassment women face in the cyber space. Section 66A of the Information Technology Act, 2000 was enacted after the RituKolhi Case to protect the women who faced such harassment on the cyber space. The section punished any communication of the message which was grossly offensive to the receiver. The section, however, was struck down in the case of *ShreyaSinghal v. Union of India*.²⁸ The supreme court in the case held that the usage of word "offensive and annoying" was arbitrary and curtailed the right of free speech conferred under article 19 of the constitution and did not also qualify to be a reasonable restrictions under the sub clauses of the article.

In India, a victim can approach the justice system through two ways:

- 1) Cyber Cells; and
- 2) Police Station.

Cyber cell is an initiative by the Indian government to facilitate the victims in filing complaints online.²⁹ The cell functions as an investigating team designed specifically to investigate cyber-crimes. The existence of the cell benefits the victims who are usually hesitant to approach the police to file an FIR on cyber harassment, due to possible further humiliation they might receive at the hands of the police which has been the case numerous times in the past.³⁰

²⁷S. 67; s. 67A, Information Technology Act, 2000

²⁸W.P (Crl.) No. 167 of 2012

²⁹ National cybercrime reporting portal, available at: <https://cybercrime.gov.in/> (Last Visited on December 24th2019)

³⁰Why Online Harassment Goes Unpunished in India, available at: <https://www.bbc.com/news/world-asia-india-33532706> (Last Visited on December 22nd 2019).

5. Conclusion

All the three countries mentioned in the research articles are actually well legislated countries when it comes to cyber laws. The problem lies in the fact that while the countries and the international community in general are well aware of cyber threats from a financial and security stand point and have legislated to avoid that, there are no legislations to deal specifically with cyber harassment towards women. Cyber laws rendering protection to women is mostly an offshoot of cyber-laws giving protection against privacy of people in general. For example, in India, Section 67A was enacted to mitigate the dissemination of pornography; the protection against dissemination of private videos of a female partner just so happens to be protected from that law. The world took a long time to accept the equality of women in society and to legislate to ensure their equality and protection of dignity. But with the knowledge and the current awareness that the women also deserve protection due to the sheer amount of gender-based cyber harassment they are subjected to, the international community must act quicker than it did in the past. There are steps that are being taken by the international community though; The UN general assembly just passed a resolution to start the process of drafting a new international treaty to combat cyber-crime.³¹ While there are some objections raised by U.S and European Union regarding the committee that would be established pursuant to this treaty will undermine international cooperation, the resolution has been passed and legislation will be drafted soon.

The legislations need to be updated and worded in such a way that they adapt to the changing ways of technology and the troubles that could befall women through those changing ways. Social Contract theory of society has taught us that we as humans agreed to come together as society and compromise some of our individualistic rights to ensure protection that comes with the society, the cyber space is no different from real society and therefore the same protection must be provided to our members in the cyber space.

³¹UN Gives Green Light to Draft Treaty to Combat CyberCrime, available at: <https://www.nytimes.com/aponline/2019/12/27/world/europe/ap-un-united-nations-combating-cybercrime.html> (Last visited on December 23rd 2019)