PROTECTION OF FUNDAMENTAL RIGHTS IN THE DIGITAL ERA: A STUDY IN THE LIGHT OF CYBER CRIMES AGAINST WOMEN IN INDIA

*By **Dasvinder Singh***

Research Scholar, Department of Laws, Panjab University, Chandigarh, India

INTRODUCTION

Society is progressive and always changing by nature. Nothing endures forever. The law must adapt to the changing needs of society as a result of societal development over time. If current sociological conditions continue to dictate the application of the law, it would be like stagnant water, with more drawbacks than benefits. However, there are some rights that cannot be restricted under any circumstances. These are the rights that people naturally possess as members of the human race; no government has the authority to create them or take them away, unless there are very special circumstances. They are considered fundamental rights because they are necessary for a dignified life and for that reason alone. People's fundamental rights are recognised by a number of international treaties, conventions, and protocols, including the Universal Declaration of Human Rights, the International Convention on Civil and Political Rights, and the International Convention on Economic and Social Rights.[i] These rights include the freedoms of expression, privacy, religion selection, life, liberty, and education, among others. The Indian Constitution guarantees everyone in the country some fundamental rights.[ii] The key question at hand is whether or not we also have fundamental rights in the digital sphere. If so, how can they be protected especially for the women?

Cyberspace is a term that describes an area that includes digitalized data itself, as well as the foundation (including satellite media communications), organisations, computers, and especially the web that makes the range useful. However, it lacks a standard definition. Stated differently, the "virtual environment of information and interactions between people" is what

we refer to as cyberspace. It is undeniable that cyberspace is not a static, predetermined universe that operates according to rules and uncontrollably changing elements. The world of the cyberworld is artificial, created.[iii] Cyberspace is flexible because it is a construct; a significant portion of it may very easily be modified. There are no criminal entertainers on the internet. Perhaps they are real people whose actions effect casualties in the real world by extending into cyberspace and the current reality. Thus, thieves may use the internet as a commercial hub to help them spread malicious exercises, but they—as well as their victims—remain in the real world.[iv]

People's role and importance in information and communication technology is growing along with its growth, thus it is even more important that they are not denied their fundamental rights in the contemporary internet environment. The freedom of speech and expression, the right to privacy, and the right to obtain information are the three main fundamental rights that are at stake in the cyberspace. Our fundamental rights will be flagrantly violated if the cyberspace is allowed unregulated.

MAINSTREAM PERILS IN CYBERSPACE: A SUMMARY

Innovation and technology have taken centre stage in today's fast-paced world, dominating human behaviour and standard operating procedures across all industries. The following terms define cyberspace, according to the Cambridge Dictionary:

"*The internet considered as an imaginary area without limits where you can meet people and discover information about any subject*."[v]

Nothing is unaffected by technology, and as a result, computers and information and communication technology have replaced manual intelligence as the standard means of accomplishing tasks with artificial intelligence. Without a doubt, this has made people's lives easier, but it has also created some challenges with regard to health concerns and security precautions for personal information that is provided, absorbed, and gathered while using a network connection to conduct online operations.[vi] To present, India has not passed any explicit legislation to address a wide range of data security and safety concerns. The main threats to fundamental rights in the virtual world are as follows:

CYBER STALKING

Cyberstalking is the term used to describe harassment of a woman that occurs over the internet or through a computer. It is sometimes referred to as online harassment or abuse. According to Forbes, "repeated online expression amounting to a course of conduct targeted at a specific person that causes the targeted individual substantial emotional distress and/or the fear of bodily harm" is defined as online harassment or cyber harassment. Cyberstalking is the clear term for online harassment that occurs when someone uses the internet or another electronic communication tool to interact with someone they don't want to hear from.[vii] This crime poses a serious threat to a person's fundamental right to privacy and may have a chilling effect, which could also undermine the right to free speech.

IDENTITY THEFT

Identity theft is a crime in which the perpetrator obtains a woman's identity through deception and uses it for their own gain. Within the virtual realm, the perpetrator may utilise coercion to force the victim to divulge sensitive personal information on a website, or they may trick a potential customer into disclosing credit card or debit card information on a spam website. Alternatively, the perpetrator may obtain the victim's email password by deceit, using the victim's identity to carry out illicit activities. This is a flagrant infringement on woman's right to privacy.

PHISHING

Phishing is a form of social engineering in which a perpetrator, often known as a phisher, attempts to fraudulently obtain private or sensitive information from authentic users by mimicking electronic communications from a reputable or open organisation which may be headed by women in a robotic fashion.[viii] Three phisher roles are involved in a complete phishing attack. First and foremost, mailers use botnets to distribute innumerable bogus messages that lead users to phoney websites. Additionally, data collectors create fraudulent

websites (usually hosted on compromised systems) that essentially trick users into providing confidential information. Finally, cashiers use the private information to get paid.

DISSEMINATION OF CONTENT WITHOUT CONSENT

This is yet another risk that exists in cyberspace and is a flagrant infringement against an individual's fundamental right to privacy. In this crime, the woman's private information—pictures, videos, etc.—is shared on social media and other networking sites in an attempt to harass the victim. These kinds of crimes are typically committed against women. The content may have been obtained with the victim's consent—for example, if the offender and victim have a fiduciary relationship—but the victim's consent and permission have not been secured for its broadcast.[ix]

INDUSTRIAL ESPIONAGE

Corporate or industrial espionage is the term used to describe a situation in which one business eavesdrops on another with the intention of stealing trade secrets or other sensitive information. The intention behind it is financial benefit. The person committing these kinds of crimes does so in an effort to get an unfair advantage over his rival. For them, there is no such thing as ethics. Their only goal is to increase their profits by whatever means necessary. By using their personal computers to either copy or record important, sensitive, and private information, they steal trade secrets that are kept in computer networks.

MISCELLANEOUS

Other dangers that are common in the cyber world include click fraud, cyberterrorism, mail-bombing, pornography, Trojan horses, virus attacks, online defacement, software piracy, cyberbullying, and computer trespassing. Because of all these crimes, cyberspace is becoming quite terrifying.

An Analysis of the Recognition of Fundamental Rights in Cyberspace

Of all laws, the Constitution is the mother. The Constitution is the sole source of lawfulness. For this reason, the nation's Constitution also upholds the people's fundamental rights. The internet wasn't even around back then, thus the only place where people could exercise their fundamental rights was in the actual world. However, as the internet developed, it became necessary to acknowledge fundamental rights in the virtual realm as well. A number of international agreements, like the International Convention on Civil and Political Rights[x] and the Universal Declaration of Human Rights[xi], recognise people's rights in the virtual world. Furthermore, the first international document to address cybercrimes in cyberspace was the Budapest Convention of 2001. The Constitution of our nation is, very appropriately, dynamic. It changes in step with how society does. The Constitution may be expressly amended to reflect societal demands today, or it may be impliedly amended by the nation's superior courts through their interpretation of the document. A nation's constitution serves as its foundation, and in our case, it functions as the main trunk from which all other laws branch out. People's fundamental rights are protected in Part III of the Indian Constitution. Other laws, such as the Indian Penal Code of 1860[xii] and the Information Technology Act of 2000[xiii], protect people's rights in the online realm against private violators, as fundamental rights are only enforceable against the State.[xiv] The Indian Penal Code and the Information Technology Act contain many measures that deal harshly with cyber offenders; nevertheless, the focus of this chapter will mostly be on the constitutional provisions and the role of our virtuous judiciary. Our constitutional courts do a commendable job of protecting our Constitution. The nation's honourable Supreme Court and honourable High Courts have withstood the test of time, rendering numerous historic decisions that have become turning points in the defence of the citizens' fundamental rights.

FREEDOM OF SPEECH ON THE INTERNET

Article 19(1)(a) of the Constitution grants all citizens of the nation the fundamental right to free speech and expression, which includes the ability to express oneself online. The Apex Court ruled in a well publicised decision that section 66A of the Information Technology Act was unconstitutional. The aforementioned clause gave police the authority to detain someone

for supposedly posting anything "offensive" online. According to the Court[xv], the clause was incredibly ambiguous and did not constitute a reasonable restriction within the meaning of article 19(2) of the Indian Constitution. "The section is unconstitutional also on the ground that it takes within its sweep protected speech and speech that is innocent in nature and is liable therefore to be used in such a way as to have a chilling effect on free speech and would, therefore, have to be struck down on the ground of overbreadth," the Supreme Court declared in reference to section 66A.[xvi]

Additionally, the Supreme Court of India[xvii] made the following insightful observation in a recent ruling:

We now proclaim that, under Article 19(1)(a) and Article 19(1)(g) of the Constitution, the freedoms of speech and expression, practise of any profession, and commerce, business, or occupation may be carried on over the internet. Any limitations on these fundamental rights must comply with the requirements outlined in Articles 19(2) and (6) of the Constitution, including the proportionality test.[xviii]

Therefore, even though the speech may be delivered electronically, we can conclude that the Apex Court has been the defender of our fundamental right to free speech.

RIGHT TO PRIVACY

Everybody wishes to keep their private and personal information to themselves under the privacy rights regime, but with electronic transactions, a variety of people's data are collected and stored, which can easily lead to others being able to identify that person.[xix]

In a historic decision, the Constitution Bench of the Supreme Court[xx] explicitly declared that an individual's right to privacy is a basic freedom that stems from Article 21 of the Constitution. Citizens have the same fundamental right to privacy online as they do offline, but just like with other rights, this one is subject to reasonable limitations and is not unqualified.[xxi]

When the Supreme Court ruled that data contained in closed-circuit television (CCTV) footage constituted a person's private information, it did so by citing the Puttaswamy ruling. The Court[xxii] noted, "It is unreasonable and disproportionate to monitor all actions within dance

bars' premises using CCTV cameras. Unjustified invasions of privacy result from the observation, recording, storing, and retention of dance performances; women bar dancers may even face threats and blackmail as a result. Since closed-circuit television (CCTV) footage provides a reliable means of identifying a person, it becomes crucial for his data, which in turn relates to his right to privacy.[xxiii]

Despite the declaration of the right to privacy as a basic right, our nation does not yet have a suitable data protection law. The Information Technology Act of 2000 is the only possible remedy for a victim whose basic right to privacy is violated by a private party, as fundamental rights can only be enforced against a State. A committee led by Justice B.N. Srikrishna, Retd., presented the Personal Data Protection Bill, 2018 draught legislation.[xxiv] The aforementioned Bill offered a comprehensive framework and suggested establishing data privacy in order to spearhead the nation's data protection laws. But the bill was never able to see the light of day. A Joint Parliamentary Committee was established in December 2019 in order to provide a report on the 2019 Personal Data Protection Bill. According to reports, the joint parliamentary committee was given a fourth extension by both chambers of parliament in March 2021 to present its report. Therefore, the government is failing miserably in its positive commitment to provide a framework that enables us to successfully exercise our fundamental right to privacy with each day that goes by without enacting a data protection law.

Whatsapp, a messaging software owned by Facebook, challenged a provision of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics and Code) Rules, 2021[xxv], before the Hon. Delhi High Court on May 25, 2021. The "Traceability" clause, which requires social media platforms to reveal the identify of the message's originator upon government request, is the part that WhatsApp is contesting. Whatsapp claims that any revelation will go against its "end-to-end encryption" policy and, more significantly, will infringe upon millions of its users' rights to expression and privacy. However, the government asserts that all rights, including the fundamental right to privacy, are subject to reasonable constraints and are not unassailable. We eagerly await the court's ruling. We can be positive that the court will take a balanced stance that will neither jeopardise the millions of citizens' fundamental right to privacy nor allow a threat to outweigh state security.

RIGHT TO ACCESS THE INTERNET

The Hon'ble High Court of Kerala[xxvi] has said unequivocally that the impoverished segments of society bear a disproportionate and greater burden due to their inability to use the internet, as they rely on it for their daily needs. In addition, the court made the brilliant observation that "a rule or instruction which impairs the said right of the students cannot be permitted to stand in the eye of the law," given that the UN Human Rights Council has determined that the right to internet access is a fundamental freedom and a tool to ensure the right to education.

RIGHT TO BE FORGOTTEN

Justice Sanjay Kishan Kaul recognised the importance of the "right to be forgotten" while taking social media and the internet's enormous potential into account. "The ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic" is what he observed as the "right to be forgotten."[xxvii]

A person's right to privacy is that he or she should be in control of their own data, and if they so choose, that data should be deleted from the internet. Global data protection regulations, however, only support the right to be forgotten—not the right to be erased. The term "forgotten" suggests that the data will exist in cyberspace; it will simply appear at the bottom of search results pages, whereas the term "right to be deleted" gives the owner of the data the ability to permanently remove it from cyberspace.

CONCLUSION AND SUGGESTIONS

"*Fundamental rights are not a given today. We have to protect them.*"

-Vera Jourova[xxviii]

Cyberspace is an infinite and limitless environment. There are no defined bounds to it. The internet is becoming more and more important. In the present world, it is difficult to envision a day without the internet. Furthermore, people's reliance on technology has grown along with

the internet's usefulness in these extraordinary times of the Covid-19 pandemic. This emphasises how crucial it is that we have a system in place to defend and preserve people's fundamental rights in cyberspace. The country's honourable courts have consistently looked to our Constitution as their compass and have done a remarkable job of defending fundamental rights against claims of infringement. Since fundamental rights may only be used against state actors, the Indian Penal Code, 1860, and the Information Technology Act, 2000, further reinforce people's online rights. The most susceptible, nevertheless, has been the fundamental right to privacy, which is a part of the fundamental freedoms to life and liberty that our Constitution guarantees. A thorough legal framework for data protection in the nation is desperately needed to prevent private violators from compromising this priceless privilege. The 2019 Personal Data Protection Bill appears to take an optimistic stance in achieving that objective.The aforementioned Bill suggests a broader scope. Based on commerce conducted in India, it will not only apply to those within India but also to those outside of it. Additionally, it suggests protecting private information about a person's identity, personality, and qualities that define them as a real person, as well as private information about money, health, official identification, biometrics, sexual orientation, genetics, intersex status, transgender status, caste or tribe, and political or religious beliefs. Following the Bill's enactment into an Act, organisations that handle personal data must adhere to certain requirements in order to ensure the privacy of individuals who identify themselves through their personal data. The processing of personal data would require the individual's consent.

Additionally, we require international cooperation to improve data protection and defend the nation's citizens' fundamental rights to expression and privacy. The globe has become a tiny village due to the advent of information technology, necessitating such worldwide collaboration. It is important for India to sign accords and conventions with other nations to improve the safety of rights in cyberspace. This way, when we are in need, we can turn to other nations for assistance, and if they do too, we have the necessary systems in place to take appropriate action. Our Constitution gives the Parliament the authority to enact laws pertaining to any treaty or international agreement that serve as functional provisions. In addition, individuals must also do their share by exercising caution and awareness anytime they engage in any online activity. Therefore, by working together, we may strive to create a secure online environment where no one's fundamental rights are violated.

ENDNOTES

[i] Alexandra Rengel, "Privacy as an International Human Right and the Right to Obscurity in Cyberspace", Groningen Journal of International Law, Vol. 2, No. 2, (2014).
[ii] *Ibid.*
[iii] Anil Kumar Bakshi, "The complexities of freedom of speech and expression in cyberspace in digital India", Vol.5, Issue 8, (2018).
[iv] Lance Strate, "The varieties of cyberspace: Problems in definition and delimitation", Western Journal of Communication, Vol. 63, Issue 3, (1999).
[v] Available at: https://dictionary.cambridge.org/dictionary/english/cyberspace. (Visited on October 31, 2023).
[vi] *Supra* Note 1.
[vii] Available at: http://www.legalserviceindia.com/legal/article-3763-a-study-of-indian-law-on-protection-of-right-to-privacy-in-the-cyber-world.html.(Visited on October 18, 2023).
[viii] DikshaBhasin& Aryan Mehta, "Cyber stalking: New Age Terror", International Journal of Law Management & Humanities, Vol.2, Issue 1, (2018).
[ix] Marc A. Rader & Syed M. Rahman, "Exploring Historical And Emerging Phishing Techniques And Mitigating The Associated Security Risks", International Journal of Network Security & Its Applications, Vol.5, No.4, (2013).
[x] The International Convention on Civil and Political Rights, 1966, art.19.
[xi] The Universal Declaration of Human Rights, 1948, art.19.
[xii] The Indian Penal Code, 1860, s.354A, s.354C, s.354D, s.500, s.506, s.509.
[xiii] The Information Technology Act, 2000, s.43A, s.66, s.66B, s.66C, s.66D, s.66E, s.66F, s.67, s.67A, s.67B, s.67C, s.69, s.69A, s.69B, s.72A.
[xiv] Available at https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/internet-related-identity-theft%E2%80%93a-discussion-paper.pdf. (Visited on October 20, 2023).
[xv] *ShreyaSinghal* v. *Union of India*, (2015) 5 SCC 1.
[xvi] *Supra* Note 8.
[xvii] *AnuradhaBhasin*v. *Union of India and Ors*,2020 SCC OnLine SC 25.
[xviii] TanayaSaha&AkanchaSrivastava, "Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization", Vol. 8, Issue 1, (2014).
[xix] PayalThaorey, "INFORMATIONAL PRIVACY: LEGAL INTROSPECTION IN INDIA", Indian Law Institute Law Review, Vol. 2, (2019).
[xx] *K.S. Puttaswamy* v. *Union of India* (2017) 10 SCC 1.
[xxi] *Ibid.*
[xxii] *Indian Hotel and Restaurant Association* (AHAR) v.*The State of Maharashtra* (2019) 1 SCC 45.
[xxiii] Silvia Suteu, "Constitutional Conventions in the Digital Era: Lessons from Iceland and Ireland", Boston College International and Comparative Law Review, Vol. 38, Issue 2, (2015).
[xxiv] Dr.GagandeepKaur, "Privacy Issues in Cyberspace: An Indian Perspective", Available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1875746_code796065.pdf?abstractid=1875746&mirid=1.(Visited on October 21, 2023).
[xxv] The Information Technology (Guidelines for Intermediaries and Digital Media Ethics and Code) Rules, 2021, were notified on February 25, 2021, by the central government to impose a code of ethics and to mandate a three-tier grievance redressal framework in order to regulate the social media.
[xxvi] *FaheemaShirin R.K.*v. *State of Kerala & Others*,WP(C).No.19716 OF 2019(L).
[xxvii] Available at: https://thewire.in/tech/joint-committee-on-data-protection-bill-gets-fourth-extension-to-submit-report. (Visited on October 24, 2023).
[xxviii] Available at: https://www.azquotes.com/quotes/topics/fundamental-rights.html. (Visited on October 24, 2023).