International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Dignified Virtual Existence of Real People: A Matter of Human Right

Shreya Verma

Student at Department of Law Guru Ghasidas Vishwavidyalay, Bilaspur, Chattisgarh, India

Abstract

The ever-evolving human world has faced and adapted to numerous challenges. A significant current challenge is navigating the complexities of the digital age, with its benefits and threats to fundamental human rights. The digitalization of the economy, interaction, education, and communication has brought new opportunities and freedoms, but it has also created significant threats, such as online harassment, trolling, phishing, malware, hacking. And online scams. This article explores the current legal scenario of cyber and digital law in India and selected other nations, and the challenges they face.The article provides necessary context by defining key terms and concepts such as cyber security and artificial intelligence along with their associated needs and repercussions. The article further emphasizes the evolving issues related to people's digital lives and their implications on individual's fundamental rights. It provides a comparative analysis of the stance of different nations on the right to internet access as a human right. Supported by relevant case laws, it delves into the loopholes of the current legal frameworks and the shortcomings of its proper implementation. The article also provides suggestions to address the gaps in policies regarding digital law and enhanced cybersecurity, enabling a dignified virtual existence. With the increasing prevalence of virtual social interaction expected in the future, creating a safe digital environment is paramount. This paper explores actionable intermediary liability and the need for global cooperation in addressing online harms.

Keywords: Digital Law, Cybersecurity, Artificial Intelligence, Ethics, Human Rights

INTRODUCTION

Living in a safe society with dignity is as important as water and air for peaceful survival of individuals. The world is moving towards a new digital age where virtual existence is the future and the need for sound policies in harmonising changes is crucial.

The digital age has ushered in unprecedented opportunities for communication, collaboration, and access to information. However, it has also introduced a complex web of challenges, particularly in the realm of cybersecurity and online harassment. This research paper aims to explore the current legal frameworks in place to combat these issues, specifically focusing on the Indian context.The paper will delve into the inadequacies of the existing legal framework, particularly in light of the rapid advancement of technology. Furthermore, this paper also seeks to address the pressing need for stronger global cooperation in combating cybercrimes, and the need to view digital rights through the lens of human rights, thereby safeguarding dignity and security in the virtual sphere. Through this research, I aspire to provide valuable insights into the ongoing discourse surrounding cyber law, human rights and online safety.

THE DIGITAL LANDSCAPE

Cyberspace, a domain encompassing interconnected digital systems and networks, has become integral to social, economic, and political life. However, its expansion has introduced novel challenges that necessitate a comprehensive understanding and robust countermeasures.

Key Definitions:

- Cyberspace: Digital systems and the online world make up cyberspace, which covers everything accessible through computer networks and the internet. This includes everything from corporate networks and social media platforms, to bank accounts and cloud services.
- Cybersecurity: The application of technologies, processes and controls to protect computer systems, networks and data from unauthorised disclosure, theft or damage. The goal is also to reduce the risk of cyberattacks.
- Cyberpeace: Peace in cyberspace. Cyberpeace exists when human security, dignity and equity are ensured in digital ecosystems. People and their rights are at the centre of this story, not technology.

DIGITAL RIGHTS

The digital environment offers tremendous opportunities to enhance people's ability to exercise their human rights, but it can also create new and exacerbated risks, as well as new links and tensions between rights. For example, efforts to safeguard rights associated with online safety by removing harmful content online like hate speech may be seen as interfering with others' freedom of expression. In developing their digital policies, countries need to consider their impact on human rights to ensure that digital transformation remains human-centric and rights-oriented.[2] Digital rights are those human rights and legal rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices, and telecommunications networks. The concept is particularly related to the protection and realization of existing rights, such as the right to privacy and freedom of expression, in the context of digital technologies, especially the Internet. It is now firmly entrenched by both the African Commission on Human and Peoples'Rights[3](ACHPR) and the United Nations[4] (UN) that the same rights that people have offline must also be protected online, in particular the right to freedom of expression. As stipulated in article 19(2) of the International Covenant on Civil and Political Rights (ICCPR), the right to freedom of expression applies regardless of frontiers and through any media one's choice. However there exists various challenges in realisation and implementation of these rights across the world which will be discussed in this article.

CYBERCRIMES

Cyber crime can be defined as a crime or an unlawful act where the computer is used either as a tool, a target or both. In other terms, cyber crimes in India can be defined as unauthorized access to some computer system without the permission of the rightful owner or place of criminal activity and include everything from online cracking to denial of service attacks. Some examples of cyber crime include phishing, spoofing, DoS (Denial of Service) attack, credit card fraud, online transaction fraud, cyber defamation, child pornography, etc.[5]

Cyber criminals always choose an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where the transaction of a huge amount of money is made on an everyday basis and hack sensitive information. Catching such criminals is difficult. Hence,

that increases the number of cyber-crimes. Computers are vulnerable, so laws are required to protect and safeguard them against cyber criminals.Some major types of cybercrimes are as follows:-

- Data breach: The exposure of confidential, sensitive or protected information to an unauthorised person. This could be accidental, such as a USB drive left on a train or an email attachment sent to the wrong person, but it can also be deliberate, as when malicious actors access a network and exfiltrate (target, copy and transfer) data.
- Malware : Malicious software. These are pieces of code designed to damage, destroy or subvert computer systems. It includes viruses that can replicate and stop systems working; ransomware, which blocks systems until a ransom is paid; and spyware, which is hidden on the target system and spies on the device users.
- Hacking: Criminal hacking is the act of gaining unauthorized access to data in a computer or network. Exploiting weaknesses in these systems, hackers steal data ranging from personal information and corporate secrets to government intelligence. Hackers also infiltrate networks to disrupt operations of companies and governments. Computer and network intrusions cost billions of dollars annually, according to the FBI.
- Web Hijacking: Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.
- Child Pornography: The internet is a primary tool for child sexual abuse, exploiting children's increased online access. Pedophiles distribute pornography, engage in online grooming by posing as peers, and then manipulate children into in-person meetings for sexual exploitation and the creation of child pornography. They use tactics like bribery and false promises to gain trust and overcome inhibitions, ultimately producing and distributing explicit content for profit.
- Email spoofing : Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.
- Cyber Defamation: When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.
- E-commerce/ Investment Frauds: An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud is attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.
- Cyber Terrorism: Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism is an attractive option for modern terrorists for several reasons like it is cheaper, more anonymous, vast ranging and can be operated remotely.

ONLINE HARASSMENT

Online harassment is a form of cybercrime and can be called cyberaggression, cyberbullying, cyber-harassment, cyberhate, cybervictimization, and deviant online conduct. The term online harassment refers to the utilisation of information and communication technologies by an individual or a group to repeatedly inflict harm upon another person. This may encompass issuing threats, causing embarrassment, or

inducing humiliation in a virtual environment. Such behaviour extends to the expression of discriminatory attitudes and beliefs, such as sexism, racism, xenophobia, homophobia, transphobia, or ableist prejudices. It can also involve instances of online sexual harassment, cyberstalking, and the perpetration of image-based sexual abuse or other forms of unwarranted online behaviour of a sexual nature.

There are 6 common types of online harassment.

- Cyberstalking: Cyberstalking is the use of the internet or digital tools to repeatedly harass, threaten, or stalk someone. It includes sending unwanted messages, hacking accounts, or spreading lies online. The goal is often to scare or distress the victim. Cyberstalkers often use social media, email, or other online platforms. Cyberstalking involves using digital platforms to intimidate or control someone by continuously monitoring or harassing them online, they can track the victim's online activity. Cyberstalkers may impersonate their victims, post false information, or make threatening comments. They often create multiple accounts to avoid detection and can track the victim's location or personal activities using GPS or spyware. Cyberstalking can result in offline threats and is a serious situation of destruction of privacy which can often require legal action to stop. Cyberstalking is harmful and illegal.
- Catfishing: Catfishing refers to the creation of a fictitious online persona, or fake identity (typically on social networking platforms), with the intent of deception,usually to mislead a victim into an online romantic relationship or to commit financial fraud. Perpetrators, usually referred to as catfish, generally use fake photos and lie about their personal lives to present themselves as more attractive for financial gain, personal satisfaction, evasion of legal consequences, or to troll.
- Online Impersonation: Online impersonation is when someone pretends to be someone else online, usually in order to trick people into giving them information or money. This can happen on social media, dating websites, or even through email. Sometimes people will create fake accounts using someone else's name and photos, or they'll hack into an existing account and change the information. They may also use different methods to contact people, such as direct messages, comments, or even emails.
- Doxing: The word "doxing" is derived from the term "dropping dox," or "documents." Doxing is a form of cyberbullying that uses sensitive or secret information, statements, or records for the harassment, exposure, financial harm, or other exploitation of targeted individuals.
- Trolling: Trolling is the act of leaving an insulting message on the internet in order to annoy someone. This may include online hate – personal attacks that target someone because of their race, culture, religion, gender sexual orientation or disability. The troll may also encourage mob mentality, urging others to join in the attack so it becomes a pile on.
- Pornography: Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and internet pornography delivered over mobile phones.

UNDERSTANDING CHARACTERISTICS OF CYBERBULLYING

Anonymity: The ability to remain anonymous for those who engage in cyberbullying is one of its distinguishing features. In contrast to traditional bullying, where the perpetrator and the victim are typically acquainted, cyberbullying frequently takes place in secret. Bullies may become more daring and destructive because they feel that they are not going to face immediate repercussions when they remain anonymous. Anonymity has been linked to an increase in the frequency and intensity of cyberbullying

incidents, according
to studies. For example, a study conducted by the Cyberbullying Research Center discovered that people's willingness to engage in cyberbullying is significantly influenced by anonymity because it eliminates the fear of social stigma and retaliation.

Reach and Accessibility: Unlike traditional bullying, cyberbullying is more widespread because it is not limited by physical boundaries. Bullies can now harass their victims from anywhere at any time thanks to the internet, which expands the possibility of harassment beyond school hours and into the victim's home—a place that ought to be a safe haven. Victims may believe there is no way out of the abuse because of this

Constant accessibility:Studies reveal that the pervasiveness of technology in the lives of youth intensifies the issue of cyberbullying since these individuals are nearly always online and consequently always at risk.[8]

Permanence: Cyberbullying is made more severe by the permanence and public nature of online content. It can be challenging, if not impossible, to completely remove harmful content once it has been posted online. It can be shared, copied, and preserved even after being removed from the original source, so it might persist indefinitely. The victim's mental health and reputation may suffer long-term consequences as a result.

PLATFORMS FOR CYBER CRIMES AND ONLINE HARASSMENT

Online harassment can occur across a wide range of digital platforms. Cyberbullying frequently occurs on social media sites. Platforms like Facebook, Instagram, X (formerly Twitter), and TikTok are frequently used for harassment due to their widespread reach and potential for anonymity. Harassment can take the form of abusive comments, spreading rumours, posting embarrassing photos or videos, and creating fake profiles.

Cyberbullying also often occurs via text messaging and instant messaging apps. Apps like WhatsApp, Messenger, and direct messaging features on social media can be used to send harassing messages, threats, and unwanted content. Cyberbullying also occurs in online forums and gaming communities. Platforms like Reddit and online gaming communities can be breeding grounds for harassment, particularly when anonymity is involved. Online gaming environments often involve voice and text communication, which can be exploited for harassment, including verbal abuse and threats. This can manifest as rumours being spread, verbal abuse directed at a specific person, or even coordinated attacks by a group of users against one another. The competitive
environment and interactive nature of games can frequently intensify aggressive behaviour.[9]

REPERCUSSIONS ON VICTIMS EMOTIONAL HEALTH

Online bullying and harassment affects people just as deeply as any other form of bullying and harassment.Online Harassment can have a significant impact on the victim's mental and emotional health. The victim may experience anxiety, depression, fear, and other psychological symptoms. In some cases, the victim may also experience physical symptoms such as headaches, nausea, and fatigue. Cyberbullying can also affect the victim's social life, causing them to isolate themselves from friends and family.[10]

They may suffer from a lack of confidence or lowered self-esteem. They may doubt their self-worth and the validity of their opinions, which may mean they avoid talking about their feelings and what is upsetting them.[11] Sometimes, people experiencing online harassment can also become more aggressive towards

others and even start to harass people themselves, as this can gives a sense of power to remedy the vulnerability of being a victim. They may start avoiding social media altogether, deleting all their email or social media accounts, or conversely spending even more time on the internet. The person may decide to use drugs or alcohol or food as a means of escape. Sometimes people may think about self-harm or even suicide.

An Investigation by the National Institute of Health found that adolescents who experience cyberbullying are at higher risk of developing psychosomatic symptoms.[12]The long-term effects on self-worth can last into adulthood, which can have an impact on opportunities for education and employment. The victim's general quality of life may be negatively impacted by the aftereffects of cyberbullying, according to theAmerican Psychological Association.[13]

CURRENT FRAMEWORK FOR CYBER LAWS IN INDIA

These laws and institutions collectively form the legal framework for addressing cyber crimes and regulating digital activities in India.

1. Information Technology Act, 2000: The primary legislation governing cyber activities in India. It defines cyber crimes and provides a legal framework for e-commerce, digital signatures, and cyber offenses. It establishes various cyber offenses such as hacking, data theft, and spreading of viruses. [14]

In Kamlesh Vaswani vs. Union of India (2015),the Supreme Court, was called upon to address the issue of the circulation of child pornography on the internet. This case highlighted the necessity of strong legal provisions to combat cybercrimes and protect vulnerable groups.[22]

- Section 43A: This section enables compensation in case of a breach of data privacy due to negligent handling of sensitive personal data. AI systems that process user data must ensure that they comply with this provision to avoid legal repercussions.
- Section 66D: This section penalises individuals for cheating by impersonation using a computer resource. It is particularly relevant for AI-driven deepfakes and other AI-generated fraudulent content.
- Section 67: This provision prohibits the publishing or transmitting of obscene material in electronic form. AI systems capable of generating inappropriate or harmful content could fall under this section.[15]
- Section 67A: This section addresses the penalties for publishing or sending electronic content that includes sexually explicit acts. It can be used in situations where sexually graphic content is disseminated online with the intention of intimidating or harassing other people.[16]
- Section 67B: This section addresses the penalties for publishing or disseminating electronic content that shows children engaging in sexually explicit behavior. When minors are the target of cyberbullying with sexually explicit content, it may be used.[17]

2. Indian Penal Code (IPC), 1860: Certain cyber crimes are punishable under the IPC, such as hacking (Section 66) and identity theft (Section 66C).

- Section 292 A [18]:This section addresses printing anything that is blatantly indecent or meant to be used as blackmail. It covers printing, selling, or transferring any written or printed document that is obscene or meant to be used as blackmail. This provision penalizes engaging in or earning any profit from such a business, which includes the sale, import, export, printing, or other activities involving such materials or their advertising in a way that would be detrimental to morals.
- Section 354 C [19]: This section deals with voyeurism. It states that any man who takes a picture of a woman performing a private act in a situation where the woman seems to be assuming her privacy or

who shares the image with a third party would be guilty of an offense. This clause only applies to men, as it is gender specific. This provision does not punish women. Upon his first conviction, he faces a minimum one-year sentence, which could go up to three years, along with a fine. A second offense results in an increase in prison time of at least three years, with the possibility of seven years in prison plus a fine.

- Section 499[20]: Addresses defamation, encompassing both offline and online forms. This section defines defamation as any spoken or written statement, or online content posted on various platforms, that damages another person's reputation. Those found guilty of defamation can be penalized under Section 500 of the IPC, which stipulates punishment that may include simple imprisonment for up to 2 years, a fine, or both.

Bhatia v. State of Delhi (2020): In this particular case, the victim was the target of harassment and defamation by a cyberbully who had set up phony social media profiles. The accused was charged with defamation and impersonation, among other IPC provisions. The ruling emphasized the grave repercussions of cyberbullying and upheld the victims' access to legal recourse under current legislation.[21]

3. The Indian Evidence Act, 1872: Provides guidelines for collecting and presenting electronic evidence in court. It recognizes electronic records as evidence in legal proceedings.
4. The Copyright Act, 1957: Protects digital content from unauthorized reproduction, distribution, and use.
5. The Right to Privacy: While not a standalone law, the right to privacy is protected under Article 21 of the Indian Constitution. The Supreme Court has also recognized privacy as a fundamental right in landmark judgment of Justice K.S.Puttaswamy(Retd) vs Union Of India, 2018 , in which a nine judges' bench of Supreme Court held that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. [23]
6. The National Cyber Security Policy, 2013: Aims to protect information infrastructure in India and strengthen cyber security measures.
7. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016: Governs the use and protection of Aadhaar data, India's biometric identity system.
8. Cyber Appellate Tribunal (CAT): Established under the Information Technology Act to hear appeals against decisions made by Adjudicating Officers.
9. Cyber Cells and Cyber Crime Investigation Units: Various state police departments have dedicated units to investigate cyber crimes.
10. International Cooperation: India cooperates with international organizations and other countries to combat cyber crimes that transcend national borders.
11. The Digital Personal Data Protection Act , 2023 : It regulates digital personal data processing within India and for Indian services abroad, requiring consent for lawful purposes, except for specified legitimate uses. Data fiduciaries must ensure data accuracy, security, and deletion post-purpose, while individuals gain rights to information, correction, and grievance redressal. The central government retains exemption powers for state security and can establish the Data Protection Board of India for enforcement.Key provisions of the Act include:

- Data Protection Principles: These principles mandate that AI platforms obtain user consent before processing personal data, ensure transparency, and allow users to withdraw their consent.
- Data Localization: The Act requires certain sensitive data to be stored within India, which impacts AI

systems that rely on cross-border data transfers.

- Data Breaches: Companies deploying AI must report data breaches to regulatory authorities within a specific timeframe, further ensuring accountability.

12. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) : It aims to regulate online intermediaries, including social media, digital news, and OTT platforms, to prevent the spread of unlawful content. Specifically, Rule 3(1)(b) requires these platforms to prevent users from sharing "grossly harmful, harassing, or defamatory" content. This is particularly relevant for AI platforms that generate content, as failure to comply could result in the loss of their "safe harbour" protections, meaning they can be held liable for user-generated content.[24]
13. Rules on Deepfakes and Misinformation : India currently does not have specific legislation addressing deepfakes or misinformation generated by AI. However, the Information Technology Act, 2000, and the Indian Penal Code (now Bharatiya Nyaya Sanhita) provide provisions to tackle crimes associated with deepfakes.

- Section 66E of the IT Act: This section covers privacy violations related to deepfakes, with penalties including imprisonment or fines.
- Section 509 of the IPC: This section addresses cases of insulting a woman's modesty, which could be used to prosecute deepfakes that exploit women's images or videos

14. CERT-In (Cyber Emergency Response Team – India): CERT-In has been operational since 2004. It is a national focal point for immediate response to computer security incidents as they occur.
15. India's Cyber Crime Coordination Center (I4C): A comprehensive and coordinated response to all types of cybercrime. Cyber Swachhta Kendra: Launched in early 2017, Cyber Swachhta Kendra provides users with a platform to analyze and clean their systems from various viruses, bots/malware, Trojans, etc.
16. The Protection of Children from Sexual Offences Act (POCSO), 2012: Section 13: Relates to the use of children in sexually explicit media. This is applicable in cases where children are involved in or targeted by cyberbullying that includes sexually explicit content.

GAPS IN CURRENT LEGAL FRAMEWORK AND OTHER CHALLENGES

In the last decade, India has made transformational changes in the adoption of digital technology. It has helped the nation become the fastest-growing digital economy. As it continues to expand, it has become a way of life for citizens. Online platforms, smartphones, telecommunication networks and Digital Public Infrastructure are a few examples of it. This has produced some unseen and unheard challenges not only for policymakers but also for the security apparatus.[25]

Global Cyber Index

As per the GCI (Global Cyber Security Index) report published by the ITU in 2018, only 58% of countries have published National Cyber Strategy.[26] That still leaves almost 42% of the world's nations without a cybersecurity strategy! Further, 9% of the Nations do not even have a cyber law in place,[27]21% do not attend any International forums pertaining to cyber-crime and/or cyber security and 51% of Nations do not have any public-private partnership model for strengthening of cyber security measures.[28]

Here are the challenges faced in cyber law in today's world:

- Rapid Changes in Technology: Technology evolves rapidly, and by the time laws are established, the technology has often already advanced. This time gap between the creation and enforcement of laws

makes it challenging to protect people and facilitate effective business operations. Additionally, different laws in each country create difficulties in prosecuting cybercriminals who operate across borders.

- Jurisdictional Issues: Due to the international nature of the internet, one of the biggest obstacles to combating cyberbullying is its international reach. Law enforcement is made more difficult by the fact that individuals from different jurisdictions are frequently involved in cyberbullying. Cyberbullying has the potential to cross national borders and complicate legal matters, in contrast to traditional bullying, which takes place within a particular geographic area and legal framework. It can be challenging for local authorities to take legal action when a bully operating from one nation targets a victim in another. An International Telecommunication Union report states that in order to effectively combat online harassment, international cooperation and harmonization of laws are necessary due to the global nature of cybercrime.[29]
- Maintaining Privacy with Security: The government's increased installation of surveillance can intrude on individuals' privacy. However, inadequate security measures could leave the nation vulnerable. Balancing national security needs with individual privacy rights is indeed a challenging task.
- Digital Evidence and Law Enforcement: Having digital evidence such as emails, chat logs, or call records is crucial when dealing with cybercrimes. However, it is incredibly difficult to verify the authenticity and integrity of this evidence. Law enforcement agencies need to be equipped with advanced tools and ongoing training to handle digital evidence effectively, especially as technology continues to evolve.
- Harmonization Between Nations: The criteria and definitions of what constitutes cyberbullying vary amongst legal systems. Legal responses and enforcement may become inconsistent as a result of this lack of consistency. Cyberbullying is covered under specific statutes in certain countries,while it is covered by more general anti-bullying or harassment laws in others. Lack of a common definition can lead to gaps in legal protection and make prosecution more difficult. In terms of cyberbullying legislation, for instance, the U.S. and the U.K. take different tacks; the U.K. has more extensive anti-cyberbullying laws than the U.S.[30]
- Shortage of Technical Staff: Cybercrime investigations are hindered by a lack of specialized technical personnel, insufficient IT knowledge among general police officers, and legal restrictions that limit investigations to higher-ranking officers who are often unavailable.
- Lack of Infrastructure – Cyber labs: State cyber forensics labs need to be upgraded as new technologies emerge. Cryptocurrency-related crime continues to be underreported due to the limited ability to solve such crimes. Most government cyber labs are well equipped to analyze hard drives and mobile phones, but many still employ "electronic evidence examiners" so they can provide an expert opinion on electronic records.
- Perpetrators' Identification Privacy and Anonymity Issues: One of the biggest obstacles to identifying and prosecuting cyberbullies is their anonymity on the internet. Pseudonyms and anonymous accounts are frequently used by offenders, making it challenging for law enforcement to identify them. This anonymity may make it difficult to hold people responsible for their deeds.
- The matter is made more complex by privacy concerns, since obtaining personal data to identify offenders may give rise to moral and legal dilemmas. Sometimes, the use of privacy laws and regulations to safeguard people's personal information can impede the investigation of cases of cyberbullying.

- Intermediary Liability: While Section 79 of the IT Act outlines the responsibilities of intermediaries (e.g., social media platforms), its vague language often creates confusion about the extent of their liability in moderating content. This raises significant concerns about censorship, platform accountability, and user rights.[31]There is thus a need to strengthen cyber related legislation across the globe, and more so the international cooperation in terms of forensic examination, evidence seizure/ collection &extradition of cyber criminals.

POTENTIAL SUGGESTIONS TO FILL THE GAPS

1. Regular Amendments : Periodic updates are essential to ensure that the Act remains relevant in addressing emerging threats.Using Technology to Improve Response and Detection through Artificial intelligence is one technological advancement that can be used to better identify and deal with online harassment Although they must be used carefully to protect privacy, these tools can more effectively identify abusive patterns and harmful content.
2. Global Cooperation: Collaborating with other nations would enhance India's ability to tackle cross-border cybercrimes effectively.Bringing International Legal Standards into Harmony, International legal norms must be harmonized in order to combat cyberbullying across national boundaries. International collaboration can simplify enforcement and guarantee uniform protections, which will facilitate the handling of cross-border cases. Certain efforts have been made at international level by the United Nations (UN) and some regional organisations like the OECD (Organisation for Economic Cooperation and Development), CoE (Council of Europe), etc.[32]A Global Treaty and Regulatory/Legislative Framework to Combat Cyber crimes is the need of the hour for making a safe digital environment across the globe.
3. Awareness: Campaigns for Public Education and Awareness Cyberbullying can be increased with the support of educational initiatives and public awareness campaigns. These campaigns ought to emphasize raising awareness of the problem, fostering responsible internet conduct, and advancing digital citizenship.
4. Intermediary Responsibility: Social media companies' involvement in collaborative approaches is crucial. Social media companies ought to improve their moderation procedures and policies in order to stop and deal with cyberbullying. Working together with law enforcement can guarantee quicker responses and increase the efficacy of these actions.
5. Strengthen Security: Using strong passwords, enabling multi-factor authentication, and adopting reliable cybersecurity tools can minimise risks.
6. Capacity Building: Training officials in cyber laws and digital forensics is necessary to improve enforcement capabilities. Increasing Law Enforcement Agencies' Collaboration with improving cooperation amongst law enforcement organizations is crucial for handling cases that span several jurisdictions. Creating procedures for information exchange and collaborative inquiries can assist in getting around legal obstacles and enhance responses to cyberbullying.
7. Counseling and Legal Assistance Services : Giving victims access to counseling services and legal aid is essential to their healing and quest for justice. Counseling services can help with the emotional effects of cyberbullying, while legal assistance can help them through the legal system.
8. Defending Victims' Rights and Privacy : Ensuring the privacy and confidentiality of victims' personal information is crucial during the legal proceedings. Legal frameworks should guarantee that victims' personal information is kept private and that they are shielded from additional harm.

9. Proposed New Rights: the gaps in the protection that existing fundamental rights offer citizens in the digital era may not be that large and the existing fundamental rights certainly are not redundant. Nevertheless, there may be situations in which additional fundamental rights may be needed. Focusing only on existing legal frameworks of fundamental rights can be constraining in
this respect, as these frameworks, even though they perhaps indicate what is missing, may not fully reflect what is needed.

- The right to internet access : Sometimes products and services are only offered online or are (much) more expensive if purchased offline. In such cases, citizens who have no or limited internet access can be disadvantaged. Building on a right to internet access, as a condition sine qua non, also a right to digitization education is something to reflect on. Such a right, a further
specification of a right to education,could address the digital divide and digital illiteracy.
- The right to a clean digital environment: a right to a clean digital environment may be directly related to the right to a clean (offline) environment, since a clean digital environment may require less energy and natural resources or at least will use these more effectively.
- The right to a safe digital environment: In the digital age, traditional human rights classifications blur, but the government's duty of care remains crucial for online safety, including digital education and a secure environment. While absolute safety is unattainable, governments must actively regulate and establish clear norms for online safety, extending existing duties to the digital realm, beyond cybersecurity, to encompass a fundamental right to a safe online experience.

CONCLUSION

In conclusion, the current digital landscape and the future's advanced technological world that humanity is to see needs proper supervision. The article discusses various terminologies related to the virtual world.It digs deeper into the question of digital right as a human right. It examines various Cybercrimes and emphasises on Online Harassment at its core. It delves deeper into the various sources and methods through which it persists. It touches upon the crucial aspect of the emotional and psychological state of individuals ,who have been victims of online harassment and other cybercrimes.

The study goes through the current state of legal framework for cyber laws in India and then it also underscores the limitations that exist in this framework. It points out the lack of global cooperation and inadequate implementation of current laws as a major setback for achieving cyberpeace. The research proposes practical solutions including, awareness campaigns among
laymen, global cooperation in tackling international cybercrimes, maintaining pace with evolving technology through regular legal amendments in cyber law and most importantly recognising New Digital Rights as Human Right. These solutions aim to bridge the gap between the increasing rate of cybercrimes and ways to deal with these online anonymous criminals, to ensure a safe
digital environment to all and a dignified virtual life.

References

1. Glossary of Cyber Terms, cyberpeaceinstitute.org (https://cyberpeaceinstitute.org/glossary/#:~:text=Security%20in%20cyberspace.-,Cyberspace,bank%20accounts%20and%20cloud%20services.)
2. Digital freedom: the case for civil liberties on the Net", BBC News,1999-03-04
3. ACHPR, 'Resolution on the right to freedom of information and expression on the internet in

Africa', ACHPR/Res.362(LIX) (2016) (accessible at https://www.achpr.org/sessions/resolutions?id=374).
4. UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet' A/HRC/32/L.20 (2016) at para 1 (accessible at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf).
5. Cyber Crime and Types, Indian Cyber Squad,(https://www.indiancybersquad.org/cyber-crime-type)
6. 'What is online Harassment', University of Oxford,reportandsupport.ox.ac.uk(https://reportandsupport.ox.ac.uk/support/what-isonline-harassment)
7. Sameer Hinduja & Justin W. Patchin, Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying, 17 J. SCH. VIOLENCE 346-367 (2018).
8. Smith, P. K., Mahdavi, J., Carvalho, M. & Tippett, N., 2008. Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), pp.376-385.
9. What is Cyberbullying? October 7,2024, stopbullying.gov(,https://www.stopbullying.gov/cyberbullying/what-is-it)
10. Impact on Victims, University of Winchester,(https://www.winchester.ac.uk/RHD/Anti-Bullying-and-Harassment/Impact-on-Victims/)
11. The Psychological Effects of Cyberstalking on Victims, Mary Jane,(https://www.longdom.org/open-access/the-psychological-effects-of-cyberstalkin g-on victims-99698.html)
12. Gini, G. & Pozzoli, T., 2013. Association between bullying and psychosomatic problems: A meta-analysis. Pediatrics, 132(4), pp.720-729.
13. American Psychological Association (APA), Bullying, (2017), available at https://www.apa.org/topics/bullying.
14. https://criai.org/page.php?page=cyber-law-in-india-#:~:text=Indian%20Penal%20Code%20(IPC)%2C,identity%20theft%20(Section%2066C)., Crime Research Investigation Agency of India
15. Shreya Singhal and Ors. V. Union of India AIR 2015 SC 1523 ; Writ petition (Criminal) No. 167 of 2012
16. Ibid.
17. Ibid.
18. Indian Penal Code 1860 https://lddashboard.legislative.gov.in/sites/default/files/A1860-45.pdf 19.Ibid
19. Ibid
20. Ibid
21. Tanuj Bhatia (Minor) vs Appejay School Pitampura, Delhi & Anr. On 28 July, 2016
22. Kamlesh Vaswani vs Union Of India And Ors. On 26 February, 2016
23. (https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023), The Digital Personal Data Protection Bill,2023
24. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018 Equivalent citations: AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1, (2018) 4 CURCC 1, (2018) 255 DLT 1, 2018 (4) KCCR SN 331 (SC), AIRONLINE 2018 SC 237
25. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,

2021,[updated as on 6.4.2023](https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Int ermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.202 3-.pdf)
26. India stares at a steep cyber crime challenge. Is it prepared?, The Indian Express,(https://indianexpress.com/article/opinion/columns/india-cyber-crime-challen ge- 9351602/)
27. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/ draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, p 18, Accessed 02 March 2025
28. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cyb ersecurity-Index-EV5_print_2.pdf, p 17, Accessed 02 March 2025
29. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cyb ersecurity-Index-EV5_print_2.pdf, p 20,Accessed 02 March 2025
30. Cyber Law: Emerging Trends and Challenges, August 27 ,2024 (https://eimrglobal.org/cyber-law-trends-and-challenges/)
31. International Telecommunication Union, Trends in Cybercrime: The Role of International Cooperation (2019), available at (https://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/2019/Pages/rep ort.aspx.)
32. Cyber Security in India: Challenges and Measures, November 4,2022(https://www.geeksforgeeks.org/cyber-security-in-india-challenges-and-measures/)