
Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2021); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:10, ISSUE:5(1), May:2021
Online Copy of Article Publication Available: www.ijmer.in
Digital certificate of publication:http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
DOI: http://ijmer.in.doi./2021/10.05.27
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 10th May- Publication Date:30th May 2021

ROUTINE ACTIVITY THEORY IN RELATION WITH CYBERCRIME- STALKING AND BULLYING COMPARATIVE ANALYSIS BETWEEN INDIA AND THE UNITED STATES OF AMERICA

Ankita Kumari
Student
New Delhi

Introduction

Today we live in the world where everything is circled around the internet. The development in the field of internet is commendable that nowadays everything which we do is regulated around the information technology. With the development and advancement in every field the crime also got advanced. Earlier crime used to happen in the old fashion way of committing the offence in real world but now offender have taken the advantage of the information technology and have sharpen and modernized their weapons. [1]Now they hide behind the screen of their computer and do crime in virtual world which affects the life of people in real world. So, Cybercrime in simple world can be defined as commission of crime with the help of electronic devices which have internet connection for example – laptop, computers, mobile. Cybercrime are of any kinds some of them are stealing, phishing, hacking, revenge pornography, defamation, threating in this paper we will discuss about the cyberstalking and bullying. We will look after the legislative policy of two different countries and compare and analysis them and how the policy is related to the victimization theory. Victimization theory we are going to discuss here is Routine activity theory and how it is related to cybercrime. The legislation of India and the united states of America for Cybercrime will be compared.The paper will include the critical analysis of the legislation also.

In India the offences related to the cybercrime are dealt under the legislation by [2]The Information Technology Act 2008 accompany by Indian Evidence Act and Indian penal code and in United states Cybercrime comes under the legislation of [3] the Computer fraud and Abuse Act(“CFAA”).

Relation of Main policy with Victimization theory

In order to explain the cybercrime victimization, the best way is to explain it with the help Of Routine Activity Theory. Routine activity theory was proposed by the “Marcus Felson and Lawrence E. Cohen”. By this theory it has been proposed that in order to crime to take place there should be presence of these three essentials which are- offender, absence of guardian, suitable target the hypothesis isn't fundamentally keen on understanding anoffender' inspiration yet rather centres around the qualities of wrongdoing where "the spatio-transient association of social exercises encourages individuals to make an interpretation of their criminal tendencies intoactivity.

Offender

Every offender who commits a crime wants to find out the loopholes in the system in order to perform the crime in most convenient and less dangerous way. In Cybercrime a offender commit the crime in the real world by the virtue of virtual reality and hiding behind the computer screen give them a boost of doing the offence more. They can do the crime just by the virtue of one link. By that one link they can find out a lot of information about their target.

Suitable target

The next essential is the suitable target most of the criminal have a desirable pattern of committing crime by choosing their target. [4]Some of the criminal have pattern of choosing their target and then following the target and get information about them by the virtue of the social networking sites cases of cyber stalking is increasing rapidly offender find out about everything by the virtue of their accounts- the routine and then use it for the purpose of the committing the offence. Students who are engaged on internet usually fall under the trap of these criminal they talk to them and exercise the offence. Cyber stalking leads to pornography, kidnapping they all interlink. Offender first earn the trust of their target by stalking them and then present themselves the version which there would like to talk to cyber stalking leads to cyber bullying after getting the access to all the personal details they used it to threaten the victim. but it does not mean that people who are less active on the cyberspace does not fall under the trap.Offenders stalk all those people who are less active and use it as an opportunity to get the money as they fall under the trap of clicking the link for easily because of their knowledge about the field.

[1]Stephen, Arunbaby, Comparative Analysis of Cyber Stalking Legislations in UK, US and India, CULJ,6, 61-76, (2017).
[2]The Information Technology Act 2008


Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2021); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:10, ISSUE:5(1), May:2021
Online Copy of Article Publication Available: www.ijmer.in
Digital certificate of publication:http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
DOI: http://ijmer.in.doi./2021/10.05.27
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 10th May- Publication Date:30th May 2021

[3] The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030

[4]S. Elizabeth Wick, Patterns of Cyber Harassment and Perpetration among College Students in the United States: A Test of Routine Activities Theory,11, OP,24,26-27(2017).

Absence of the guardian

Mostly crime took place when there is no guardian to took care or analysis the situation and that turns out to be the most perfect situation for the offender and the same thing happen when a person is on the internet without the guidance of the guardian. The routine activity online conduct may likewise incorporate utilizing unguarded networks through associating with any open Wi-Fi for example air terminal, railway stations, restaurants, transport, eateries, inns). At the end of the day, people regularly put themselves at more serious danger of being hacked without even acknowledging it. Delicate data for example, account numbers, passwords, banking data, credit cards details while associated with a Wi-Fi network without sufficient network safety security permits persuaded culprits who are in a similar existence (on a similar organization) to discover freedoms to enter PCs and access individual information.

The legislation of both the countries made in order to tackle the problem which arrive because of the elements mention in the routine activity theory. There are many crimes which happen because of presence of these elements two of those cybercrimes are cyberstalking and cyber bullying. the cyber stalking could happen by the virtue of e- mails, messages,Stalking would be done by the virtue of the routine activity theory as he will follow his victim and finds out about the whole activities and events and then use it in order to harass the person by posting them on the internet and threaten the victims for the purpose of having sexual relationship. We can take the example of Manish kathuria case in which the defendant talked with plaintiff on the internet and got information about the defendant then use it against the plaintiff in order to have sexual relationship threaten the plaintiff to upload the same on the internet. Because of this case the IT act got amended and Sec 66-A was added in the act earlier these types of cases used to go through IPC 509 but now through section 66-A.

Parameter of contrast

- In India the legislation for cybercrime is The Information Technology Act 2008. In united states of America, the legislation for cybercrime is federal Computer fraud and AbuseAct("CFAA").
- The United State of America was one of the first country to have a legislation forcybercrime.
- The laws are more rigid and strict in The United State of America as compare toIndia**.**
- The conviction rate of cybercrime is low it is 8% whereas the conviction rate of The United State of America is high it is 55% of the presentcases.
- [5]United State of America made the Wire Fraud statue in order to prosecute online criminal though noas such law is made inIndia.
- In India along with ITA there are other act also like Anti-money laundering act, Indian evidence Act, Indian Penal Code. In the United State of America, they follow Economic espionage Act, Fraudulent online identity sanctionact.
- In order to tackle Cybercrime, there is crime mapping in The United State of America where as in India there is no existence ofit.
- In India there is one law for the Cybercrime where as in The United State of America there are state as well as federal law for Cybercrime states like Washington, Ohio and Rohde Island have their separatelegislation.
- In India there are establishment of cybercrime cells but still need of well- trained law enforcement bodies where as in USA there are experienced and well-trained law enforcement inplay.

Critical Analysis

India and The United states of America both have their respective legislation in order to tackle with the various kind of Cybercrime which are faced by the people. In India the cybercrime is stated under The Information Technology Act 2008 which is amended. As technology and development [6]In the field of computer came late in the India so till 90's there were no legislation regarding the cybercrime in India but later on as there was increase in the crime there is introduction of legislation in India the information Technology Act 2008 which is amended later on and became the legislation we have now. Where as in The United State of America the advancement in technology in the field of computers came early. So as a result, the Cybercrime in The United State of America initiated faster. As there were very few legislations in the world regarding the cybercrime at that time the offenders were targeting the countries who did not have any legislation in the field of the cybercrime which they still continuing to do as that decrease the chance of gettingcaught.

[7]Although India have mentioned the aspect of cybercrime in the legislation but still there are some missing like legislation only focus and mentioned the breach of privacy but does not mention communication threats. In India there is a establishment of cybercrime but what is lacking is that India does not have enough well-trained, advance, specials in the field of cybercrime. Although there is

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2021); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:10, ISSUE:5(1), May:2021
Online Copy of Article Publication Available: www.ijmer.in
Digital certificate of publication:http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
DOI: http://ijmer.in.doi./2021/10.05.27
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 10th May- Publication Date:30th May 2021

legislation but the execution of those crime is not quite advance. If someone commit offence online or visit the ban sites there are quite less chances that there will be some enquiryhappenagainst theoffender.Thislackofexecutionisincreasingandboosting thelevelofconfidenceofthe offenders in committing the crime. Their too much emphases and burden on the judiciary branch to interpret the law which sometimes lead to imprisonment of victim. In the United State of America, the laws and regulation are strict and rigid which result in less chances of escape of the offender in The United State of America. [8]There isstatelaw as well as federal law in USA which make the legislation of the country stronger. In order to track the criminal, there is crime mapping which in India only exist in the mind of the people. there is lack of advance technology and people in the cyber branch because the people who are committing Cybercrime have more experience in the field which leads to their escape easy. The extra diction regulations in India are quite slow which had become the benefit for the offender. But still India is quite ahead of many countries in the world for tackling cybercrime the legislation of India has specified punishment for the offenders like sec 67 of the act "prohibits the publishing of the obscene photo on the internet which is punishable for the imprisonment of 5 year or fine of 3 lacs or both" Sec 65 "state that Tampering with Computer Source documents will be punishable with the imprisonment up to 3 years or fine of 2 lacs or both" sec 72 of the act dealt with the offence of hacking which is punishable up to imprisonment of 2 years or fine of 2lacs.

Conclusion

As it is clear that society is dependent upon the information technology way too much which increase the chance of cybercrime to happen with keeping in mind the routine activity theory as preparators took advantage of it.

Taking everything into account, the comparative analysis uncovers that India actually has far way to go there is a need of amendment in the legislation and execution of the laws have to be improve. It needs more financing to embrace the sort of advances that would help its policing techniques. The US needs to settle on Policing system- based innovation choices as it would be savvier and the officials could be prepared uniquely on explicit advancements. Crimes happen because the cyberspace is open for every individual and even after efforts there will always some aspect of the cybercrime will always be there.

[5]RajlakshmiWagh, Comparative Analysis of Trends of Cyber Crime Laws in USA and India,2,61,69-70(2013).
[6]Arunbaby Stephen, Comparative Analysis of Cyber Stalking Legislations in UK, US and India ,6, CULJ,61,69-70(2017).
[7] https://www.mondaq.com/india/technology/963026/cybersecurity-comparative-guide(last visited 09 Mar. 21)
[8] Dr. Ajay Kumar Garg, Shikha Kuchhal, Data Protection Laws in India: A Comparative Study,3, IJAR,75,75-76(2013).

Filename:	27
Directory:	C:\Users\DELL\Desktop
Template:	C:\Users\DELL\AppData\Roaming\Microsoft\Templates\Normal.dotm
Title:	
Subject:	
Author:	Windows User
Keywords:	
Comments:	
Creation Date:	5/15/2021 12:19:00 PM
Change Number:	7
Last Saved On:	6/1/2021 11:42:00 AM
Last Saved By:	Windows User
Total Editing Time:	24 Minutes
Last Printed On:	6/8/2021 7:15:00 AM

As of Last Complete Printing

Number of Pages:	3
Number of Words:	1,908 (approx.)
Number of Characters:	10,881 (approx.)