International Journal of Early Childhood Special Education (INT-JECSE)
DOI: 10.48047/intjecse/V14I6.395 ISSN: 1308-5581 Vol 14, Issue 06 2022

CYBER LAWS AND HUMAN RIGHTS

Ms.Arpita Sehgal, Research Scholar,
Department of Law, Jayoti Vidyapeeth Women's University, Jaipur
arpitasadvocate@gmail.com

Abstract
This research paper provides an in-depth analysis of the complex interplay between human rights and cyber law in the context of the quickly developing field of digital technology. It is critical to comprehend how the legal frameworks controlling cyberspace interact with the defense of fundamental human rights at a time when technology is becoming more and more part of our daily lives. In this essay, I will examine the difficulties and possibilities brought about by this interaction, highlighting both the possibility of preserving individual liberties and the dangers of violations in the digital sphere. It uses a multidisciplinary approach to study important topics like privacy, freedom of speech, information access, surveillance, and cybercrimes, with the goal of advancing knowledge about how cyber law may successfully handle human rights concerns in the digital age.

The study explores the subject of cybercrime and its effects on human rights in more detail. It offers insight into the nature and consequences of cybercrimes, examines the legal frameworks for stopping them, and tackles the necessity of protecting human rights throughout cybercrime investigations. Additionally, the paper explores emerging trends such as artificial intelligence, block chain technology, and internet governance, considering their potential impact on human rights and the future of cyber law.

Keywords : Human Rights, Cyber, digital, technology, internet.

Introduction

In the field of both cyber law and human rights, the digital revolution has created previously unheard-of opportunities and difficulties. It is critical to comprehend the intricate interactions between the legal frameworks controlling cyberspace and the defense of fundamental human rights as technology continues to pervade every area of our lives.

The digital revolution has changed how we engage with one another, communicate, and obtain information. Technology has permeated every aspect of our everyday life, from social media platforms to e-commerce websites, cloud computing to artificial intelligence. Individuals' reliance on digital platforms and technology has increased the risks and vulnerabilities that exist to their personal information, privacy, and freedom of speech.

A key tenet of a democratic society is the idea of human rights, which embrace the inherent worth and liberties of every person. The right to privacy, freedom of expression, access to information, and protection from discrimination is only a few of these rights.

Research Methodology

This research study takes a multidisciplinary strategy to achieve these goals by fusing the views of law, technology, and human rights. The process includes a thorough examination and analysis of the current literature, which includes scholarly studies, legal treatises, reports from recognized organizations, and legal texts. Case studies and comparative legal analyses of various legal frameworks will be used to demonstrate various perspectives on cyber law and human rights.

The study paper intends to advance knowledge of the intricate interactions between cyber law and human rights in the digital age by employing this methodology. It aims to draw attention to the difficulties presented by new technologies and investigate practical methods for safeguarding human rights while reaping the rewards of the digital revolution.

The Intersection of Cyber Law and Human Rights

The phrase "cyber law and human rights intersection" refers to the legal and policy issues that come up when addressing an individual's rights and freedoms within the context of the digital world. It entails looking at how conventional human rights laws and protections fit into and adjust to the quickly changing digital environment. Data protection, privacy, online freedom of expression, cyber security, and intellectual property are just a few of the topics covered by cyber law, which also include other laws and rules that apply to digital activity.
Fundamental human rights are still pertinent and necessary in the digital age to safeguard people's liberties, autonomy, and dignity. The following fundamental human rights standards are particularly important for the digital sphere:

1. **Right to Privacy[1]:** Individuals have the right to control their personal information and data, and organizations and governments are obligated to safeguard such information from misuse and unauthorized access.
2. **Freedom of Expression[2]**: In the digital age, where communication channels and social media play a crucial role, the ability to freely express ideas and opinions is essential. But this right must also be balanced against issues like encouragement to violence, false information, and hate speech.
3. **Right to Information Access[3]:** With the internet now serving as a major information source, it is essential to have the ability to obtain and share information online in order to participate in society and exercise other rights[4].
4. **Right to Due Process[5]**: People should have access to just legal processes and protections in the digital sphere, including defenses against arbitrary surveillance, censorship, and illegal online behavior[6].

Importance of Cyber Law
In the digital age, cyber law is essential for defending and advancing human rights. Here are some justifications for why cyber law is crucial:
a) Protecting Privacy: Cyber law offers regulatory frameworks and processes to safeguard people's privacy and personal information against unauthorized collection, use, and disclosure by public and commercial organizations[7].

b) Protecting Freedom of Expression: Cyber law provides regulations and standards to strike a balance between the right to free speech and legitimate concerns like defamation, hate speech, and the protection of intellectual property rights in the online space.

[1] Article 21 of the Constitution of India
[2] Article 19(1)(a) of the Constitution of India
[3] Article 19(1) of the Indain Constitution
[4] Raj Narain v. State of Uttar Pradesh (1976)
[5] Article 21 of the Constitution of India
[6] Maneka Gandhi v. UOI (1978)
[7] PUCL v. UOI

c) Combating Cybercrimes: Cyber law has laws to combat a variety of cybercrimes, including hacking, identity theft, online fraud, and cyber bullying. These rules aid in the prevention and prosecution of such offenses, protecting people's rights and fostering a safe online environment[8].
d) Fostering Online Safety and Security: Cyber law supports the adoption of cyber security measures to shield people, organizations, and governments from online dangers. This improves confidence and trust in online relationships and helps guard against potential harm.

Evolution of Privacy in Cyberspace

With the development of the internet and the growing digitalization of personal data, privacy rights have evolved in cyberspace. At first, protecting personal information from unauthorized access and use by third parties was at the forefront of privacy concerns in the digital world. More thorough privacy protections were obviously required as internet usage and functionality increased.
The acknowledgment of privacy as a fundamental human right was an important advance in the history of privacy rights in cyberspace. In its 2013 resolution on right to privacy in the digital age, the UN General Assembly reaffirmed that privacy is a fundamental human right and urged all of its member nations to uphold and defend it online.
Many nations have passed laws and rules that particularly address online privacy. As an illustration, the General Data Protection Regulation (GDPR)[9] of the European Union, which took effect in 2018, offers a thorough framework for the protection of the personal data of EU people. It provides people more control over their personal data and places requirements on the businesses that gather and use it.
Furthermore, the development of privacy rights in cyberspace has been greatly influenced by judicial decisions and legal precedents. The necessity for constitutional rights against arbitrary searches and seizures of digital information has been acknowledged in landmark instances, such as the United States Supreme Court's ruling[10].

Challenges of Privacy in the Digital Age

Due to the enormous amounts of data generated, gathered, and shared online, the digital age has created significant issues for privacy. Among the principal difficulties are:

1. Cybercriminals frequently target businesses in order to get unauthorized access to private data breaches and hacking. Identity theft and serious privacy violations can result from data breaches.
2. Governments and other organizations monitor online activity and gather a vast amount of personal data through comprehensive surveillance practices. Concerns about widespread surveillance and the degradation of personal privacy are raised by this.
3. As data becomes more readily available, businesses and organizations employ these techniques to examine customer behavior and preferences. As a result, there may be intrusive, targeted advertising and even discrimination depending on the information gathered.
4. Once personal information is shared online, people frequently have little control over it. Data may be kept indefinitely, disclosed to third parties without permission, or used for reasons other than those for which it was originally intended.
5. Smart devices and the Internet of Things[11] devices proliferate and capture and transmit massive amounts of personal data, and privacy issues are being raised. The risk of unauthorized access or improper use of sensitive data presents a serious problem.

Legal Mechanism for Privacy Protection

[8] Cyber Crime Prevention Act
[9] https://gdpr-info.eu/
[10] Carpenter v. United States (2018).
[11] https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/

Several legal measures have been put in place to combat the threats to privacy in the digital age, including:

1. Numerous nations have passed thorough data protection laws that control the gathering, storing, and processing of personal data. Examples include the EU's General Data Protection Regulation (GDPR), the US's California Consumer Privacy Act[12] (CCPA), and Canada's Personal Information Protection and Electronic Documents Act[13] (PIPEDA).
2. There are laws and rules in place to secure data while it is being sent and stored, including legislation relating to encryption. These regulations frequently demand that businesses employ encryption and security controls to protect customer information from unauthorized access or breaches.
3. Privacy by design is a strategy that encourages the incorporation of privacy concerns into the planning and creation of systems, procedures, and products. It makes ensuring that privacy measures are initially included rather than added afterward.
4. International agreements and frameworks accords like the Convention for the Protection of Individuals with respect to the Automatic Processing of Personal Data (Convention 108) and the APEC Privacy Framework try to harmonize privacy protections between various jurisdictions.
5. Laws and regulations frequently call for organizations to get individuals' informed consent before collecting or processing their personal data. Additionally, they emphasize the value of transparency by mandating businesses to be transparent about their data practices and privacy policies.

Freedom of Expression and Access to Information

The terrain of freedom of expression has undergone a considerable transformation because to digital technologies. People now have strong tools at their disposal for participating in public debate, sharing information, and expressing their ideas, thanks to the internet, social media platforms, and other digital technologies. This has increased opportunities for participation in public discourse and democratized the flow of information.

In the information era, the right to freedom of speech applies to all forms of communication, including text, images, audio, and video. Through blogging, social networking, online forums, video-sharing websites, and other digital means, people can express their opinions. These innovations have given people the ability to reach a global audience and have been crucial in advancing social justice, political transformation, and human rights.

However, the freedom of expression is likewise threatened by digital technologies. Due to the abundance of information available online and the simplicity of distribution, damaging content, hate speech, and misinformation may spread quickly. Freedom of expression can be compromised when governments and commercial organizations place limits on digital platforms, such as censorship, surveillance, or content takedowns.

It's critical to strike a balance between encouraging free speech and tackling significant issues like hate speech, incitement to violence, and the distribution of false information in order to protect the right to freedom of expression in the digital era. It is necessary to do this by putting in place legislative frameworks that uphold the right to free speech while also offering protections against misuse or injury. Governments should collaborate with online communities, civil society, and global organizations to create laws that uphold human rights while resolving the problems brought on by digital technologies.

[12] https://www.forbes.com/advisor/business/what-is-ccpa/

[13] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda

DOI: 10.48047/intjecse/V14I6.395 ISSN: 1308-5581 Vol 14, Issue 06 2022

Ensuring Access to Information in Digital Era

The operation of democratic societies, the ability to make informed decisions, and the exercise of other human rights all depend on having access to information. Ensuring that everyone has access to knowledge presents new difficulties and opportunities in the digital age.

Governments, public society, and the commercial sector should collaborate to address these issues and close the digital gap. This involves supporting digital literacy programs, offering affordable internet access, and investing in infrastructure to increase broadband connectivity. To ensure that marginalized people, notably those in rural areas and developing nations, have equal access to and participation in digital information spaces, efforts should be taken in this direction.

Initiatives involving open data may also be extremely important in fostering information access. Governments should proactively release public data in digital formats so that the general public has free access to it. Open data can empower citizens, promote transparency, and support social progress and innovation.

However, guaranteeing information access extends beyond technical setup. In addition, it calls for supporting independent journalism, fostering media diversity, and shielding reporters and whistleblowers from abuse and intimidation. Governments should implement measures that support diversity, openness, and media independence both offline and online.

Cyber Surveillance and Human Rights

As surveillance technology has advanced and spread, it has both advantages and disadvantages for people's privacy and human rights. Closed-circuit television (CCTV) cameras, facial recognition software, biometric databases, data interception tools, and internet surveillance tools are a few examples of regularly used surveillance technology.

These technologies have the ability to harm privacy rights and improve public safety while also assisting law enforcement efforts. For instance, widespread surveillance involving the tracking of people's whereabouts without their knowledge or agreement can result from facial recognition technology. The rights to privacy and freedom of expression might be compromised when data interception techniques are used to monitor personal communications.

These surveillance devices' effects include:

1. **Privacy invasion:** Without people's knowledge, surveillance technologies are capable of gathering enormous volumes of sensitive personal data. This intrusion into personal space may chill people's behavior and restrict their freedom.
2. **Discrimination and Bias:** The potential for bias and discrimination against particular groups has led to criticism of facial recognition systems and other surveillance technology. These technologies have the potential to unfairly target and harm marginalized people if they are not properly designed and regulated.
3. **Lack of Accountability:** Because surveillance technologies frequently work in secret, it can be challenging for people to hold surveillance organizations or individuals responsible for wrongdoings or human rights breaches. The concept of the rule of law is threatened by this lack of transparency.
4. **Cyber security hazards:** Surveillance technologies may rely on networked systems that are susceptible to hacking or unauthorized access, they can also present cyber security hazards. Sensitive personal information may be exposed as a result of such breaches, which may also help cyber attacks.

Cybercrimes and Human Rights

Cybercrimes can have a negative effect on a person's finances, privacy, mental health, and reputation. Cybercrimes can cost businesses and organizations money, disrupt operations, harm brand reputation, steal intellectual property, and compromise customer data. Considering that they might be used for espionage, sabotage, or attacks on vital infrastructure, cybercrimes can also have an impact on national security.

Cybercrimes can occur across national borders because of the interconnected nature of the digital world, making it difficult to investigate and prosecute criminals. Additionally, because cybercriminals frequently take advantage of technical flaws and swiftly changing strategies, law enforcement organizations and cyber security experts must maintain ongoing monitoring and adapt.

Countries have created legal frameworks that address various facets of these offenses in order to effectively tackle cybercrimes. These frameworks frequently include procedures for international cooperation as well as rules and regulations.

In general, cybercrime laws cover offenses like unauthorized access to computer systems, data theft, hacking, identity theft, online fraud, and distribution of malicious software. Cybercrime laws differ depending on the jurisdiction. Many nations have formed dedicated cybercrime units within law enforcement organizations and passed legislation that specifically targets cybercrimes.

Due to the transnational character of cybercrimes, international cooperation is essential to their prevention. Governments work together through extradition and legal cooperation accords, as well as the sharing of intelligence and best practices. International organizations like Interpol and the UN also make it easier for nations to work together and coordinate efforts to effectively combat cybercrime.

Safeguarding the Human Rights in Cyber Investigation

Protecting human rights during investigations and prosecutions is just as vital as fighting cybercrime. The following are some significant factors for safeguarding human rights in cybercrime investigations:

1. Investigations should be conducted with regard to the rights to privacy and dignity and in a manner that is reasonable to the offense. Targeted surveillance efforts should be supported by solid evidence.
2. Legal representation, a fair trial, and the assumption of innocence until proven guilty are just a few of the rights that should be provided to anyone who is suspected of committing cybercrimes.
3. Personal data gathered during investigations should be treated in line with applicable laws and regulations, and privacy rights should be respected.
4. Even in the context of combating cybercrimes, freedom of expression and access to information should be preserved. To prevent unjustifiable restrictions or interference with legal internet activities, precautions should be taken.
5. It is important that investigations into cybercrime be carried out without considering factors such as race, religion, gender, or other protected characteristics. Avoiding any potential bias or prejudice is a good idea.
6. Cybercrime victims should receive adequate support and assistance, including access to legal recourse, counseling services, and financial recompense where necessary.

Governments and law enforcement organizations should develop clear guidelines, give investigators specialized training, and set up oversight systems to check compliance with human rights norms to ensure the protection of human rights in cybercrime investigations.

Emerging Trends and Future Consideration

Human rights and artificial intelligence (AI) are two topics that are increasingly of concern in today's society. As AI technologies develop, there are more and more conversations and disputes about how they may affect ethics, privacy, and human rights. Among the most important factors in this regard are:

a) Bias and Discrimination: AI systems have the potential to reinforce or exaggerate biases and discrimination that already exist in training data, producing unjust results. To preserve people's rights, it is essential to make sure AI systems are created and implemented fairly and responsibly.

b) Privacy and Surveillance: Artificial intelligence (AI) technologies like facial recognition and predictive analytics present privacy and surveillance issues. To protect people's privacy rights, it is essential to safeguard personal data and establish clear policies around data collection, use, and retention.

c) AI-powered autonomous weapons: The creation and use of these weapons present serious ethical and human rights issues. To guarantee that AI is utilized in line with international law and human rights standards, worldwide efforts are currently being made to establish regulations and frameworks.

d) The right to explainability: Transparency and explainability are becoming increasingly important when AI systems make judgments that affect people's lives. For the protection of human rights, it is essential that everyone has the right to know how choices are made and to contest them.

To address these issues, governments, organizations, and technologists must work together to create ethical standards, laws, and frameworks that guarantee AI technology uphold and defend human rights.

Blockchain Technology and Trust in Cyberspace

The promise of block chain technology[14] to improve security, trust, and transparency across a range of industries has drawn a lot of attention. Trust in cyberspace and block chain-related factors to consider include:

a) Decentralization and Trust: Block chain's decentralized structure eliminates middlemen and promotes confidence in peer-to-peer exchanges. As a result, people may feel more empowered and rely less on centralized authorities.

b) Data Integrity and Security: Because of the distributed ledger's immutability and transparency, block chain technology is a good fit for applications where data integrity and security are essential. To retain confidence in block chain systems, it is crucial to solving weaknesses like private key management and smart contract security.

c) Regulatory and Legal Challenges: Since block chain technology frequently functions across borders, there are concerns regarding legal systems, regulatory compliance, and international trade. Building suitable rules and guidelines can aid in building confidence in block chain-based systems.

d) Sustainability and Scalability: Block chain networks' energy usage and scalability are important issues that need to be addressed. To guarantee long-term viability and trust in block chain technology, effective consensus processes, and sustainable solutions are required.

Exploring block chain's potential uses and constraints, as well as resolving its technological, legal, and regulatory issues, can help build trust and transparency in the digital world.

Internet Governance and Global Corporation

The regulation of the Internet and international cooperation are essential to ensuring its stability and continuous growth in today's society[15]. Important factors to remember in this area are:

a) Multi stakeholder Approach: Governments, businesses, civil society organizations, and technical specialists should all be involved in Internet governance. In order to meet the global character of the internet, collaboration, and inclusive decision-making processes can guarantee that many perspectives are taken into account.

b) Digital Divide: For everyone to have equal access to the advantages of the internet, it is essential to close the digital divide. The development of digital literacy, the expansion of internet infrastructure, and the removal of socioeconomic obstacles to access for underserved populations should all be priorities.

c) Cyber security and Data Protection: Strong mechanisms for data protection and privacy must be established, and international collaboration is necessary to combat cyber threats, share best practices, and provide a secure and trusted online environment.

d) Content Governance and Freedom of Expression: It can be difficult to strike a balance between the protection of free speech and the control of dangerous content. It is crucial to create frameworks that address illegal content while upholding fundamental rights.

Managing difficult geopolitical, technical, and societal difficulties is necessary for improving internet governance and promoting international cooperation. To ensure an open, safe, and inclusive internet that respects fundamental rights and has a beneficial influence on society, cooperation between many stakeholders is essential.

Conclusion

[14] https://www.ibm.com/topics/blockchain

[15] https://www.unesco.org/en/internet-governance

The complicated interplay between cyber law and human rights in the digital era has been thoroughly examined in this study paper. Several important conclusions have been drawn from the consideration of important concerns such as privacy, freedom of expression, access to information, surveillance, cybercrimes, and new trends.

The conclusions show the need for strong legal systems that balance defending people's rights with addressing societal issues. They emphasize how crucial it is to continuously modify and improve these frameworks in order to successfully meet new difficulties brought on by digital technology. The comparative analysis of foreign strategies also highlights the variety of legal responses and the implications for the protection of human rights.

The research report makes suggestions for further study, including additional analysis of the effects of cutting-edge technology, assessment of international collaboration, and inquiry into the moral implications of surveillance technologies. Additionally, it emphasizes the consequences of cyber law and the defense of human rights, highlighting the necessity of inclusive legal frameworks, global collaboration, and improved digital literacy. This study article intends to add to the ongoing discussion and efforts to ensure the preservation of fundamental human rights in the constantly changing digital environment by taking into account these findings, recommendations, and implications.

References

1. https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one
2. https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue
3. https://publicknowledge.org/cybersecurity-and-human-rights/
4. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763
5. https://www.ohchr.org/en/stories/2022/08/activists-internet-shutdowns-violate-human-rights
6. https://theconversation.com/should-cybersecurity-be-a-human-right-72342
7. https://www.un.org/en/chronicle/article/cyberbullying-and-its-implications-human-rights
8. https://www.eff.org/deeplinks/2022/12/global-cybercrime-and-government-access-user-data-across-borders-2022-year-review