The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 3 | March 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Protecting Human Rights in the Face of Cybercrime and Cybersecurity Threats

Dr. Sabreena Ansari
Assistant Professor, Modi Law College,
Kota, Rajasthan, adv.subreena@gmail.com

Anjali Kumari
Research Scholar, Babasaheb Bhimrao Ambedkar University,
Lucknow , U.P., kumarianjali281@gmail.com

Avinash Shandilya
Research Scholar, University of Allahabad, U.P.
avinashcs0029@gmail.com

ARTICLE DETAILS

Research Paper

Accepted on: 24-03-2025

Published on: 15-04-2025

Keywords:

Cyber space, Information Security , Phishing, Human Rights, Cyber space, Cyber crime, Hacker

ABSTRACT

In this technologically advanced age, where your computer contains everything, It has become much simpler to obtain almost any information that we desire. In less than a second, we can connect with someone in any country. Although technology and the internet have improved our lives and made them easier for us, there are also many negative aspects to them. The internet and digital communication technologies have opened up vast opportunities for people of all ages, including students, to share knowledge and access information. People are connecting with one another through email, chat rooms, and social media sites like Facebook, Whatsapp, Twitter, etc., so it is not overstated. However, as more people use the internet, the rate of cybercrime is also rising quickly. Cybercriminals can easily breach sensitive data, and crimes in cyberspace are becoming increasingly common. Hackers equipped with sophisticated technology and backed by organized cybercrime groups. For example, a hacker might be hired to install malicious software on someone's device. Today's malware is

difficult to detect and is designed to steal information for financial gain. Some people think that hacking offers higher earnings than working in cybersecurity roles. Countless cases of bank fraud involve scammers calling victims and draining their bank accounts. This article develops the understanding and explores to the reader how cyber security in current technological world can be associated with as a part of Human Rights.

DOI : https://doi.org/10.5281/zenodo.15222728

"Human rights are not privilege conferred by the government . they are every human being entitlement by virtue of its humanity" - Mother Teresa

Cyber security

" Cybersecurity is a shared responsibility , and it boils down to this : in cybersecurity , the more systems we secure , the more secure we all are"

Jeh Johnson

Information security, also known as cyber security or IT security, is the medium of ensuring the Information accessibility, privacy, and accuracy. It includes a continuously changing set of tools, risk management techniques, technologies, training, and best practices to protect networks, devices, programs, and data from attacks or unauthorized access. The science of cyber security is paramount due to the rise of dependency of society on digital devices, Bluetooth, digital network, developing of smart devices and some other advanced gadgets which utilizes and manipulates users data of which abuse will put the concerned user to danger. Cyber security is necessary and thus will help in stoping someone from compromising this data.

Cyber security is an ever-evolving field because new cyber threats emerge with each new change, necessitating new security measures.

Several typical forms of cyber threats include

- *Malware*

- *Ransomware*
- *Phising*

A few prevalent forms of security are

Network: It protects your internal networks from maliciously motivated unauthorized access and secures your network by safeguarding infrastructure and preventing access to it.

Cloud computing : It guards and keeps an eye on the data stored in your cloud resources. To aid business users in better protecting their data. New security tools are constantly being developed and implemented by cloud providers.

Antivirus : It safeguards the data By checking the computer for known threats

Cybercrimes : any unlawful conduct directed at the safety of computer systems and the data they process through the use of electronic means. While in a broader sense it is defined as "Any illegal behaviour shown or committed by or in relation to a computer system or network, including such crimes as illegal possession and providing or disseminating information through a computer system or network."

In accordance with the IT Act of 2000, any criminal activity involving a computer or the internet that uses a computer as a tool is subject to internet security.

India is the third-ranked country worldwide among the top 20 countries that are victims of internet crimes, according to the Internet Crime Report for 2019, which was published by the United States' Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation.

Aside from the USA, the UK tops the list of victims of internet crimes, with 93,796 victims, followed by Canada (3,721) and India (2,901).

In India, a total of 27,248 cases of cybercrime were reported in 2018, according to data made public by NCRB. which calls for bank fraud were the most common. The Central government started the portal for National Cyber Crime Reporting last year, and it has already received 33,152 complaints, which lead to the filing of 790 FIRs.

Hacking or unauthorized access to computer networks: In this particular form of cyber crime the hackers by any means directly intrudes into the user computer or any network device by means of illegally access and therefore steal their stored data. Thereafter , they manipulate the retrieved information or sell it to third parties for exchange with money It is a common cybercrime in most nations, and most recently, hackers have gained access to the Twitter accounts of numerous famous people and committed cyberfraud.

Virus attack: Programs known as viruses generally attach themselves to a computer/digital device or a user file and then spread themselves and infect system and personel files or other connected terminals on that particular network. Mostly they have an influence on computer data by means of deleting or altering it. Whereas worms do not require a host to attach to, they replicate themselves. They merely create functioning copies of themselves, which they do repeatedly until they occupy all of the memory space on a computer. Example: I Love You; Love Letter; Girlfriend

Salami attack: It is an attack on a computer network where the intruder transfers small sums of money from one file to another one that is accessible to him or her. Taking a small amount of money out of X, Y, and Z's accounts, for instance, and depositing it into A's personal account

Cyber defamation: This happens when libel is committed using a computer or an internet network. As an illustration, sending offensive messages or an email to the target. When an employee of a company began sending disparaging, defamatory, and obscene emails about the company's managing director, it was determined that this was India's first case of cyber defamation. The emails were sent frequently and anonymously to many of their business partners in an effort to damage the company's reputation and goodwill.

Theft of computer system: It means stealing of any digital device like computer , or any accessory peripheral device attached to it .

"Security used to be an inconvenience sometimes, but now it's a necessity all the time"

Martina Navratilova

Cyber security , cyber rights and human rights

The World Wide Web (WWW) as well as the internet have been both into existence since the 1960s. According to the International Telecommunications Union, upto 76% of people in the developing

countries and around 40% of the world's population residing now male use of the internet .Government, business, and civil society organizations are increasingly using online platforms for gathering information and to share and service delivery. But due to increasing ambit of cybercrime as well as cyber security have expanded, a worrying querry has emerged: How will these issues affect human rights? Does it violate a person's right?

Cyber security and human right

There are numerous national and international laws that apply to cyber security, such as Article 19 in the UDHR, which talks about the right to freedom of speech, to communicate, and to have access to any information. Similarly, everyone has the right to life, liberty, and personal security, according to Article 3. However, it is challenging to enforce these rights due to international law. Consequently, many nations, including India, ignore the law.

Cyber security violates the rights to privacy, freedom of speech, freedom of the press, and free flow of information. The government has created a number of regulations to safeguard computers used for illegal purposes, but many of them are vague, lack democratic accountability systems, and have unclear checks and balances, which can lead to human rights abuses and hinder innovation. All of these events demonstrate how the state uses excessive force to maintain its existence and sees security as its own defense against political instability, which in turn feeds insecurity.

As we can see, social media sites have some limitations on what we are allowed to say, write, and post. Cyber security laws can frequently be used to censor critics, keep tabs on communications, and punish online users for expressing their opinions. Government officials have the right to monitor user communications at any time if they have reason to believe someone is not telling the truth. All of this is a flagrant violation of the UHDR's or the country's own law on human rights. As an illustration, Omar Abdulaziz's surveillance, which led to the extrajudicial killing of a journalist in Saudi Mr.Jamal Khashoggi. A litigation claims that Abdulaziz's mobile phone was targeted by spyware which was installed by the Saudi Arabian government, by putting in danger the confidentiality of his discussions about various opposition projects with Khashoggi and that too in the time period just before Khashoggi's murder.

Shreya Singhal v Union of India AIR 2015 SC 1523

Two girls were held to detention by the Mumbai state Police in 2012 for posting comments related to protesting the Shiv Sena's strike on the death of its chief. The petitioners were alleged of posting their comments on social media via Facebook and thereafter also liking them at the same time, which aroused a large-scale holler from the mass public. It was held that Whether Sections 66-A, 69-A, and 79 of the IT Act , 2000 are legally and constitutionally valid according to the situation of the case above And does Section 66A of the IT Act violate the freedom of speech and expression as a fundamental right?

Verdict

The court noted that because of the expressions in 66A's complete open-endedness and lack of definition, it is not protected by Article 19(2) of the Indian Constitution. In Actual terms , Section 66A had no proximate relationship or link to causing a disturbance in the peace or to inciting someone to commit a crime, so the court overturned it. The court attitude was that legislation cannot in any form curtail or restrict the fundamental right to freedom of speech and expression, and therefore this right is protected by Article 19(2) of the Indian Constitution.

Cyber crime and human rights

Cybercrime infringes on a number of human rights, including the right to secrecy, the right to be free from torture, and the right to privacy. Hackers frequently encrypt sensitive information belonging to users or businesses and demand a ransom to unlock them. They also steal data and use it for other purposes. Similar to the recent incident, where they hacked the Twitter accounts of numerous well-known individuals and used them fraudulently to steal money, some demanded payment to restore their accounts. By posting their videos and photos on various websites, they extort children and violate their rights.

Nascoom v Ajay Sood and others 119 (2005) DLT 596, 2005 (30) PTC 437 Del

Phishing on the internet was ruled to be unlawful in a landmark decision by the Delhi High Court, which entails an order and the reimbursement of damages. According to the court, *"_phishing is a type of internet fraud in which a perpetrator poses as a reputable organisation, like a bank or insurance company, in order to obtain personal information from a client, such as access codes, passwords, etc."* despite the fact that In India, there is no particular rule that penalizes Phising yet Delhi High Court mentioned that the commission of Phishing is still and can be considered as under passing off and hence liable to be punished for damaging Nasscom's reputation

One of the most well-known cybercrime incidents is the Bank NSP case, when a trainee in bank management was engaged to be married. Using the resources of company i.e., computers, the couple sent and received numerous emails. After a while, the two broke up, and the girl initiated to send emails to the boy's foreign clients using phoney email addresses like "Indianbarassociations." She was able to do such task by manipulating the bank's computer. When the boy's business lost a lot of customers, he sued the bank. And it was seen and taken into consideration the bank's system.

Conclusion

In India and all through all over the world the usage of science and technology has been increased on a huge scale and therefore a lot of dependency on these devices has been placed by the the human being . due to this there are various laws that have been enacted by the legislature to make ease the usage of technology as well as to overcome the issues associated with this technology . Cyber security is a collective term that focuses on the security related the technology used in day to day uses of it .In India there are itself a lot of penal provisions to prevent cybercrime, yet they seem to be ineffective due to nature of having large ambit of it .As the technology is developed by human some become hackers who are always coming up with new ways to get around cyber security and steal important information. Due to this it's a critical question on the issue of hindering the human rights of people . Government is therefore responsible for to making and implementing the policy that should be made to ensure that fundamental human rights are not violated. A legal, ethical analysis of the topic of surveillance, communications monitoring, privacy, consent, and technology is necessary. Only then would there be an opportunity to encourage accountability in the technologically advanced world of today and protect fundamental human rights

"Let's face it: the future is now. We are already living in a cyber society, so we need to stop ignoring it or pretending that is not affecting us"

Marco Ciapelli

References

1. https://psu.pb.unizin.org/ist110/chapter/12-2-computer-security/

2. https://www.legalserviceindia.com/legal/article-4724-cyber-security-and-cyber-crime-infringes-human-rights-.html
3. https://curiousforlaw.com/cyber-security-and-privacy-a-responsibility/
4. https://www.thelawgurukul.com/post/cybercrimes-and-the-regulation-of-cyber-laws
5. Mr. Karra Kameswara Rao " HUMAN RIGHTS AND CYBERSPACE_ USE AND MISUSE " *Bharti Law Review , July –Sept, 2016*
6. Vittorio Fanchiotti , Jean Paul Pierini " Impact of Cyberspace on Human Rights and Democracy*" 2012 4th International Conference on Cyber Confl ict*