International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

HUMAN RIGHTS IN CYBER WORLD

Prajakta Amit Patil
F. G. Naik College of Arts, Sci (IT) and Commerce, Koperkhairne, Navi Mumbai

ABSTRACT
This paper focuses on Human Rights in cyber world and their violation by personally and groups as well as due to commission of cybercrimes and applications of laws.

Cyberspace is virtual communicative space created by digital technologies. It is not limited to operation of computer networks, but also encompasses all social activities in which digital information and communication technologies are deployed. Point of global concern arises when we talk about safeguarding human rights in cyberspace. When we talk about human rights and cyberspace, we also talk on the issue of cybercrimes.

Crimes which are done on internet or by making internet a medium are known as cyber-crimes. Many of time cyber criminals perform such crimes which violates human rights of individuals.

The solution which the legal authorities take out to combat this issue is by limiting the content which is being posted on internet which in turn curtails the human rights of the individuals.

Thus, human rights on cyberspace are violated in both ways, by crimes also and by application of laws also.

International organizations have now started to take this issue seriously and laws are being made on this issue.

Keywords: Human Rights, Cyber Space, Cyber Crime, Hacking, Cyber Security, Cyber World

INTRODUCTION:

Whatare the Human Rights and why do Human Rights in Cyber World matter?

Human rights are rights which are provided to an individual by virtue of him being a human being.

The concept of human rights acknowledges that every single human being is entitled to enjoy his or her human rights without distinction as to race, colour, sex, language, religion, political or otheropinion, national or social origin, property, birth or other status.

Human rights are legally guaranteed by human rights law, protecting individuals and groups against actions which interfere with fundamental freedoms and human dignity.

Cyberspace is the virtual communicative space created by digital technologies. It is not limited to the operation of computer networks, but also encompasses all social activities in which digital information and communication technologies (ICT) are deployed.

Human Rights in cyber space is a new field of global concern. With the advent of internet and the popularity which it has gained in the recent years,it is necessary to monitor the cyber space and protect the human rights of people in it.

As we increasingly conduct our lives online – shopping, socializing and sharing information – our digital rights, particularly the rights to privacy and freedom of expression, are becoming more important.

We need to understand how our data is being used by companies, governments and internet giants such as Facebook and Google. Is it being handled fairly and scrupulously, or sold or shared without our consent.

The internet provides you a platform to exercise the right to freedom of expression and information Misuse of this information and violation of our basic human rights in Cyber World has given birth to a new category of crime and criminals i.e., cyber crime and criminals.

Cyber criminals are intruding into the private lives of the individuals thereby infringing the human rights of internet users. Internet is a strong medium of expression of your ideas and thus it should be without any restrictions. To control and supervise criminal activities on internet, human right of expression many at times can be violated.

Human rights in Cyber world

Human rights in Cyber World should not only be articulated as individual rights, but should be recognized both as individual and as collective rights.

1)UNIVERSALITY AND EQUALITY: All humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.Everyone is entitled to all rights and freedoms

ISSN 2394 - 7780

without distinction of any kind, "such as ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status".

for e.g

- Persons with disabilities have a right to access, on an equal basis with others, to the Internet.
- Gender equality -Women and men have an equal right to learn about, define, access, use and shape the Internet.
- Net neutrality and net equality - The Internet is a global commons. Its architecture must be protected and promoted for it to be a vehicle for free, open, equal and non-discriminating exchange of information, communication and culture

2) RIGHTS AND SOCIAL JUSTICE: Everyone has the duty to respect the human rights of all others in the online environment.

e. gOn the Internet the right to an appropriate social and international order includes:

Rights includes Protection against all forms of crime, right to enjoy secure connections to and on the Internet

Persons with disabilities have a right to access, on an equal basis with others, to the Internet.

The Internet and the communications system must be governed in such a way as to ensure that it upholds and expands human rights to the fullest extent possible

The Internet as a social and international order shall enshrine principles of multilingualism, pluralism, and heterogeneous forms of cultural life in both form and substance.

3) ACCESSIBILITY: Everyone has an equal right to access and use a secure and open Internet. The right to access to, and make use of, the Internet shall be ensured for all and it shall not be subject to any restrictions except those which are provided by law, are necessary in a democratic society to protect national security, public order, public health or morals or the rights and freedoms of others, and are consistent with the other.

4) EXPRESSION AND ASSOCIATION: Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural or other purposes.

5) PRIVACY AND DATA PROTECTION: Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity, right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.

No one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference or attacks

6) LIFE, LIBERTY AND SECURITY: The rights to life, liberty, and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

On the Internet, the right to life, liberty and security includes:

Every one shall be protected against all forms of crime committed on or using the Internet

Everyone has the right to enjoy secure connections to and on the Internet.

Everyone has the right to seek, receive and impart information and ideas through the Internet.

The freedom and pluralism of the media shall be respected.

Freedom of Religion and Belief -includes freedom, either alone or in community with others and in public or private, to manifest his or her religion or belief in teaching, practice, worship and observance.

7) DIVERSITY: Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression

e.gAll individuals and communities have the right to use their own language

Right to participate in the cultural life of the community

8) NETWORK EQUALITY: Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritization, filtering or traffic control on commercial, political or other grounds.

9) DUTIES AND RESPONSIBILITIES:

Everyone has duties to the community in which alone the free and full development of his personality is possible.

Everybody has the duty and responsibility to respect the rights of all individuals in the online environment

Power holders must exercise their power responsibly, refrain from violating human rights and respect, protect and fulfill them to the fullest extent possible.

Cyber Crimes affecting Human Rights and Human Rights Protection in Cyberspace

When we talk about the human rights and cyberspace, we also talk on the issue of cybercrimes.

Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.

Also Cybersecurity laws and policies have a direct impact on human rights, particularly the right to privacy, freedom of expression, and the free flow of information.

Policymakers have created several national policies with the intention of protecting the Internet and other information communication technologies (ICTs) systems against malicious actors.

However, many of these policies are overly broad and ill-defined, and lack clear checks and balances or other democratic accountability mechanisms, which can lead to human rights abuses and can stifle innovation.

For example, extreme cybersecurity laws can be used to censor dissidents, monitor communications, and criminalize online users for expressing their views.

Thus the human rights on the cyberspace are violated in both the ways, by crimes also and by application of laws also.

The international organizations have now started to take this issue seriously and laws are being made on this issue.

Cyber laws are formed by International Organizations -

1)To protect the basic needs and interests of individuals in cyber-world

2)To Prevent misuse of Basic Human rights Cyber world are prevented by incorporating Cyber laws .

Under International law, states are legally obliged to respect, protect and fulfill the human rights of their citizens. Governments have the primary responsibility for realizing human rights within their jurisdictions. The duty to protect requires governments to protect against human rights violations committed by other actors, including businesses. States are also obliged to take appropriate steps to investigate, punish and redress human rights abuses which take place within their territory and/or jurisdiction.

However, other actors also have responsibilities under the International human rights regime. The Universal Declaration of Human Rights calls on "every individual and every organ of society" to promote and respect human rights. While these responsibilities do not equate to legal obligations (unless they have been enacted as such under national legislation) they do form part of prevailing social norms which companies and other private organizations should respect.

Thus while the primary responsibilities under the Charter remain with governments, the Charter also provides guidance to governments about how they must ensure that private companies are respecting human rights, and guidelines to companies about how they should behave so as to respect human rights in the Internet environment.

The Indian Parliament passed the Information Technology Act 2000 and amended in 2008 on the United Nations Commissionson International Trade Law (U.N.C.I.T.R.A.L) model Law.

The law defines the offences in a detailed manner along with penalties foreach category of offences. Thus cyber laws are the safe savior tocombat cyber-crime.

ISSN 2394 - 7780

CONCLUSION

As world is becoming too small as everybody is connected to cyber space ,as technology advances ,Cyberspace with its benefits has a darker side also and marks the presence of cyber-crimes which ultimately lead to the violation of human rights.

To overcome and protect human rights in cyber world ,Apart from Governing bodies which implement Cyber laws to prevent cyber crimes , it is everybody's responsibility of protecting individualsand groups against actions which interfere with fundamental freedoms and human dignity.

FUTURE WORKS

The future of human rights in cyberspace depends on the evolution of the laws and its interpretation in continuouslychangingtechnologies. Internationally acceptable laws should be there to safeguard the human rights of the individuals in the cyberspace.

Future work needed in this space for countries to acceptance and implementation "Internationally Acceptable Standard" for Protection of Human Rights in Cyberspace.

REFERENCES

- https://www.religion-online.org/article/human-rights-in-cyberspace/
- https://en.wikipedia.org/wiki/Human_rights_in_cyberspace
- https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf
- https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer
- http://ijldai.thelawbrigade.com/index.php/2017/05/24/the-flip-side-of-curbing-cyber-crimes-violation-of-human-rights/
- https://www.humanrights.gov.au/sites/default/files/document/publication/human_rights_cyberspace.pdf
- http://docs.manupatra.in/newsline/articles/Upload/C4971E8F-86E8-48E1-886B-CEF0B774397F.pdf

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER CRIME & CRIMINAL LAW

Chinmayi S. Vaidya
F. G. Naik College of Arts, Science (IT) and Commerce

ABSTRACT

Cybercrime is defined as a crime in which a computer is used as a tool to commit an offense .Cybercrimes are responsible for the interruption of normal computer functions.which may lead to fraud. This research paper covers the following topics of Cybercrimes :- the definition, why they occur, laws governing them, cybercrime prevention procedures.The number of people using internet is increasing day by day which has led to the rise in cybercrime.Lack of knowledge among people contributed to the growth in cybercrime .

Keywords: CyberCrime, Hacking, Internet, Cyber Laws, Breach

INTRODUCTION

With the advent of internet, a number of crimes related to the same have emerged. The space within which the internet operates is known as cyber space. The term cyberspace was originally coined by science fiction writer William Gibson.It is also called as "Hacking".

Internet is major source of Cyber Crime. This includes anything from downloading to stealing millions of dollars from online bank accounts. Cybercrime also includes other offenses, such as making viruses on other computers or stealing confidential information

Following are the examples of cybercrime.

1) Internet Fraud.

2) Spams.

3) Cyberbullying.

4) Gathering Information Illegally.

5) Identity Theft.

6) Phishing scams.

7) Hate Crimes.

Defining the Problem

We are duscussing about CyberCrimes.There are so many ways to define CyberCrime.Basic definition of CyberCrime is to steal or process information of an individual without their knowledge using computer and the internet.Some popular definitions are:

- **Webopedia**:-Cyber crime encompasses any criminal act dealing with computersand networks (called hacking)
  (https://www.webopedia.com/TERM/C/cyber_crime.html)
- **ResearchGate:**-Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.

  (https://www.researchgate.net/publication/265350281_Cybercrime_definition)
- **SearchSecurity**Cybercrime is any criminal activity that involves a computer, networked device or a network.

  https://searchsecurity.techtarget.com/definition/cybercrime
- **BritaniccaCybercrime**, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealingidentities, or violating privacy.

  https://www.britannica.com/topic/cybercrime

Laws of cybercrimes

In this section of this paper we'll discusses different Laws that governs cybercrime

ISSN 2394 - 7780

CYBER LAWS IN INDIA

1. **IT Act of India, 2000** The IT Act of India was passed by the Indian Government in May 2000.it contains the various cyber laws of the state. It is the law that deals with cybercrime and e-commerce. The Act was based on the United Nations Model Law on Electronic commerce. The Act aims to provide legal structure for all electronic transactions in India. Chapter IX of the Act states about the various penalties for cybercrime offences. The Act also talks about the compensation for the victims affected by cybercrime which does not exceed Rs. 100, 00,000. The Act talks about the various offences that can be classified as cybercrime.

2. **National Cyber Security Policy, 2013** This act was formalized by the Indian Government in 2013. It was taken as a step to counter cybercrime. The purpose of this document is to ensure a secure a safe cyberspace for the citizens of India. The policy states that education and training programmes are required for reducing the cybercrime rate. The policy aims to create 500,000 professionals within 2018 through advanced training and skill development programs.

3. **Cyber Swachhta Kendra** The Cyber Swachhta Kendra is an initiative taken up by the Government of India to create a secure cyberspace by detecting botnet infections and to enable cleaning and securing systems of users so as to prevent further infections. This policy is set up in accordance with the objectives of the 'National Cyber Security Policy.

Cyber Laws in United States

Federal Government Regulation

There are three main federal cybersecurity regulations –

– 1999 Gramm-Leach-Bliley Act

– 2000 Homeland Security Act, which included the Federal Information Security Management Act (FISMA)

Recent Federal Laws

Cybersecurity data Sharing Act (CISA) – Its objective is to enhance cybersecurity within the us through increased sharing of knowledge regarding cybersecurity threats, and for alternative functions.The law permits the sharing of web traffic data between the U.S.government and technology and manufacturing companies. The bill was introduced in the U.S.Senate on July ten, 2014, and passed within the Senate Oct twenty seven, 2015.

Federal Exchange information Breach Notification Act of 2015: This bill needs a insurance exchange to advise every individual whose personal info is thought to own been nonheritable or accessed as a results of a breach of security of any system maintained by the exchange as before long as potential however not later than sixty days when discovery of the breach.

PREVENTION:

How to protect yourself against cybercrime

1. Use a full-service internet security suite

Norton Security provides period protection against existing and rising viruses,worms,Trojan Horses i.e malware as well as ransomware and helps shield your personal and monetary info once you go surfing

2. Use strong passwords

Don't repeat your passwords on totally different sites, and alter your passwords often.

Make them complex. That means using a combination of at least 10 letters, numbers, and symbols.

3. Keep your software updated

It is very important to update your operating System to remove patches and loopholes.

Patching those exploits and flaws will create it less probably that you'll become a law-breaking target.

4. Manage your social media settings

Keep your personal and private information secure. Social media cybercriminals can get your information on a just one click.

5. Strengthen your home network

It's a good idea to use virtual private network. A VPN will encrypt all traffic.

If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data.

It's an honest plan to use a VPN whenever you a public

6. Keep up to date on major security breaches
find out what info the hackers accessed and alter your positive identification forthwith.

7. Know what to do if you become a victim
If you are a victim of a cybercrime, you immediately contact to the local police and, in some cases, the FBI and the Federal Trade Commission. If you think cybercriminals have stolen your identity. These are among the steps you should consider.

Contact the companies and banks where you know fraud occurred.

Place fraud alerts and get your credit reports.

Report identity theft to the FTC.

Try Other Relevant ToolsPlagiarism Checker Grammar Checker Spell Checker

FINDINGS

Findings on internet usage
94.25% respondents download various content from the internet, while only 5.8% do not download anything. 68.1% of the total respondents admitted that they downloaded movies, 85.3% of the total respondents download music, 66.25 downloaded various study material while only 39.2% downloaded general content such as Apks, books, software, games etc. □ 27.5% respondents download content very frequently. 43% respondents download quite often. 20.3% respondents download less frequently. 7.7% rarely download any content while only 1.4% never downloads anything.

FINDINGS ON CYBERCRIME AWARENESS AND SAFETY

25.1% respondents are very aware about cybercrime. 51.7% know about cybercrime. 21.7% don't know very well about cybercrime, while only 1.4% doesn't know anything about cybercrime.

Findings on awareness on anti cybercrime schemes by government□ Only 5.3% respondents are very well aware of the anti cybercrime schemes. 18.3% just know about it. 31.3% have heard about it. 30.8% don't know very well and have little information regarding it. 14.4% don't know about it. □ 53.4% of the total respondents know about the Information Technology Act, 2000. 48.1% of the total respondents know about the National Cyber Security policy, 2013. 18.8% of the total respondents know about the Cyber Swachhta Kendra.

Findings on trust on the existing Cybercrime laws □ Only 9% strongly agree that the cybercrime laws are strong enough to cybercriminals. 39.6% respondents agree that they are effective to control cybercriminals. 18.5% respondents disagree that the laws are effective while 6.3% strongly disagree that the laws are powerful enough to control and stop the cybercriminals. 26.6% respondents are on both sides, they are neutral. □ 15.8% strongly agree that the cybercrime can be completely eliminated in Kerala. 41.9% agree that the cybercrime can be eliminated in Kerala. However 14.4% disagree to it and 2.7% strongly disagree to the belief that the cybercrime can be eliminated in Kerala. The remaining 25.2% are neutral to this thought
(https://acadpubl.eu/hub/2018-119-16/1/130.pdf)

CONCLUSION

In Cybercrime internet is weapon to steal the information. Only remedy to the Cyber Crime is awareness among people.This basic awareness can help prevent potential cybercrimes against them.Training programs for youngsters helps a lot to reduce Cyber Crimes.The only possible step is to make people aware of their rights and duties and to make a law which is more strict.

REFERENCES

- (International Journal of Pure and Applied Mathematics Volume 119 No. 16 2018, 1353-1360 ISSN: 1314-3395 , page no-3,Sreehari A, K.J Abinanth, Sujith B, Unnikuttan P.S, Mrs.Jayashree)
- http://www.cameron.edu/search?cx=014940064196211141993%3Aottnfsmx9t0&cof=FORID%3A11&q=2_Hackers.docx
- Laws Relating to Cyber Crimes: Theories and Legal Aspects by Aqua Raza https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066200
- https://techterms.com/definition/cybercrime
- https://acadpubl.eu/hub/2018-119-16/1/130.pdf
- https://www.researchgate.net/publication/322086317_CyberCrime_and_Security
- https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html