International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 25-01-2026, Accepted: 24-02-2026, Published: 11-03-2026
Volume 12, Issue 1, 2026, Page No. 434-439

Artificial intelligence and online harassment: Examining the limits of free speech in the context of cyber crime and digital data

Nishu Singh
Research Scholar, Departmet of Law, Bundelkhand University, Jhansi, Uttar Pradesh, India

Abstract
A new dawn of digitally mediated communication technologies has emerged due to the fast adoption of Artificial Intelligence (AI) in digital communication systems. As AI is beneficial in terms of content spread and content moderation, it has also accelerated the magnitude and complexity of online harassment with harmful speech amplifying, automated trolling, and AI-generated abuse. The paper is a critical analysis of the changing boundaries of freedom of speech with regards to cyber-crime and the governance of digital data. It examines the overlap of constitutional rights to expression with new legal regimes on the topic of platform liability, content moderation and data protection. The study assesses the conflict between the protection of the discourse of democracy and aversion to the harm of digital using a doctrinal and comparative legal method. This paper claims that a human-oriented rights-based AI regulatory framework is necessary to strike freedom of expression and protection of dignity, privacy, and cyber security within the current digital ecosystem.

Keywords: Artificial intelligence, online harassment, freedom of speech, cyber-crime, data governance, content moderation

Introduction

The virtualization of communication technologies has rebuilt the structure of the general discourse. Social media, content systems that are run by algorithms, and applications that run on AI are the new forces that define the way people discuss, learn, and participate in democracy. Although the internet firstly was touted as a place of free speech and participatory culture, the fast adoption of Artificial Intelligence (AI) into digital systems has made this story more complex. Recommendation systems, automated moderation tools and generative technologies powered by AI have hugely increased the volume and pace of communication, though they have also increased the risks of online harassment and cyber-crime.

The debate about the freedom of expression and the security against cyber-evils has emerged as one of the greatest constitutional and regulatory issues of the twenty-first century. Freedom of expression is a guaranteed right in the human rights international law under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), but it also allows restrictions that may be imposed on the speech to protect the rights and reputation of other individuals. In the context of the digital world, it is more complicated to clearly define what rules may be imposed on the speech to protect the rights and reputation of other people when harmful expression is magnified, automated, or generated with the usage of the AI.

In this paper, AI will be placed in the larger context of cyber-crime and management of digital data, and how technological progress is changing the line between what is considered legal to express and where regulation is needed.

1. Background of the Study

The growth of the digital platforms has completely changed the nature of communication. Contrary to conventional media, algorithms on the internet provide a personalization of content and maximize user interaction. These are fed by machine learning models that crunch and process large volumes of user generated data and generate feedback loops that affect the visibility, virality, and formation of public opinion.

The legal systems of various jurisdictions have been unable to cope up with this changing environment. In India, Article 19(2) has the limitation that the freedom of speech and expression guaranteed by Article 19(1) (a) to the Constitution is subject to reasonable restrictions, whereas, in the United States, the first amendment uses the legality, necessity and proportionality tests to determine whether a restriction on freedom of expression is justified. At the international level, the United Nations Human Rights Committee has made it clear that restrictions on online freedom of expression must be justified by legality, necessity, and proportionality.

The appearance of AI-based communication technologies has exacerbated regulatory problems since malicious speech is no longer one-sided. With automated bots, algorithmic amplification and synthetic media technologies, it is now able to reproduce, magnify and distort content faster than ever before. Therefore, cyber bullying has shifted its face to individual interpersonal wrongdoing to stereotypically enhanced online harm.

2. The emergence of Artificial Intelligence in Online Communication

Artificial Intelligence has already become part of the operation of modern digital platforms. AI systems are used in content suggestion, focused advertising, audience profiling, somewhat engineered moderation, and content creation. Suggestion engines affect the content users are exposed to and shape political discourse and social narratives by personalized feeds.

This is made more difficult by generative AI technologies. Tools that are able to generate plausible text, pictures, audio, and video have increased the ability to express creativity and have been used to spread fake information, impersonation, and reputation damage. Deepfake technologies are deep learning models that enable the

generation of artificial media that can be used to harass or even assassinate personalities.

Regulatory systems have started reacting to such developments. The introduction of the Digital Services Act and the Artificial Intelligence Act by the European Union indicates a change to a more systemic approach to responsibility to algorithmic systems and platform governance. AI is not a neutral technological resource, but an active way of organizing communication spaces and threatening infrastructure. The digital communication brought about by AI thus needs to re-evaluate the manner in which freedom of speech functions in algorithmically mediated realms.

3. Development of Online Harassment in the era of AI

The development of AI-powered features has changed online harassment in a distinctly different way. Cyberbullying and hate speech in traditional forms have been enhanced by organized botnets, automated trolling, and visibility as a result of an algorithm. Studies show that algorithmic amplification has the potential to expand the scope of polarizing and harmful information since the ranking systems based on engagement favour emotionally provocative content over other information.

Deepfake pornography, identity spoofing and synthetic impersonation may infringe the right of dignity, privacy and data protection and make it hard to attribute and hold liable. Also, the AI-generated abuse is not always attributed to a particular identifiable person, as opposed to the traditional crimes of speech, which leads to complicated issues of platform accountability and intermediary liability.

Laws dealing with cyber-crime are now becoming more conscious of these harms. As an example, the Information Technology Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021 of India impose due diligence requirements on the intermediaries in order to discourage the misuse of the digital platforms. On the international level, the states are urged to fight the misuse of the digital platforms without compromising the freedom of expression criteria under Articles 19 of the ICCPR.

The AI age has therefore turned the concept of online harassment into a technological phenomenon that is scalable. The matter of this development requires a reevaluation of the boundaries of free speech, which are digitally mediated societies.

Theoretical and Conceptual Framework.

The nexus of Artificial Intelligence (AI), online harassment and free speech needs some conceptual clarity to comprehend how technological structures inform legal and normative frames. This section describes the theoretical basis that is required to examine AI-based communication systems and how they influence cyber-crime and the management of digital data.

1. Artificial Intelligence as a concept

Artificial Intelligence is the term which is used to refer to the computational systems developed to fulfill the functions which are commonly performed by the human intelligence such as the pattern recognition, language processing, and predictive analysis. Modern AI systems work based mainly on machine learning models that extract patterns on high volumes of data and optimize the performance demonstrating through training. The field of deep learning, which is a form of machine learning, is based on the principle of multi-layered artificial neural networks to work with complex inputs, including images, speech, and text. Deep learning is the basis of automated content moderation, targeted advertising, and recommendation algorithms that digital platforms apply.

Generative AI is another advancement that allows text, images, audio and video to be generated synthetically. Huge language models and generative adversarial networks (GANs) can produce very realistic content that is indistinguishable to that created by humans. Huge language models and generative adversarial networks (GANs) are enabling impersonation, misinformation and abusive content generation. The harmful expression can be structurally amplified by the algorithmic amplification, i.e. when the engagement-based ranking systems amplify emotionally charged or controversial content. As such, AI is not a neutral technology, but an active mediator of visibility and impact in digital ecosystems.

2. Interpretation of Online Harassment

Online harassment represents a continuum of harmful digital practices that pose a threat to dignity, safety and psychological health. Cyberbullying is habitually aggressive behavior with the use of electronic media, and it may be directed at vulnerable people. By comparison, trolling and hate speech can include intentional provocation or discrimination towards an individual or a group with protection. The international human rights law acknowledges that national, racial or religious hatred advocacy, which amounts to incitement of discrimination or violence, may be banned.

Doxxing and cyber stalking are more intrusive types of harassment, and entail the unauthorized release of personal information or stalking with the aim of intimidation. These evils have been compounded by the use of AI. Deepfake technologies can be used to create the non-consentual intimate imaging or defamatory audiovisual material. Danielle Keats Citron has cautioned that artificial media endangers privacy, democratic, and personal freedom by being automated, replicable and imputable to the action of one person making it hard to hold anyone responsible.

3. Free Speech in the Digital Age

The freedom of expression takes center stage in both the constitutional democracies and the international human rights law. The international covenant on civil and political rights, article 19, has recognized the right to opinions and the right to seek, receive, and impart information as part of the benefits of free speech as a guarantee of truth-seeking, self-governance and autonomy of choice.

The theory of harm principle by John Stuart Mill, which is expressed in his treatise On Liberty states that no one can be wielded power over any individual to the extent that he/she causes harm to others. The principle still finds use in arguments advocating regulation of harmful online content. Marketplace of ideas theory this concept is linked to Justice Oliver Wendell Holmes in Abrams v. United States, the competition of ideas under free exchange of ideas is the source of truth, but in the current state of algorithmic amplification, there is a breakdown in this theory by discriminating the availability of equal opportunities to the marketplace. Structural neutrality of the classical theory on

free speech is challenged when AI systems engage more than they are accurate or polite.

4. Cyber Crime and Digital Data Governance

Offenses that are carried out using digital networks are considered cyber-crime, which includes identity theft, internet fraud, cyber stalking, and distribution of illegal content. The legal systems are becoming increasingly aware of the necessity to deal with technology-facilitated harms at the same time that the constitutional protections are not violated. In India, the Information Technology Act offers legal procedures to cover computer related crimes and intermediary liabilities.

The issue of digital data governance also makes the regulation more complex. AI systems use large datasets to train and optimize them, leading to the concerns of privacy, surveillance, and profiling. According to Shoshana Zuboff, this is what she terms as "surveillance capitalism" in which personal information becomes a predictive and controllable measure of behavior, and where artificial intelligence in content moderation tools is more likely to marginalize the marginalized, posing an equality and due process issue. Aside, moderation of platforms, Tarleton Gillespie notes that the decisions made by the platform moderators determine the limits of the popular discourse in a manner that is often unclear and unaccountable.

In this regard, technological design should be placed in wider constitutional, human rights, and cyber-crime contexts whenever investigating AI and online harassment. The theoretical framework of the above-presented conceptual foundations offers the theoretical basis when assessing limitations of freedom of speech in digitally mediated societies.

Review of Literature

The current literature in the field of Artificial Intelligence, online harassment and free speech is inter-disciplinary and involves law, technology, sociology, and political theory. Nonetheless, the clarity of the doctrine is still changing, especially concerning the harms that are enabled by AI and constitutional constraints in India.

1. Global Scholarship on AI and Free Speech

The restructuring of the framework of a social discourse by AI has been critically studied in global scholarship. Jack Balkin suggests that digital platforms demonstrate a role of information fiduciaries and thus have a strong level of control in the speech ecosystems, effectively undermining traditional theories of free speech like the marketplace of ideas. The article by Tim Wu concerning information monopolies identifies the fact that concentrated digital power can undermine expressive freedom.

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) has since been the most common way that the international human rights discourse has perceive digital technologies as a factor in the protection and suppression of speech. In General Comment No. 34, the UN Human Rights Committee underlines that there is no limitation on freedom of expression on the internet, and any restriction should be justified in terms of legality, necessity and proportionality.

Constitutional jurisprudence has been used in the Indian context to deal with speech rights being extended in the digital world. Shreya Singhal in v. Union of India, the same vagueness and chilling effect of the section 66A of the Information Technology Act were struck down as being unconstitutional by Supreme Court, which rejuvenated the strong recognition of protections of online speech under Article 19(1) (a).

2. Research into Online Harassment and Digital Violence

Researchers have reported the emergence of technology-enabled harassment, especially gendered harassment and trolling. The literature on cyber harassment by Danielle Keats Citron indicates structural loopholes in the law to address digital harassment, putting forward that pseudonymity and algorithm visibility exacerbate discriminatory behaviors. Literature on online misogyny and hate speech also indicates that anonymity and platform design make negative content more effective through more visibility.

Scholarly analysis has been done on the overlap of online harassment and the constitutional rights of online harassment in India, especially concerning hate speech and incitement. The court ruling of the Supreme Court in Pravasi Bhalai Sangathan v. Union of India dealt with issues of hate speech regulation and the boundaries of judicial authority in the absence of a legislative change, especially concerning privacy with dignity under Article 21 of the Constitution. More recently, the Indian scholarship explored the issues of deepfake technologies and AI-generated abuse with references to privacy and dignity.

3. Cyber Crime Regulations in Legal Scholarship

Cyber-crime has been a traditional area of legal scholarship and has been concerned with identity theft, hacking, online fraud, and obscenity laws. The Information Technology Act is the major statute used to regulate cyber offences in India with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. There have been controversies over whether the current provisions are sufficient to cope with AI-enabled harms or thirdly, it is argued that there may be the need to have new regulatory mechanisms.

Regulatory model a comparative approach to the EU regulatory model, specifically the Digital Services Act and the Artificial Intelligence Act, are examples of systemic risk-based regulation. These models are not based on criminal liability, but on structural platform responsibility.

4. Content Moderation and Platform Liability Literature

One of the most controversial fields of digital law is platform liability. In a work by Tarleton Gillespie, the issue of content moderation decisions being political subjects to influence the discourse of the masses is longstanding, and their tend to do so without transparency is also a longstanding issue in the United States of America following the Communications Decency Act of 1996, section 230 of that statute.

Section 79 of the Information Technology Act of India also offers protection of the safe harbour conditionally under the conditions of due diligence. The Supreme Court in Shreya Singhal made clear that intermediaries must respond to court orders or government notifications and not individual complaints. Scholarship remains divided on whether this

further governmental regulation subjects intermediaries to the danger of over-censorship.

5. Gaps in Existing Literature

Nevertheless, there is still a lot left to be desired despite a lot of scholarship. To start with, the part of the literature that considers AI as a technological breakthrough or a content moderation tool does not delve into the field of analyzing AI as a source of harmful speech by its own. Second, theoretical debates about free speech are often based on the assumption of neutral communication spaces, which does not take into account the effect of algorithmic amplification. Third, AI generated harassment is understudied in Indian jurisdiction in comparison to Western ones.

Thus, there is an urgent need to combine AI technology with constitutional free speech values, cyber-crime laws and digital data control into one conceptual framework through doctrinal analysis. The research paper attempts to fill this gap by placing AI-assisted online harassment in the framework of international human rights standards and Indian legal constitutionalism.

Research Methodology

1. Nature of Research

The current research uses a doctrinal and analytical approach to research. It does not utilize any of the empirical instruments like interviews, surveys, and field research. Rather it critically analyzes the statutory measures, constitutional law, judicial precedents, and international legal tools that are applied in Artificial intelligence, online harassment, cyber-crime and online data management. The study is most likely of a normative nature and seeks to examine the changing boundaries of free speech in digital space that is mediated by AI, especially through the prism of the Indian constitution.

2. Research Design

The descriptive part describes the technological premises of AI, the type of online harassment, and cyber regulation regime framework. The analysis part of it critically assesses the interplay of these developments with the constitutional guarantees in Article 19(1) (a) and allowed limits in Article 19(2) of the Constitution of India.

The paper also features a comparative legal reflection, which makes use of regulatory initiatives like the European Union Digital Services Act and Artificial Intelligence Act along with the Indian framework as the Information Technology Act and the Digital Personal Data Protection Act, 2023. The comparison method helps to evaluate the global trends in regulation and apply them to Indian legislation.

3. Sources of Data

The research is based solely on secondary data which is based on reliable legal sources.

Primary sources include:

- Indian provisions of constitutions.
- The Information Technology Act among other laws.
- Jurisprudence Judicial rulings of the Supreme Court of India and foreign constitutional courts.
- The international treaties, including the International Covenant on Civil and Political Rights.

Secondary sources include:

- Scholarly books
- Journal articles which have been peer reviewed.
- Government policy papers, Government reports.
- World institutional publications.

4. Methods of Data Collection

The evidence has been gathered via research in the library, such as the access to legal databases, official legislative texts, and reported case law. Its methodology will include the systematic review of policy and structured case law analysis of AI governance frameworks.

5. Data Analysis Method

The study applies the thematic analysis to determine recurrent legal and conceptual issues, doctrinal interpretation to assess statutory and constitutional provisions and a comparative approach to assess cross-jurisdictional regulatory models.

6. Ethical Considerations

Though it is not the case that empirical data is gathered, ethical considerations are at the center. The research has proper representation of the legal authorities and it does not mischaracterize the judicial precedents. It is also critically concerned with the problems of the data privacy, AI bias, and algorithmic transparency, understanding its consequences on the constitutional right and digital justice.

Legal and regulatory environment

1. Legal Framework International

Digital right protection is becoming a part of the international human rights law. The United Nations has confirmed that the same rights enjoyed offline should be safeguarded online, especially freedom of speech and privacy. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) has confirmed the right to seek, receive, and impart information, which should be accompanied by restrictions that are both lawful, necessary and proportional.

2. Comparative Analysis of Jurisdiction

The First Amendment in the United States offers a robust protection to speech with a couple of exceptions, specifically, the incitement and true threats. The Digital Services Act and the General Data Protection Regulation (GDPR) in the European Union are systemic regulatory frameworks that place platform accountability and data protection in the forefront. In India, the Information Technology Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021, rules and regulations on intermediary liability and online content regulation are neighboring.

3. Emerging AI Regulations

The Artificial Intelligence Act of the European Union provides a risk-based regulatory framework of AI systems. A number of states, such as India, have also defined national AI policy frameworks to provide a balance between innovation and constitutional protection.

Use of Artificial Intelligence and the Threat

Artificial Intelligence serves as a tool to control online space and creates new types of digital harm. The responsibility and constitutional protection is complicated by its duality nature.

1. Artificial Intelligence-based Content Moderators

Moderation tools moderating the digital platforms are increasingly based on AI as they strive to scale hate speech, fake information and illegal content. The automated filtering systems examine text, pictures and videos to either mark or eliminate content as required by law. In India, information technology act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021 provide the Intermediate due diligence rules, which promote proactive monitoring systems. Nevertheless, some issues of the over-censorship and the lack of transparency in the procedure are of concern.

2. Algorithmic Enhancement of Speech of Malignancy

The polarizing or sensational content has a potential of being amplified with the participation of engagement-based algorithms, which makes harmful speech more severe. According to scholars, the algorithmic ranking systems focus on the content that is likely to produce interaction and this aspect may be distorting the neutrality presumed in the classical free speech theory.

3. AI-Generated Harassment

With AI-based bots, deepfakes and fake media, it is possible to harass, impersonate an identity and cause reputational damage at a scale. Danielle Keats Citron places much emphasis on the fact that deepfake technology presents immense privacy and dignity risks.

4. Concerns of Predictive Policing and Surveillance

There is a constitutional issue involving privacy and due process of surveillance and predictive policing based on AI systems. Justice K.S. Puttaswamy v. Union of India, since privacy is acknowledged as a basic right in Article 21 by Union of India, it is pertinent to seek proportional protection.

Free Speech in the Digital Ecosystem

1. Constitutional Perspectives

In India, freedom of speech and expression is guaranteed by the constitution through Article 19(1) (a) of the Constitution. Nevertheless, there are new challenges in the digital environment because speech is now disseminated immediately and enhanced with algorithmic systems. Shreya Singhal v. Union of India the Supreme Court reiterated that the constitutional protection of online speech equal to offline expression, and invalidated statutory provisions that created a chilling effect that were too broad and unreasonable.

2. Reasonable Restrictions and Public order

Article 19(2) allows reasonable limitations in the name of public order, decency, morality and other mentioned grounds. Courts have stressed that a proximate nexus between the restrictions and the harm which is expected is necessary. In Superintendent, Central Prison v. Ram Manohar Lohia, the Supreme Court made it clear that the restrictions should be based on the order of the people and not on far-fetched or speculative dangers.

3. Hate Speech vs. Protected Speech

The difference between the speech that is protected and the punishable hate speech is a complicated one. Article 20(2) of the International Covenant on Civil and Political Rights requires the incitement to discrimination or violence to be prohibited. Indian jurisprudence still finds itself walking this fine line between ensuring that politics remains strong and to keep the targeted harm away.

4. Privacy, Dignity and Expression

The acceptance of privacy as a basic right in Justice K.S. Puttaswamy v. Union of India reinforces the constitutional right of dignity in digital expression. The digital environment needs a balance between the right to express and the right not to suffer due to the application of AI-enhanced harmful features.

Judicial Trends and Case Studies

1. Cases of Online Harassment: Global Cases

The judicial responses to online harassment indicate the changing awareness of harm on the internet. In Elonis v. United States, the U.S. Supreme Court has considered criminal liability on threats occurring through social media, noting that mens rea is necessary in criminal speech on the internet. The case exemplifies the challenge of separating hyperbolic speech and punishable threats in the digital context. Likewise, the presence of cyber stalking and technology-mediated abuse has been dealt with by courts in different jurisdictions by applying traditional principles to online space using current criminal law frameworks.

2. Judicial Interpretation of Free Speech in Cyberspace

In India, Shreya Singhal v. Union of India is the case where the most senior authority on constitutional protection of online speech, they struck down the Section 66A of the Information Technology Act on the ground of vagueness and over breadth. The Court held that restrictions had to pass a test of incitement and proximate cause to public disorder. This jurisprudence concurs with the U.S. norm that is defined in Brandenburg v. Ohio, which guards speech, unless it tends to lead to an imminent act of lawlessness.

3. Cases on Platform Accountability

Judicial interpretation of intermediary safe harbour in Section 79 of the Information Technology Act has been used to judge the platform liability in India. In Shreya Singhal, the Supreme Court explained that intermediaries must respond to the court orders or notices by the government, which would strike the right balance between freedom of expression and control.

Conclusion

Artificial Intelligence, online harassment, and free speech is one of the most complicated regulation issues. AI driven systems have revolutionized communication and they have allowed quick sharing of information, automated modulation, and individual interaction. Meanwhile, the technologies have made scalable harassment, deepfakers, and amplified malicious content by algorithms, and intrusive data practices.

Regarding the aspect of international law, human rights law acknowledges that freedom of expression is equally applicable in online conditions, and it allows restrictions to be carefully stipulated to safeguard the rights, dignity and security of other people. The progress in the regulatory sectors in places like the European Union indicates the change to a more systemic responsibility, AI governance based on risk, and better data protection systems.

In the Indian context, constitutional rights to free speech need to be balanced with the issues of public order, privacy and online security. The changing legal system relating to intermediaries and data protection is an attempt to strike the right balance between innovation and responsibility. Proportional, rights-based, and principled form of regulation is, therefore, mandatory so that AI can make democracy talk stronger without compromising human dignity and digital justice.

Reference

1. International Covenant on Civil and Political Rights. 1966. Art. 19 & 19(3).
2. The Constitution of India. 1950. Art. 19(1)(a) and 19(2).
3. Brandenburg v. Ohio. 395 U.S. 444 (1969).
4. UN Human Rights Committee. General Comment No. 34: Article 19 – Freedoms of opinion and expression. CCPR/C/GC/34. 2011.
5. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books, 2019.
6. Citron DK. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review,2019:107:1753.
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).
8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
9. Russell S, Norvig P. Artificial Intelligence: A Modern Approach. 3rd ed. Pearson Education, 2010.
10. Goodfellow I, Bengio Y, Courville A. Deep Learning. Cambridge: MIT Press, 2016.
11. Gillespie T. Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. New Haven: Yale University Press, 2018.
12. International Covenant on Civil and Political Rights. 1966. Art. 20(2).
13. Mill JS. On Liberty, 1859.
14. Abrams v. United States. 250 U.S. 616 (1919) (Holmes J., dissenting).
15. Balkin JM. Information Fiduciaries and the First Amendment. University of California Davis Law Review, 2016:49:1183.
16. Wu T. The Master Switch: The Rise and Fall of Information Empires. New York: Alfred A. Knopf, 2010.
17. UN Human Rights Committee. General Comment No. 34: Article 19 – Freedoms of opinion and expression. CCPR/C/GC/34. 2011.
18. Shreya Singhal v. Union of India. (2015) 5 SCC 1.
19. Citron DK. Hate Crimes in Cyberspace. Cambridge: Harvard University Press, 2014.
20. Pravasi Bhalai Sangathan v. Union of India. (2014) 11 SCC 477.
21. UN Human Rights Council. The promotion, protection and enjoyment of human rights on the Internet. A/HRC/RES/32/13. 2016.
22. Regulation (EU) 2016/679 (General Data Protection Regulation).
23. Regulation (EU) 2024/1689 (Artificial Intelligence Act).
24. Justice K.S. Puttaswamy (Retd.) v. Union of India. (2017) 10 SCC 1.
25. Superintendent, Central Prison v. Ram Manohar Lohia. AIR 1960 SC 633.
26. Elonis v. United States. 575 U.S. 723 (2015).