Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2024 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Protection of Human Rights in Cyberspace

Anmol Chalana[a] Prof. (Dr.) Arvind P. Bhanu[b]

[a]Amity University, Noida, India [b]Additional director/Joint head, Amity Law School, Noida, India

Received 08 April 2024; *Accepted* 09 May 2024; *Published* 13 May 2024

The article discusses how the internet and cyber laws affect our rights and safety online. It explains that cyberspace, where we do things like email, online shopping, and social media, is vast and hard to control. Because of this, cybercrime, like hacking and identity theft, has become a big problem. The article also talks about how everyone should have the right to use the internet freely, without restrictions from the government. However, it acknowledges that sometimes, governments limit internet access for reasons like national security. The article points out that social media can both help and harm human rights. It can spread awareness about rights violations and allow people to share their experiences, but it can also invade privacy and enable online harassment. Overall, the article suggests that we need to find a balance between protecting ourselves from cyber threats and safeguarding our rights. It calls for better laws to fight cybercrime and more education for internet users to stay safe online. Additionally, it emphasizes the importance of quick action to help those who have been victimized by cybercrimes.

Keywords: *cyberspace, cybercrime, human rights, cybersecurity.*

CYBERSPACE AND CYBERCRIME: AN INTRODUCTION

Cyberlaw governs cyberspace. Cyberlaw covers 'data storage devices hard discs, computers, networks, software, USB (universal serial bus controllers) discs, pen drives, flash drives, etc.' the

websites, electronic messages, the internet, and electronic gadgets like mobile phones, ATMs, etc. Cyberspace is ungoverned by legislation. Cyberspace disregards jurisdiction.[1]

For Example: A hacker in India might potentially access the virtual safe of a bank that is stored on a computer in the United States and then transfer millions of dollars to a bank in Switzerland within a matter of minutes. It is sufficient for him to have a mobile phone, in addition to a laptop and a desktop computer.

The potential for anonymity in cyberspace is great. The primary target of cybercrime is electronic data. After its first publication, a software source code that is potentially worth crores of rupees might be stolen and distributed illegally over the globe in a couple of days, all thanks to the prevalence of cyberspace as the fundamental cause of piracy. Theft of physical data is greatly facilitated by the Internet since the 'actual' owner of the data never loses possession of the 'original,' yet the data is still taken in its entirety.

Cyberspace is an Internet-facilitated virtual reality. This area lacks substance and is purely conceptual. Messages sent in this region can only be sent from one computer to another over the Internet. Cyberspace facilitates efficient communication, allowing information to be sent from one physical location to another. Cyberspace has several potential uses, such as a marketplace, a platform for economic growth, a venue for entertainment 'virtual games and the expression of creative talents', and a medium for interpersonal communication.[2] Digital India estimates that there were 687.6 million people in India using the internet as of January 2020. This massive amount allows us to make educated guesses about Cyber Space in India and its expansion.

Any illegal activity that is carried out via a computer and an associated network is referred to as 'cybercrime'. The conduct of a crime may include the use of a computer, or the computer itself may be the target of the crime.[3]

[1] Rodney D. Ryder, *Guide to cyber laws : (information technology act, 2000, e-commerce, data protection & the Internet)* (Wadhwa 2001)
[2] SK Verma and Raman Mittal, *Legal Dimensions of Cyberspace* (Indian Law Institute, New Delhi 2004)
[3] *Ibid*

THE INTERNET AS A HUMAN RIGHT

The World Wide Web (WWW) first appeared in the 1990s, while the Internet itself dates back to the 1960s. However, cyberspace is still uncharted territory when it comes to the rights and obligations of individuals. The International Telecommunications Union reports that as of 2015, internet usage has grown to include more than 76% of the global population and about 40% of the global population in industrialised nations. Cyberspace platforms are being used by government, industry, and civil society groups to disseminate information and provide services. As a result, the internet has grown into a vital medium for the dissemination of ideas and information protected by the First Amendment. Freedom of thought, conscience, and expression are guaranteed under *Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR)*.[4]

The judgement that free and unrestricted access to the internet is a fundamental right for all citizens of the nation was handed down by the highest court in the state of Kerala. In 2017, Kerala was the first Indian state to proclaim that Internet access is a fundamental human right. As a direct result of this, the government of Kerala has made internet connection more inexpensive for everyone else while also providing free access to citizens of Kerala with low incomes. People living in Kerala will find it much simpler to access both the official and unofficial services offered by the state as a result of this change.[5] Due to the internet's ability to keep us constantly in touch with people all over the globe, it's hard to fathom a world without it.[6] The government has the right to limit people's access to the internet for reasons such as maintaining order and protecting the country's security. Nonetheless, the government and the state cannot limit residents' internet access. In a recent decision, the Supreme Court of India addressed the case of *Anuradha Bhasin v Union of India*.[7] Article 19(1)(a) of the Indian Constitution guarantees the right to access the internet. The internet was slowed down in the state of Jammu and Kashmir.

---

[4] International Covenant on Civil and Political Rights 1976, art 19(2)
[5] *Faheema Shirin RK v State of Kerala & Ors* AIR 2020 Ker 35
[6] Stephanie Borg Psaila, 'UN Declares Internet Access a Human Right' – Did It Really?' (*Diplo*, 10 June 2011) <https://www.diplomacy.edu/blog/un-declares-internet-access-human-right-did-it-really/> accessed 18 March 2024
[7] *Anuradha Bhasin v Union of India* (2020) 1 MLJ 574

The Supreme Court ultimately ruled that internet access is a basic human right and ordered the government of the state of Jammu and Kashmir to reverse its decision to restrict access to the internet across the region.

Everyone in the world needs to be able to express their ideas and viewpoints in any manner they deem appropriate, whether it is vocally, in writing or print, via the arts, or through any other medium of their choice. This right ought to extend to everyone. The *United Nations Commission on Human Rights (UNHRC)* provides extensive criticism of this paragraph in its General Comment number 3, which may be found here. According to a decision made by Human Rights Watch, the freedom to access information, ideas, and viewpoints through the internet and when it comes to civil and political rights, the International Covenant on 'the right to free expression, including the right to transmit this information to others.'[8]

To strike a fair balance between individual liberties and collective duties, the law often draws a line between public and private behaviour. There is less of a distinction due to the internet's fast expansion into more areas of everyday life.[9] People throughout the globe now consider their online pursuits to be an integral part of their daily lives.[10] They are so reliant on private conversations, that it is not an exaggeration to call them slaves i.e. 'always connected to friends; family, and social groups as in a virtual world'.

DIMENSIONS OF CYBERCRIME

With the expansion of the Internet came a corresponding rise in the frequency with which cybercrimes were committed throughout the globe. The criminals have devised a multitude of schemes to steal the money that people have worked so hard to obtain. The common cybercrimes are:

Phishing - In the cybercrime known as phishing, the perpetrators make contact with their intended victims by any available means of contact, including but not limited to phone calls,

[8] Asoke Mukerji, 'The Need for an International Convention on Cyberspace' (*cirsd*) <https://www.cirsd.org/en/horizons/horizons-spring-2020-issue-no-16/the-need-for-an-international-convention-on-cyberspace> accessed 15 March 2024
[9] *Ibid*
[10] *Ibid*

emails, and text messages. To fool users, a hacker might offer a fake website that looks and functions just like the real thing. Hackers can steal sensitive information like login credentials for online banking and credit card services if their victims input such information on the phished website. Addressing the case between *Yahoo and Akash Arora*[11], The defendant deceived and influenced others by creating a website that was very similar to Yahoo and then using that website. An assault of phishing with a very high level of intensity is known as a whale attack.[12]

Theft Scams - The cybercriminal behind this attack will assume the victim's identity and then use it to shop online under their name. Identity theft schemes have existed for as long as there have been people, but the Internet has made it much easier for criminals to steal someone else's personal information and pass themselves off as the victim. Updating your numerous accounts consistently is something that should be done to protect yourself against fraud involving identity theft. In the case of *Gagan Harsh Sharma v the State of Maharashtra*,[13] The defendants were found guilty under the IT Act and the IPC of committing identity theft against their employer.

Online Harassment - As a definition, 'online harassment' refers to any kind of harassment that is carried out with the use of the internet. Constant verbal or written abuse directed at one person is considered online harassment. India has passed a number of regulations to protect its citizens against cyberbullying. Victims of Online Harassment are more likely to be targeted on social media platforms like Facebook and Twitter. If you or someone you know has been the victim of Online Harassment, you may use the platform's reporting feature to help put an end to this terrible practice.[14]

Cyber-Stalking - It is illegal to engage in the practice of cyber-stalking, which consists of tracking another person online or maintaining tabs on their actions via the internet. The use of social media platforms by criminals as a means to perpetrate the offence of cyberstalking is a rather straightforward process. It is also possible for the perpetrators to infect the system of the

[11] *Yahoo!, Inc. v Akash Arora & Anr* 78 (1999) DLT 285
[12] Priyanjali Karmakar, 'Types of Cyber Crime and Its Causes' (*Legal Service India*) <https://www.legalserviceindia.com/legal/article-3042--types-of-cyber-crime-and-its-causes.html> accessed 18 March 2024
[13] *Gagan Harsh Sharma v the State of Maharashtra* (2019) CriLJ 1398
[14] 'The State of Online Harassment' (*Pew Research Center*, 13 January 2021) <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/> accessed 18 March 2024

victim with malware, which enables them to keep close tabs on the actions that are being carried out by the victims consistently.

Hacking - The purpose of hacking, which is a kind of cybercrime, is to obtain unauthorized access to a computer system in order to steal data or cause harm to the system. Typically, malware is used in hacking, and it is sent through the internet to infect the victim's machine. After a hacker assault on a control system, the legitimate user of the system will be unable to access the data contained there until the virus is uninstalled.[15]

CONCERNS REGARDING HUMAN RIGHTS AND CYBERSECURITY

Even though certain national and international laws make an effort to take human rights concerns into account when formulating cybersecurity standards, civil society advocates and Others have started to come to the realisation that broad and universal concepts and legislation about cybersecurity have a harmful effect on human rights. Most of the time, when we discuss human rights, we are talking about the rights that are protected by the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) of the United Nations.[16] Some of the most fundamental rights that all individuals have are the rights to express themselves freely, to speak their views without interference, to retain their privacy, to hold and express their beliefs, and to organise and join organisations of their choice. In July 2012, the United Nations Human Rights Council gave its approval of the idea by noting that 'the same rights that individuals enjoy outdoors must also be safeguarded online.' This indicates that the idea has widespread support.[17] As a direct consequence of this, the human

[15] 'Cybercrime' (*Encyclopedia Britannica*) <https://www.britannica.com/topic/cybercrime> accessed 15 March 2024

[16] Cees J. Hamelink, *Human Rights in Cyberspace* (University of Ottawa Press 1999)

[17] Kettemann M, 'UN Human Rights Council Confirms That Human Rights Apply to the Internet' (*Article 19*, 15 July 2021) <https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/#:~:text=UN%3A%20Human%20Rights%20Council%20adopts%20resolution%20on%20human%20rights%20on%20the%20Internet,-Posted%20on%20July&text=ARTICLE%2019%20welcomes%20the%20adoption,the%20UN%20Human%20Rights%20Council.> accessed 15 March 2024

rights proclamations outlined in the 'International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights' are now relevant to the use of the Internet.[18]

Following the attacks that took place at Charlie Hebdo at the beginning of 2015, the Prime Minister of the United Kingdom, David Cameron, expressed his support for a ban on encrypted communication services such as WhatsApp if the United Kingdom's security agencies were not granted greater access to messages and user data. To safeguard the United Kingdom from terrorist threats, Cameron argued for greater access to encrypted communications. Prohibiting encrypted messaging services may be seen as an attack on people's right to privacy and obscurity in the name of nationwide security via increased cyber monitoring and telephonic monitoring of communications. Individuals have the right to privacy so that their personal information is not shared with unauthorised parties.[19] It is essential that the Internet continues to serve as a medium for free speech, especially for persons who want to avoid being harassed, imprisoned, or subjected to other forms of retaliation due to their political or social views. Anonymity in the digital realm refers to the capacity to express oneself freely online without fear of having that expression connected to one's real-world identity. The United Nations Special Rapporteur on Freedom of Opinion and Expression issued a study on the effects of surveillance on human rights in 2013. The impact of monitoring on people's right to free speech was investigated. The United Nations Special Rapporteur expressed worry in his report about 'the exploitation of an undefined notion of national security to justify intrusive constraints on the enjoyment of human rights.'

Many national cybersecurity laws and procedures have the potential to limit citizens' willingness to exercise their First Amendment rights to free speech and press online or to infringe on those rights outright. In order to comply with the provisions of Saudi Arabia's Anti-Cyber Crime Law and its nebulous clause on 'protection of public interest, morals, and common values,' the country has imprisoned bloggers and others who have expressed dissenting views

[18] AG Noorani, 'Cyberspace and Citizen's Rights' (1997) 32(23) Economic and Political Weekly <https://www.jstor.org/stable/4405474> accessed 20 March 2024

[19] 'UK's Cameron says Paris attack 'sickening', says press freedom must be defended' (*Reuters*, 07 January 2015) <https://jp.reuters.com/article/us-france-shooting-cameron/uks-cameron-says-paris-attack-sickening-says-press-freedom-must-be-defended-idUSKBN0KG13120150107/> accessed 20 March 2024

online, insulted public authorities or backed opposition forces against the government that was already established. Libel has become a crime by the Philippines' Cyber Crime Prevention Act of 2012, which also targeted spam and child pornography.[20] Although the libel part was deleted the following year, it was the basic intentions of the bill that prompted Filipino activists and legislators to design a measure that was later given the moniker Magna Carta for Philippine Internet Freedom in order to voice their opposition. Filtering content on the internet is feasible because of the existence of government-created cybersecurity regulations as well as private-sector firewalls that get money and assistance from the government.

'Article 17 of the International Covenant on Civil and Political Rights (ICCPR) states that no one shall be subjected to arbitrary or unlawful interference with his privacy,' This clause, however, was deemed 'flexible enough to permit necessary, justified, and proportional limits to the right to privacy' by the 'United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while combatting terrorism in 2009.' The terms 'necessary and proportionate' and 'reasonable suspicion' are widely used to describe the circumstances under which various forms of surveillance, including internet monitoring, are permitted under international law and human rights-based standards. Freedom of expression, speech, privacy, and anonymity are joined by worries about ethnic and religious discrimination against Muslims in Western cybersecurity policy and the legitimacy of online protest. No one can be stopped from protesting, debating, or sharing their thoughts online, even if cyber threats are very real. Since governments and their agencies have access to and influence over the Internet, some have suggested that further precautions are required to keep its users' data secure. Internationally agreed-upon definitions of keywords are another example of these protections, along with monitoring bodies and international legislation.[21]

[20] 'Philippines: Cybercrime Law Threatens Free Speech and Must Be Reviewed' (*Amnesty International*, 4 October 2012) <https://www.amnesty.org/en/latest/news/2012/10/philippines-cybercrime-law-threatens-freedom-expression-and-must-be-reviewed/#:~:text=October%204%2C%202012-,Philippines%3A%20'Cybercrime'%20law%20threatens%20free%20speech%20and%20must%20be,of%202012%20(Republic%20Act%20No.> accessed 20 March 2024

[21] Paul M. Taylor, *Article 17: Privacy, Home, Correspondence; Honour and Reputation - A Commentary on the International Covenant on Civil and Political Rights* (CUP 2020)

SOCIAL MEDIA AND HUMAN RIGHTS

The term 'social media' refers to the many online platforms that encourage user-generated content and conversation. People from all over the globe can connect with anyone they want, whenever they want, thanks to social media. To varying degrees, depending on the context, social media may either protect or violate the human rights of individuals all over the globe.

Protection and promotion of human rights may both benefit greatly from the use of social media. First, it provides social media users with a foundational education on their human rights by raising their awareness of those rights and encouraging them to exercise them. Several social media awareness campaigns have been released, and human rights-related content is routinely updated across several platforms. Social media provides a platform for people to exercise their right to freedom of speech, which is a basic human right. The Supreme Court upheld 'the protection of this fundamental freedom of expression' in the case of *Shreya Singhal v Union of India*[22].

In addition to this, social media provides its users with a forum in which they are free to discuss their personal experiences of the violation of human rights. In addition to this, it gives anyone who believes their human rights have been infringed a simple and speedy way to report the violations. Social media platforms may serve as a repository for information, which can be mined for facts on the criminals and their whereabouts. The sanctions that are issued to those who violate human rights are brought to light on social media platforms, which serves as a deterrent to those who might otherwise violate human rights.

Users of social media platforms are more likely to be exposed to situations in which their human rights are violated. The one-of-a-kind user ID that is issued by the social media platform may be seen by any other member of the social media platform with very little effort. Because of its ease of access, the human right to privacy of people is often violated. 'This right is not only a human right but also a fundamental right,' According to the decision that was made in the case of Justice *K.S. Puttaswamy v Union of India*[23]. Teenagers who participate in online communities are an

[22] *Shreya Singhal v Union of India* (2013) 12 SCC 73
[23] Justice *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1

obvious target for individuals who abuse human rights. In addition, several terrorist organisations use social media platforms to access people's accounts and steal their personal information.

Through the use of social media platforms, it is much simpler to disseminate any inappropriate message or information that is directed against a specific person or group of people in particular. Because the information that is uploaded is readily available to the general public and may be accessed by users of social media platforms in a short amount of time, social media platforms have the potential to be used in order to commit crimes such as cyberstalking and online harassment.

CONCLUSION

There have been many international accords put into effect that are connected to cybercrime. In general, The criminality, investigative procedures and authorities, digital evidence, regulation and risk, jurisdiction and international cooperation, and other thematic components of existing global and regional legal instruments and state laws differ widely. These treaties also vary in terms of their applicability and the regions they cover (i.e., whether they are multilateral or regional). This variation creates further challenges for identifying, investigating, and punishing cyber criminals, as well as preventing cybercrime.

There must be safeguards in place to prevent the abuse of Internet censorship legislation and to guarantee that they are consistent with the rule of law and human rights. These regulations limit what may be seen and downloaded online. To prevent laws from being misused to illegally restrict access to content, there must be more clarity in the law. The only way to do this is to make the meaning of current laws more explicit. When laws and investigative powers that were first enacted to target one sort of cybercrime are later utilized to target other, less serious types of cybercrime, this is called ‘mission creep’ or ‘function creep’ and it is a concern.

These kinds of actions pose an immediate danger to people's basic human rights. Human rights are violated in a very serious way for victims of cybercrimes such as phishing, identity theft, online abuse, and cyberstalking. The right to privacy, as well as the freedom of expression and

the press, are among the basic human rights that have been violated by cybercrime. Either social media is a defender or a violator of human rights, depending on your perspective. To combat cybercrime, India has enacted the Information Technology Act. The government has taken many additional measures to combat cybercrime, such as creating a special agency to deal with it and launching cybercrime education and awareness initiatives. These safeguards and laws, however, are becoming inadequate as predators rely more and more on cutting-edge technology to commit cybercrimes.

The study's author calls for the introduction of laws tailored to combat cybercrime. Users of the Internet should get regular training on how to protect their mobile devices and personal computers against cyberattacks. Cybercriminal organisations often target financial institutions, large corporations, and IT service providers; as a result, they merit special focus. According to the findings, victims of cybercrime need fast relief by having their cases settled.