Page 1637 - 1656

DOI: *http://doi.one/10.1732/IJLMH.25885*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 1

2021

Are Laws Pertaining to Cyber Crimes in India Sufficient in the Current Scenario

MUKUL VERMA[1]

ABSTRACT

As the world moves toward digitalization more and more aspects of human life is getting associated with their digital presence. In recent times every aspect of human life leaves atleast some form of digital footprint. For example what a person does, what he or she consumes, where he or she lives, what are their prefences are all recorded in form of digital footprint. Moreover important information like bank details, personal information, medical records are also being increasingly stored online.

This have given rise to a new menace of cyber crime. Hackers increasingly target and steal this personal information of individuals and use them to do various things like blackmail, misuse of data etc. India is still a developing country in terms of digital presence but still cases of cyber crimes have become increasingly frequent. Indian authorities have implemented various laws and policies regarding that of cyber crimes.

This study was undertaken to analyze the effectiveness of this lawas and policies in the current scenario where Indian is poised to become one of the largest internet userbase in the world.

Keywords: *Cyber Crime, Internet, Digital footprint, Cyberspace, Criminal Law, Law*

I. INTRODUCTION

The approach of e-innovation has brought assortment of chances and a portion of these, of course, are of a criminal sort. The Cyberspace made by PC innovation gives a mode of doing numerous things in proficient way. The utilization of machine supplanting human hands gave more prominent chances and alternatives. The mechanization of organizations, banks, instructive establishment, and railroad reservation curve reflections showed wherever that shows reliance of human culture on these modest PCs. Today, antiquated paper-based working example is only obsolete, as it can't stay up with rapid existence of current world[2].

Social orders world over in the only remaining century have been generally worried about

[1] Author is a LLM student (Batch 2019-20) at Parul University, Vadodara, Gujarat, India.

[2] Guide to cyber Laws, Rodney D. Ryder,(2003) Wadhwa Nagpur, Page 2.

crime influencing the physical people and property. They have as needs be developed state frameworks of law and implementation to manage the types of crimes. Fast industrialization and urbanization has brought new types of crimes including more extensive worries of social request, wellbeing, and security.

On the off chance that Cyberspace is the kind of network a goliath neighborhood made up of organized PC clients around the globe - at that point it is common that numerous components of a conventional society can be viewed as bits and bytes." With electronic business, rise electronic shippers, connected teachers furnish arranged training and specialists meet with patients on the web. It should not shock anyone that there are likewise Cyber criminals carrying out Cybercrimes[3].

To comprehend the ocean change PC innovation has acquainted with criminal action, the speculative model may direct it appropriately: Consider this one.

“One can analogize a denial of service attack to using the telephone to shut down a pizza delivery business by calling the business telephone number repeatedly, persistently and without remorse, thereby preventing any other callers from getting through to place their orders While it may be possible for someone to execute this scheme, it would be very onerous to do so because it would require a great deal of physical effort and concentration on the perpetrator’s part, he would have to be constantly dialing, maintaining the connection until it was broken and then redialing quickly to prevent any other call from coming in. It would also involve a significant risk of apprehension because the victim could contact the authorities, who would presumably have no difficult tracing the calls to the perpetrator, since he would presumably be using his personal or business telephone.”[4]

The occurrence of customary crime, more often than not, is anything but difficult to bargain by law controlling office. Here area can be followed out, individual can be distinguished, realities and issues can be examined, calls can be investigated, *mens rea* can be discovered and risk can be forced. In any case, in the occurrence referred to over, the legitimate apparatuses might be deadened to manage previously mentioned issues. By and large, and in the vast majority of the customary crime facilitates, the issue of ward may not emerge in above case, physical hunt is conceivable or more all the law appropriate to both culprit and casualty is same. Too incredible degree, the conventional lawful framework is well prepared to deal with, research, investigate, and analyze the realities identified with the crimes.

[3] L. C. Amarnathan, Cyber crime prevention and control strategies March 2002, CBI bulletin 5 DIG

[4] Cyber Crime law & Policy Perspectives, Dr. Mrs. K. Sita Minikyan (2009), Hind Law House Pune, Page 198.

Boundary between Cyber-crime and that of supposed conventional crime can be followed out on some recognized footings. In any case, amusingly, one may deceive term in physical sense. Along these lines physical mischief perpetrated to PC, taking of PC machine, burglary of PCs from the home or establish or any piece of PC, for example, hard plate, screen or console, making misrepresentation in selling PC machine isn't PC crime however on first sight it might is by all accounts 'Crime carried out against a PCs or by methods for PC' Ok 'Destructive' act perpetrated from or against a PCs or systems administration. The portrayal of Cybercrimes given above as elaborative sense[5].

Cybercrime is anything but difficult to carry out (in the event that one has the know - how to do it), difficult to identify (in the event that one realizes how to eradicate one's tracks) and regularly difficult to situate in jurisdictional terms, given the geological indeterminacy of the net. The capacity of Cyber criminals to transform into new and various types of withdrawn exercises avoiding the range of existing corrective law makes difficulties for law implementation around the globe. Cyber-criminals can abuse holes in their own nation's criminal law to defraud their kindred residents without any potential repercussions. They can likewise misuse holes in the criminal laws of different nations to deceive the residents of those and different countries.

Moderately, in simplicity of Cyber-criminality, Cyber space permits these assaults effectively do and such interruptions can he made easily with next to no danger of anxiety. As a matter of first importance, it is hard to fix the personality to the culprit in Cyber-space as it is anything but difficult to veil a phony character. You can have a veil of celebrated saint, heroin, and lawmaker or even cop with photograph character in tie Cyber-space. It is hard to see the individual really sitting before terminals and just the showed personality is just source in Cyberspace. Besides, it is hard to find the ward and territory of the culprit. Neither it potential his goals and advantage he get from such deviation. Nonetheless, one can confront these fundamental' troubles in Cyber-space[6].

By and large, it is mixed up conviction that Cyber-space is equivalent words of crime carried out over the Internet-organizing, as previous is a lot more extensive articulation enveloping - other than Internet, the PC and its systems administration, information present in computerized structure in the PC or on any storable devise, programming and equipment in any practical structure. Cybercrime might be perpetrated even by remaining disconnected and it isn't important that the individual ought to genuinely stay present online in the systems

[5] Law of Crimes (Indian Penal Code, 1860) S.R.Myneni, (2009) Asia Law House, Hyderabad, Page 2.

[6] PSA Pillai’s Criminal Law: V.Suresh and D.Nagasa (2000) Butterworths Wadhwa, New Delhi, Page 11.

administration of PCs. Unis programming theft is the crime carried out by the individual by taking the product duplicate on circle or floppy and transmits it.

II. The pattern of 'PC proficiency' attach the procedure of cybernation

Today the courses relating to 'PC proficiency' preparing become an essential piece of educational plan Due to the huge utilization of electronic gadgets inside the air accessible around the new age, the new age handily got electronic teaching. Directly from the period of coddling, electronic innovation encompasses them. In this way, when they come out of their youthful age and got ability of venturing into Cyber-space, tremendous Cyber-world open an escape for unending chance. In any case, because of youthful age and absence of judgment ability there are equivalent odds of their introduction to the underhanded impact of this innovation. Hence on oi e hand, innovation that is a basic piece of their educational program heaved them in the unprotected Cyber-world[7].

III. Cyber Crime - neither hard to learn nor hard to carry out

Cyber-crime is neither much difficult to learn nor much hard to carry out. In present day society, PC innovation can be educated like language. Advanced innovation encompassed our life to such an extraordinary degree, that everyone is being familiar with it. Especially, the new age for whom PC information is a basic piece of educational program, and where information dissemination is with tire help of PC it is simple for them to have accommodation open intends to carry out crime in Cyber-space. Frequencies are there, where at first, PC is (earned either to straighten something up, delight or impulse (might be legitimate or instructive) or last on learning information transformed into misconduct. The easy to use programming has fanned the fire making Cyber wrongdoing much wonderful and simple. This is valid, especially with respect to sex entertainment, disgusting talking, and theft. Today, anyone with least PC proficiency is adequate to approach Cyber-criminality and the odds are exceptionally less of being caught by the preventive organizations. These highlights make Cyber-crimes increasingly perilous and disturbing[8].

IV. Difficulties in following the cyber crime

In the event that one is sufficient blessed to conquer these troubles of finding, exploring and fixing the criminal obligation, the following complexities he needs to look about the

[7] P S A Pillai’s Criminal law, K.I. Vibhute (2014) LexisNexis, Gurgaon. Page 41

[8] Cyber Law: Talat Fatima, (2011) Eastern book company, Locknow. Page 29

assortment, assessment, investigation, impelling and recording and perusing the confirmations enemies of witnesses. Talking with model, assume in the case of Cyber-stalking refered to above, culprit utilized PC to hack and stalking the web webpage of pizza parlor through Internet, by what method can the chronicle and perusing of proof is conceivable regardless of whether, the instrumentality of an offense for example PC has been seized? Once more, regardless of whether docs lawful framework has fit for perceived such proof in electronic structure? Assume, again the hacking or stalking has been carried out from paid Cyber-bistro, at that point how the nearness of criminal can be found? To put it plainly, such issues make Cyber-criminality increasingly extreme and genuine right now.

Notwithstanding that, as because of Internet offices, Cyberspace don't perceived limits, boundaries or line of control of the countries, the issue of locale likewise make issue in Cyber-criminality. Therefore the possibility of Cyber criminals to transform into new and various types of reserved movement dodging the span of existing correctional law make difficulties for law implementation around the globe. Cyber criminals can abuse holes in their national criminal law to exploit their kindred residents without any potential repercussions. They can likewise abuse holes in the criminal laws of different nations to defraud the residents of those and different countries[9].

V. Difference between Cyber-crime and conventional crime

As a matter of first importance, Cybercrime is basically perpetrated on or with the assistance of Cyber innovation. In this manner, nature and extent of Cyber-crime ought to be broke down on various balance. In this manner, employments of PC, an electronic gadget, for the commission of crime are fundamental element of Cybercrime. Be that as it may, conventional crime doesn't have such condition point of reference.

Cyber-crime vary from supposed customary crime on the grounds that Cyber-innovation gives transgressor exceptional conditions where he can conceal his character, even miscreant can utilize counterfeit personality, he can approach the PCs of casualties without his insight and with no limitations Here no national limits can confine the section of transgressor. Simultaneously, methods created to follow out the conventional crimes may not be valuable in the event of Cybercrime. More often than not no fingerprints accessible, no blood recolor, no DNA test examination is helpful to fix the character of a person. In addition, he may not be basically including nearness inside your national limits that causes troubles in examination of crime just as capturing the criminals.

[9] Anuradhe Parasar (2006): Impact of internet on society, Page 3.

The idea of Cyber-crime is to some degree unique in relation to conventional crimes. In addition, exceptional class can be raised under the flag of Cyber-criminality to give distinctive treatment to the crimes falling under this head. The plot of commission of crime may completely extraordinary if there should be an occurrence of Cyber-crime. Accordingly, for the vast majority of the customary crime is concerned, physical nearness of criminal is basic for commission of crime. In this way while commission of customary crime and subsequently we may follow out the existences of criminal on the scene. In such cases physical nearness of a wrongdoer become most significant inquiry and his barrier as explanation assume significant job. Anyway as Cyber-crime might be carried out without being stay present on the genuine scene of commission of crime, the procedures created to follow out the guilty parties carrying out customary offenses bend not progressively helpful. In Cyber-crime one may not discover hairs, fingerprints, impressions, bloodstains, and smell of guilty parties[10].

VI. RESEARCH DETAILS

(A) Research Objectives

- To analyze the various Cyber Crime Laws
- To analyze the effectiveness of Indian Cyber Crime Laws
- To recommend possible identifications of issues affecting Indian Cyber Crime Laws

(B) Literature Review

Karve (2002)[11] discusses people who commit cybercrimes and concludes that they are mostly white-collar workers, unlike the usual criminals. They can even be high school kids. The territory that a cybercrime can stretch into is immense and can transcend continents.

Juster (2004)[12] presents a view point that while cyber-assaults would not be viewed as a weapon of mass demolition, it tends to be thought of as a weapon of mass disturbance. One individual with moderately small preparing, economical gear, and access to the Internet can possibly impair a whole system or framework.

Patil (2001)[13] talks about the need to keep up a register of 'moral programmers' or 'specialists' in each police headquarters. When the name of a moral programmer or master is enrolled,

[10] Cyber crime- Law & policy perspectives, Dr. Mrs. K. Sita Manikyam (2009) Hind Law House, Pune. Page 40.

[11] Karve, U (2002), “In info age, time for cyber savvy cops” Yours V 2.0 Frequently Asked Questions.

[12] Juster K I (2004), “Cyber security: A Key to U.S.-India Trade”

[13] Patil, Ramu (2001), “Cyber Policing: Setting a Thief to catch another”, New Indian Express

their help would be looked for at whatever point the need emerges. Law authorization should plan to take the administrations of white-cap programmers, who can go with police authorities during attacks over the span of the examination.

Kapoor (2003)[14] focuses to the way that almost 39 percent of cybercrime cases are identified with banks and money related establishments barring those of the administration. Gathering that criminals see banks as a rewarding objective for their creativity, cybercrimes in banks has been arranged to incorporate diddling/altering, burglary of information, shakedown utilizing information, unapproved bolting of information, and passage into databases; framework related, for example, messing with programs, changing project rationale, Trojan pony programs, hacking, letter drop besieging, and so forth. All the while, occasions of charge card cheats have become regular given the developing notoriety of MasterCard exchanges, Internet hacking and ATMs. Any recklessness while leading ATM exchanges fundamentally expands the dangers related with innovation driven money related exchanges. A Lebanese Loop trick, for example, includes a plastic or metal sleeve built to fit into the card opening of an ATM machine. At the point when a client embeds a card into the opening, the card is trapped in the sleeve. At the point when the PIN is entered, the exchange doesn't follow and the fraudster, professing to be a decent Samaritan asks the casualty to attempt once more, observing the PIN as it is more than once entered. At last the casualty surrenders and the fraudster evacuates the card with the assistance of a device and depletes out the client's record. More noteworthy watchfulness with respect to the client would have limited this hazard.

Poppat (2000)[15] contends for the need to make unique courts headed via prepared people to manage cybercrimes, yet with forces to collect heavier punishments in excellent cases. Except if there is strong discouragement, cybercrime will rise steeply. There is likewise a solid requirement for attorneys and judges, just as preparing government organizations and experts in PC crime scene investigation. There is a solid requirement for each episode of cybercrime including a PC or electronic system to be accounted for to a police headquarters, regardless of whether it keeps up a different cell or not.

Tippoo (2001)[16] talks about the inexorably complex methods for breaking into our protection and rupturing our security. Hacking is a code word for what is in actuality a demonstration of

[14] Vaidya-Kapoor, Gopika (2003), "Byte by Byte", Net Guide, February, 18, www. rediff. com/ netguide/2003/feb/18crime. html

[15] Poppat (2000), BBC News, "India Tackles Cyber Crime" www.news.bbc.co.uk/ 1/hi/ world/ south_asia/847727.stm

[16] Tippoo S (2001), "Cyber Crime: Are YOU safe?", Times of India

electronic war with annihilating results. There are different prospects of cyber murders, cyber psychological oppression, utilization of explosives, sedate managing, fakes and imitations. Eveiy email abandons a follow driving back to its place of cause as an email header, which is a decent pointer to the criminal.

Kumar (2002)[17] calls cybercrimes as crimes without Punishment. The issues relating to clearly identifying the perpetrator of the crime and pinpointing to his exact location creates legal and technological complications. If the perpetrator of cybercrime is in a jurisdiction that is not very cooperative with the jurisdiction, which is seeking to prosecute the perpetrator, the process of bringing the culprit to books becomes complex. As the Net can be accessed from any part of the globe, sovereign national boundaries and protections at those boundaries no longer offer any control over cybercrimes.Developing countries including India, face a further problem in having to depend on a police force that is not adequately trained and therefore stays far behind the criminals in terms of technological skills and competence. The Information Technology Act in India appears to prescribe low penalties for hackers; low compared to the damages they cause. Ideally the penalty should be related to and be over and above the amount of damages caused. Indian law on this subject also does not have any provision specifically for frauds arising from misuse of credit cards. Since computer crime has international dimensions, international cooperation is a pre-requisite to prevent computer crimes. Though an international cooperative effort was conveyed in the UN Manual on the Prevention and Control of Computer Related Crimes, it lacks the requisite wherewithal for effective implementation.

Nanda (2006)[18] regards cybercrimes simply as a normal crime facilitated by information technology but law enforcement functionaries who are good at management of normal crimes are not quite equipped to deal with cybercrimes. Emphasizing the all-pervading nature of cybercrimes, the extensive use of computers in different stages of attack on the Indian parliament is discussed. Cases of rape and murder with significant IT component in it are being reported. As the incidence of cybercrimes keep increasing, there are also instances when cases had to be closed because the courtroom did not have a computer. Cyber cafes are the preferred locations for cyber criminals and they remain largely unregulated.

Raghavan (2005)[19] talks about the issues looked in capturing a cybercriminal. More than people, it is the well-weave worldwide packs that represent a considerable number of

[17] Kumar, Atul (2002), “Cyber Crime - Crime without Punishment, available at: http://unpanl.un.org/intradoc/groups/public/documents/APCITY/UN PAN002368.pdf

[18]Nanda (2006), “Cyber Crimes and Real World”, www.boloji.com

[19]Raghavan R K(2004), “Catching the Cyber Criminar in “Frontline”

prominent PC based crimes. Regularly programmers work without anyone else however of late there is a reasonable arrangement with infection essayists. Thinking about the various tasks in the territories of dealing in people, particularly ladies and youngsters, sedate selling, sex entertainment and tax evasion that have been uncovered as of late, the job of Internet as a supplier of vehicle for correspondence among crime posses warrants consideration.

Hammond IV (2001)[20] opines that criminologists, law requirement offices, national security counsels, military authorities, cutting edge companies and research establishments all concur that cyber-crimes represent a genuine risk to society and this danger was already an issue that was well known uniquely among cyber-punk adolescents. These crimes are presently coordinated by persuaded gatherings of people with generous assets who are regularly connected to sorted out crime, global fear based oppressor gatherings or outside adversaries. The objectives in cyber-assaults now and then include the pulverization of delicate PC frameworks dealing with orders to indispensable establishments, for example, the state's power stream, plane landing and take-off administration, and so on. Justifiably, his determination is that lone a multidisciplinary approach including the instruction of the residents and the cutting edge CEOs, a better quality of insurance for the national foundations and a greater interests in PC and system security and in innovative work can effectively decrease the different dangers presented by cybercrimes.

Smith et al (2004)[21] bring up recognizable contrasts across wards, in the matter of arraigning cyber criminals. Talking about new alternatives, for example, confined or observed access to PCs and systems, and with courts starting to embrace approvals to suit the novel conditions of the cases, there is a requirement for developing a fitting condemning rule to cover cybercrimes.

Broadhurst and Grabosky (2005)[22] consider cybercrimes from different perspectives and the experts who have contributed bring with them rich knowledge and expertise in managing cybercrimes in different parts of Asia. This country specific approach and the sharing of success stories in different parts of Asia will go a long way in creating and implementing policy driven initiatives to combat cybercrimes.

Edappagath (2004)[23] drives home the importance of enforcing cyber laws. Cyber-law

[20] Hammond IV, Allen (2001), "The 2001 Council of Europe Convention on Cyber-Crime: An Efficient Tool to Fight Crime in Cyber-Space?' www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammo nd. COEConvention. Cyber-crime. pdf

[21] Smith R G et al (2004), "Cyber Criminals on Trial" Cambridge University Press.

[22] Broadhurst R & Grabosky P (2005), "Cyber-Crime : The Challenge in Asia", University of Washington Press.

[23] Edappagath, Ajmal (2004), "Cyber Law and Enforcement in the Newsletter "Information Technology in the

enforcement is a relatively new challenge for most law enforcement agencies and this challenge is made more complex by the absence of serious awareness of the importance of enforcement on cyber related laws. In view of the fact that cyber-crimes are growing at an alarming rate, the need for a concerted and pragmatic effort by all stakeholders at the national, regional and international levels is emphasized so that the target group comprised of individuals, businesses and the governments can work on the process of enacting and enforcing appropriate legal frameworks at the national and international levels after considering the various substantive and procedural aspects of fighting cybercrimes.

Rakesh (2005)[24] brought to light an interesting dimension to the study of cybercrimes where information assets are insured. If such insurance were to be done, the need for insurance companies to examine the information asset on which the attack was perpetrated becomes important. Globally corporate managers are now considering the advantages ofinsuring 'information' like insuring other assets.

Yvonne Jewkes (2006)[25] in "Cybercrime and Society," gives an unmistakable, efficient, basic prologue to current discussions about different parts of cybercrime by thinking about it in the more extensive setting of social, political, social and monetary change. Cybercrime including PC hacking, cyber-psychological warfare, media robbery, money related misrepresentation, fraud, web based stalking, detest discourse and erotic entertainment are all to be talked about and comprehended with regards to criminology, human science, law, legislative issues and culture. Drawing on the cases and models from the UK, US and Europe, the multi-dimensional investigation of cybercrimes gives a wide solicit to understanding cybercrime the board.

(C) Research Methodology

Research Philosophy

The research philosophy is provided as a way of collecting, analyzing and using data in previous terms. The research philosophy is known as how to collect data from various relevant sources to analyze the data and ultimately use it for researchers. The research philosophy is divided into three types, namely realism, positivism, and interpretivism. In the context of the current study, the researcher will use the positivism philosophy as it helps

Developing Countries" published by International Federation for Information Processing (IFIP) , Vol. 14, Dec. 3.

[24] Maini, Rakesh, Hindu Business Online (2005), "Cover against cyber crimes vital" — Insurance industry seeks tighter IT Act, tools to assess losses,Thursday, 2004,
www.blonnet.com / 2005/11/24/ stories / 2005112402750400.html

[25] Jewkes, Yvonne (2006), "Cyber Crime and Society"

researchers to conduct quantitative data analysis to reach the goals related to the research program (Flick, 2015)[26].

Research Approach

The method of classification-based study is considered as an essential part of relevant research. There are two types of research approaches, namely, the inductive Research Approach and the deductive Research Approach. In this study, the researchers will use the deductive research approachfor collecting primary data effectively. Using this approach, the researchers can provide a dataset that will benefit to gather information and bring relevant findings to the present study (Jamshed, 2014)[27].

Research Method

The research method is observed as a step-by-step action plan that gives researchers the ability to conduct their research on a regular basis. The method will choose for the study is the mixed research method. This will help the researcher learn to be more authentic so that reports can be accepted as they are. Additionally, it allows researchers to stay focused, improve their work quality, reduce resistance and save the time (Smith, 2015)[28]. Researcher will conduct a survey with various stakeholders of the legal industry to ascertain the effectiveness of current cybercrime laws.

Research design

It can be argued that the research design shows the part between quantitative and qualitative analysis. Similarly, research design helps to collect data from various sources and review them as needed. The three key research designs are descriptive, exploratory, and explanatory. In the present study, researcher will use a descriptive research design. The purpose behind the use of descriptive research design is that the researcher can achieve higher outcomes in their studies through this design (Saunders*et al.* 2015)[29].

Data collection method

Data collection methods are used to find solutions to research questions. There are two categories of data collection depending on the type of data as primary and secondary data collection method. Therefore, data collection is based on calculations and scientific

[26] Flick, U., 2015. Introducing research methodology: A beginner's guide to doing a research project. Sage.

[27] Jamshed, S., 2014. Qualitative research method-interviewing and observation. Journal of basic and clinical pharmacy, 5(4), p.87.

[28] Smith, J.A. ed., 2015. Qualitative psychology: A practical guide to research methods. Sage.

[29] Saunders, M.N., Lewis, P., Thornhill, A. and Bristow, A., 2015. Understanding research philosophy and approaches to theory development.

estimations in many settings. To learn today about customer satisfaction with the quality of service, researcher will use the mixed research method as the main method of data collection to get a better idea. The researcher will conduct the interview through a questionnaire to receive feedback from legal stakeholders (Kumar, 2019)[30].

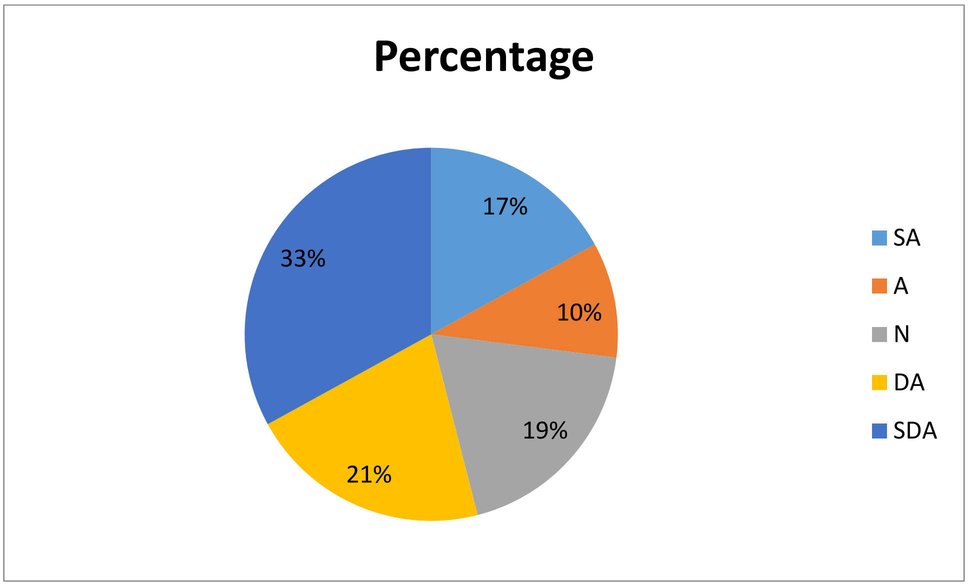
Ethics consideration

This is considered as the most important part of all research studies. It is important to maintain ethical guidance forthe researcher studies during collecting information from the respondents. The researcher should maintain the research ethics by maintaining appropriate ways of retaining the information shared by the participants. Accordingly, the researcher must preserve the privacy of the respondents (McCuskerand Gunaydin, 2015)[31].

VII. Findings and Analysis

Cyber Crime is a form of crime which needs strict and swift action?

Variable	Response	Percentage
SA	17	17
A	33	33
N	19	19
DA	21	21
SDA	10	10



[30] Kumar, R., 2019. Research methodology: A step-by-step guide for beginners. Sage Publications Limited.
[31] McCusker, K. and Gunaydin, S., 2015. Research using qualitative, quantitative or mixed methods and choice based on the research. Perfusion, 30(7), pp.537-542.

Table 1 shows the responses recorded against the above question. It was found that 17 percent of the participants were found to be strongly agreeing with the researcher, 33 percent of the participants were found to be agreeing with the researcher, 19 percent of the participants were found to be neutral, 21 percent of the participants were found to be disagreeing with the researcher and 10 percent of the participants were found to be strongly disagreeing with the researcher.

India is one of the hubs for cybercrimes due to its large tech savy population?

Variable	Response	Percentage
SA	20	20
A	29	29
N	11	11
DA	25	25
SDA	15	15

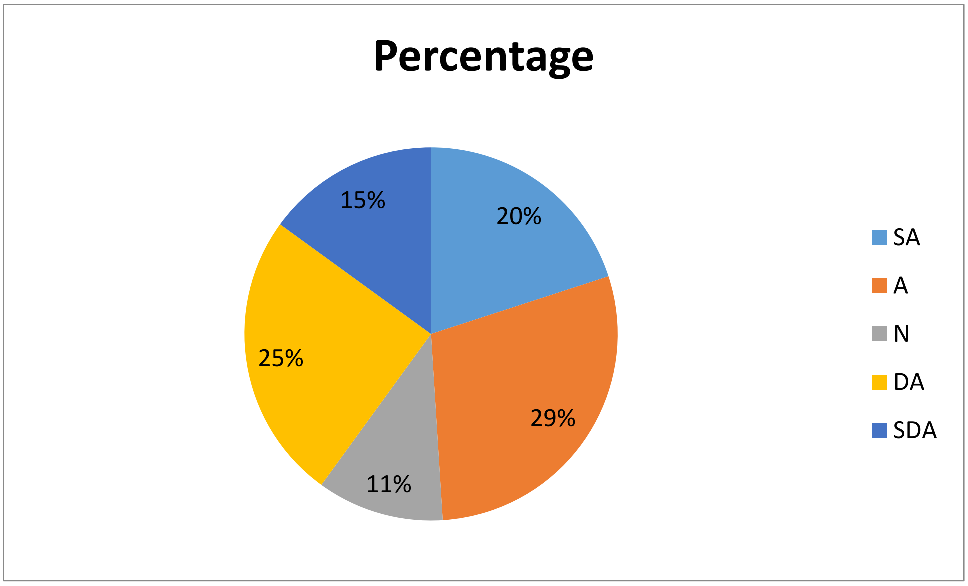


Table 2 shows the responses recorded against the above question. It was found that 20 percent of the participants were found to be strongly agreeing with the researcher, 29 percent of the participants were found to be agreeing with the researcher, 11 percent of the participants were found to be neutral, 25 percent of the participants were found to be disagreeing with the researcher and 15 percent of the participants were found to be strongly disagreeing with the researcher.

Cybercrimes can effectively cripple the infrastructure of an area if kept unchecked?

Variable	**Response**	**Percentage**
SA	20	20
A	23	23
N	16	16
DA	21	21
SDA	20	20

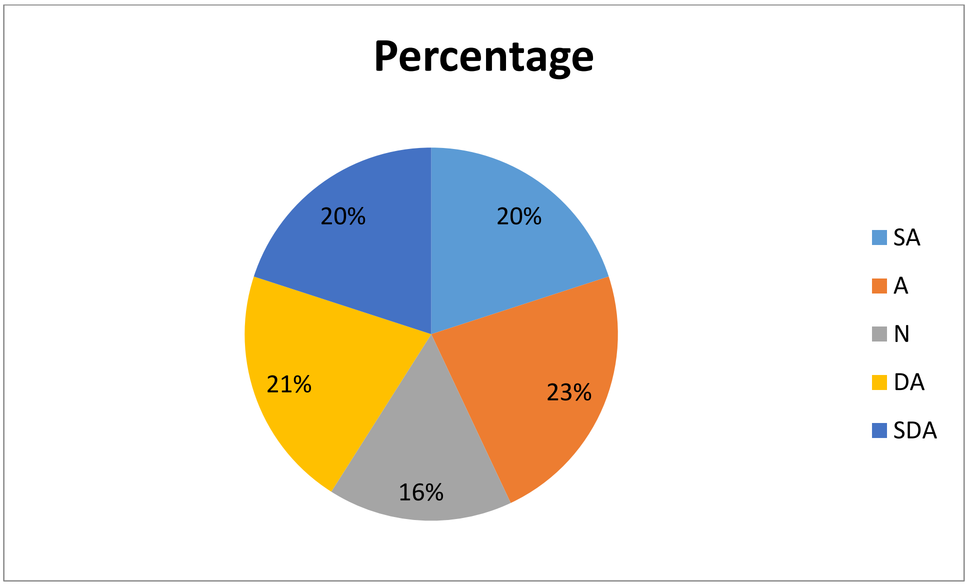


Table 3 shows the responses recorded against the above question. It was found that 20 percent of the participants were found to be strongly agreeing with the researcher, 23 percent of the participants were found to be agreeing with the researcher, 16 percent of the participants were found to be neutral, 21 percent of the participants were found to be disagreeing with the researcher and 20 percent of the participants were found to be strongly disagreeing with the researcher.

In some scenarios it is extremely difficult to track cyber criminals?

Variable	**Response**	**Percentage**
SA	10	10

A	26	26
N	15	15
DA	30	30
SDA	19	19

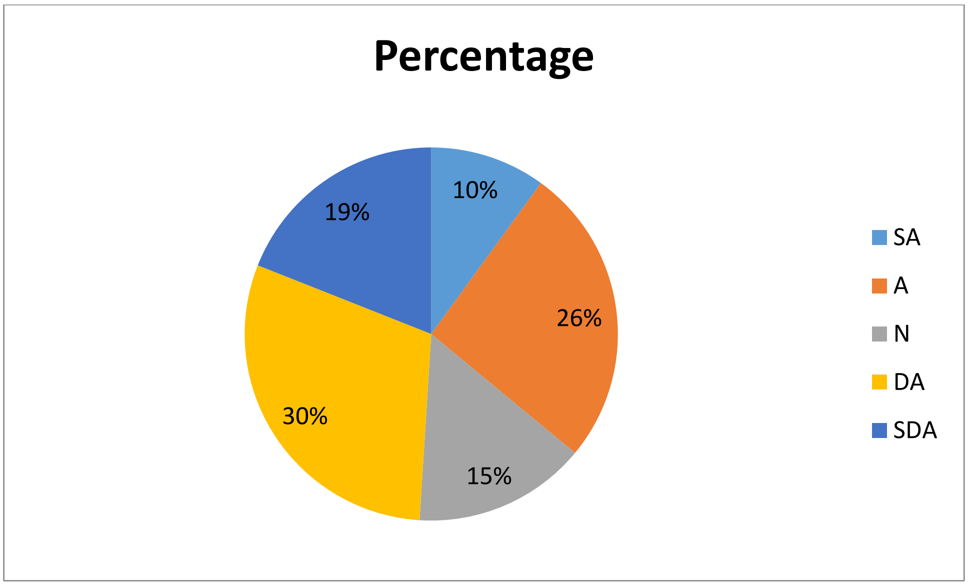


Table 4 shows the responses recorded against the above question. It was found that 10 percent of the participants were found to be strongly agreeing with the researcher, 26 percent of the participants were found to be agreeing with the researcher, 15 percent of the participants were found to be neutral, 30 percent of the participants were found to be disagreeing with the researcher and 19 percent of the participants were found to be strongly disagreeing with the researcher.

Indian cyber laws are adequate to prevent future cybercrimes?

Variable	**Response**	**Percentage**
SA	23	23
A	40	40
N	7	7
DA	18	18

SDA	12	12

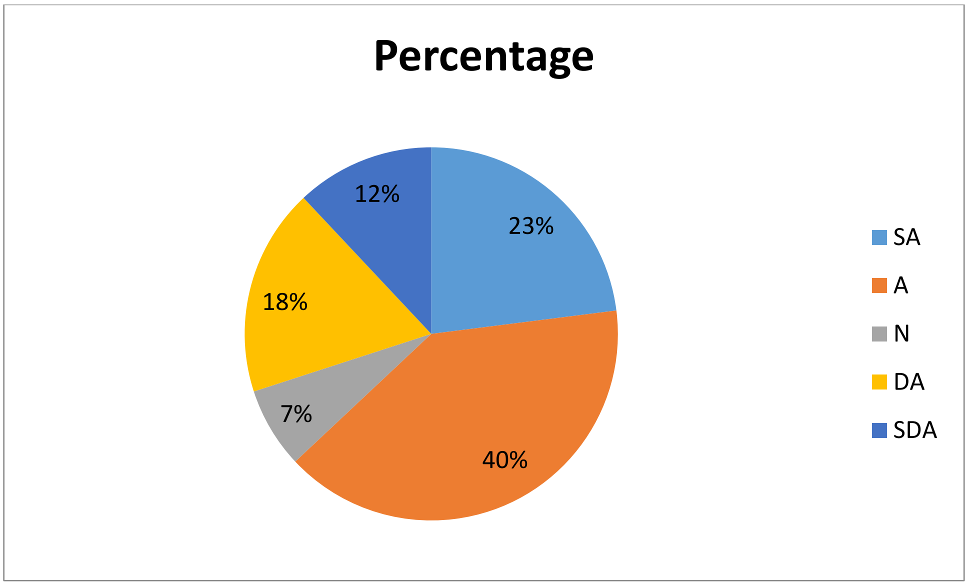


Table 5 shows the responses recorded against the above question. It was found that 23 percent of the participants were found to be strongly agreeing with the researcher, 40 percent of the participants were found to be agreeing with the researcher, 7 percent of the participants were found to be neutral, 18 percent of the participants were found to be disagreeing with the researcher and 12 percent of the participants were found to be strongly disagreeing with the researcher.

Indian cyber laws needs an overhaul?

Variable	Response	Percentage
SA	19	19
A	61	61
N	5	5
DA	10	10
SDA	5	5

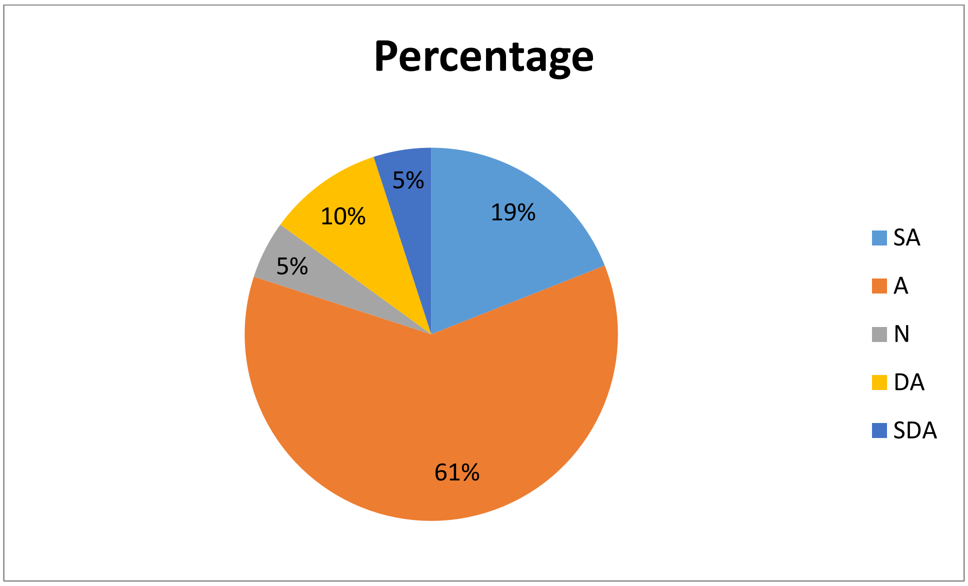


Table 6 shows the responses recorded against the above question. It was found that 19 percent of the participants were found to be strongly agreeing with the researcher, 61 percent of the participants were found to be agreeing with the researcher, 5 percent of the participants were found to be neutral, 10 percent of the participants were found to be disagreeing with the researcher and 5 percent of the participants were found to be strongly disagreeing with the researcher.

Separate dedicated units and courts are required to curb cybercrimes?

Variable	Response	Percentage
SA	20	20
A	42	42
N	8	8
DA	18	18
SDA	12	12

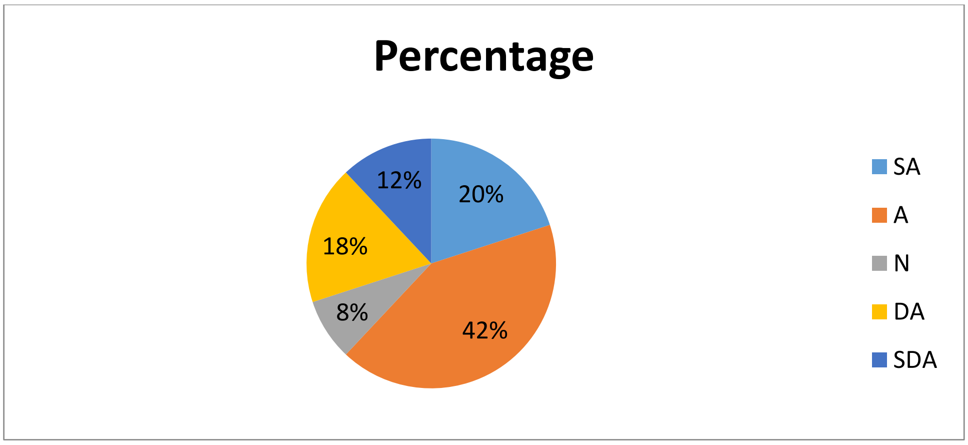


Table 7 shows the responses recorded against the above question. It was found that 20 percent of the participants were found to be strongly agreeing with the researcher, 42 percent of the participants were found to be agreeing with the researcher, 8 percent of the participants were found to be neutral, 18 percent of the participants were found to be disagreeing with the researcher and 12 percent of the participants were found to be strongly disagreeing with the researcher.

VIII. Conclusion

The cybercrime as contented earlier as a generic term, which is not having any specific definition, it can refer to all criminal activities done by using the new techniques of the ICT, means computer, internet and the cyber space. Cybercrime not defined in the Information Technology Act 2000, though it is call as a cyber law of India. Indian penal code also not defines the term cybercrime. Apart from this if, we see the conventional crime, the Indian penal code is recognized as a criminal Law, which deals with the traditional crime, however the term crime is not define in Indian Penal Code, though it is criminal law of India. Indian Penal Code only defines the term, offence under section 40 of the Act. Therefore, cybercrime and crime are not different. Even the conventional criminal law or the cyber laws are unable to define the concept of cybercrime and crime. Therefore, the Indian Penal code is applicable in various offences thought that crimes are known as a cybercrime. Indian Penal code amended along with the enactments of the Information Technology Act, 2000. All the offences, which are provided, in this Act are already going to be cover in the Indian Penal code. When any offence is going to registered under the Information Technology Act, 2000, the Indian Penal code is attracted and the relevant provisions are applicable to those offences. It shows that the conventional criminal law, Indian Penal code is competent to deals with the cybercrimes. After the amendment, the offences like defamation, forgery, cheating committed through the internet and computer are now consider as offence according to the Indian Penal Code. Before the amendments in the IT Act, there are various loopholes in the said Acts, various criminal activities are beyond the preview of the Act, due to that reason the Informational Technology Act, 2008 was enacted which bring various changes in the Act and tries to cover various criminal activities going to perform by using internet as a tool, but then also the Indian Penal Code is needed and made applicable in various cybercrimes as like hacking, data theft, cheating by internet.

*****

IX. References

1. Anuradhe Parasar (2006): Impact of internet on society, Page 3.
2. Broadhurst R and Grabosky P (2005), “Cyber-Crime : The Challenge in Asia”, University of Washington Press.
3. Cyber Crime law & Policy Perspectives, Dr. Mrs. K. Sita Minikyan (2009), Hind Law House Pune, Page 198.
4. Edappagath, Ajmal (2004), “Cyber Law and Enforcement in the Newsletter “Information Technology in the Developing Countries” published by International Federation for Information Processing (IFIP) , Vol. 14, Dec. 3.
5. Flick, U., 2015. Introducing research methodology: A beginner's guide to doing a research project. Sage.
6. Guide to cyber Laws, Rodney D. Ryder,(2003) Wadhwa Nagpur, Page 2.
7. Hammond IV, Allen (2001), “The 2001 Council of Europe Convention on Cyber-Crime: An Efficient Tool to Fight Crime in Cyber-Space?’
8. Jamshed, S., 2014. Qualitative research method-interviewing and observation. Journal of basic and clinical pharmacy, 5(4), p.87.
9. Jewkes, Yvonne (2006), “Cyber Crime and Society”.
10. Juster K I (2004), “Cyber security: A Key to U.S.-India Trade”
11. Karve, U (2002), “In info age, time for cyber savvy cops” Yours V 2.0 Frequently Asked Questions.
12. Kumar, Atul (2002), “Cyber Crime - Crime without Punishment, available at:http://unpanl.un.org/intradoc/groups/public/documents/APCITY/UN PAN002368.pdf
13. Kumar, R., 2019. Research methodology: A step-by-step guide for beginners. Sage Publications Limited.
14. L. C. Amarnathan, Cyber crime prevention and control strategies March 2002, CBI bulletin 5 DIG.
15. Law of Crimes (Indian Penal Code, 1860) S.R.Myneni, (2009) Asia Law House, Hyderabad, Page 2.
16. Maini, Rakesh, Hindu Business Online (2005), “Cover against cyber crimes vital” — Insurance industry seeks tighter IT Act, tools to assess losses,Thursday,

2004,www.blonnet.com / 2005/11/24/ stories / 2005112402750400.html

17. McCusker, K. and Gunaydin, S., 2015. Research using qualitative, quantitative or mixed methods and choice based on the research. Perfusion, 30(7), pp.537-542.

18. Nanda (2006), “Cyber Crimes and Real World”, www.boloji.com

19. P S A Pillai’s Criminal law, K.I. Vibhute (2014) LexisNexis, Gurgaon. Page 41.

20. Patil, Ramu (2001), “Cyber Policing: Setting a Thief to catch another”, New Indian Express

21. Poppat (2000), BBC News, “India Tackles Cyber Crime” www.news.bbc.co.uk/ 1/hi/ world/ south_asia/847727.stm

22. Raghavan R K(2004), “Catching the Cyber Criminar in “Frontline”

23. Saunders, M.N., Lewis, P., Thornhill, A. and Bristow, A., 2015. Understanding research philosophy and approaches to theory development.

24. Smith R G et al (2004), “Cyber Criminals on Trial” Cambridge University Press.

25. Smith, J.A. ed., 2015. Qualitative psychology: A practical guide to research methods. Sage.

26. Tippoo S (2001), “Cyber Crime: Are YOU safe?”, Times of India

27. Vaidya-Kapoor, Gopika (2003), “Byte by Byte”, Net Guide, February, 18, www. rediff. com/ netguide/2003/feb/18crime. html

*****