JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Cyber-Stalking and its Implication to Freedom of Speech: A Legal Balancing Act in the Digital Age

Dr. Kalada D.S. Nonju, Agent Benjamin Ihua-Maduenyi

Annotation: The rise of digital communication platforms has facilitated unprecedented opportunities for free expression, yet it has also given rise to new forms of harassment, including cyber-stalking. This article explores the complex interplay between cyber-stalking laws and the protection of freedom of speech under international human rights frameworks. By examining comparative legal approaches across jurisdictions and case law developments, the article critically analyzes whether existing legal mechanisms adequately address cyber-stalking without disproportionately infringing on legitimate expression. It also investigates the doctrinal challenges courts face in distinguishing between harmful conduct and protected speech. The paper concludes by proposing normative frameworks that balance the prevention of online harassment with the preservation of open discourse in democratic societies.

1.0. Introduction

In the digital era, the boundaries between public discourse and private harassment have become increasingly blurred. Social media platforms and online forums have not only democratized expression, but they have also enabled new forms of abuse, notably cyber-stalking, a persistent and often covert form of online harassment characterized by threats, monitoring, and emotional distress [1]. While states have a legitimate interest in protecting individuals from such conduct, legislative and judicial responses to cyber-stalking raise critical questions about the permissible scope of restrictions on freedom of speech. This article addresses the tension between combating cyber-stalking and safeguarding freedom of expression, a fundamental right enshrined in international instruments such as Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Cyber-stalking laws, if not carefully drafted and applied, risk suppressing legitimate dissent, political speech, and other protected expressions [2].The study adopts a comparative and doctrinal methodology, drawing on case law, statutory analysis, and international legal standards. It investigates whether existing legal frameworks effectively balance the need to curb cyber-stalking while maintaining the integrity of free speech principles. In doing so, it evaluates how courts interpret intent, context, and harm in online interactions, and whether legal thresholds for cyber-stalking sufficiently differentiate unlawful conduct from protected speech [3].

1.1. Conceptual Framework: Cyber-Stalking and Its Implication to Freedom of Speech

Cyber-stalking has emerged as a potent form of digital harassment that challenges both the criminal justice system and the normative boundaries of freedom of expression. This conceptual framework aims to delineate the core definitions, legal characteristics, and normative tensions between cyber-stalking and the protection of free speech under international law. It provides a foundation for legal and doctrinal inquiry by unpacking the conceptual ambiguities surrounding these issues and situating them within international human rights discourse [4], [5].

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Methodology

1.2. Definition of Cyber-Stalking: Characteristics and Scope

There seems to be no universally accepted legal definition of cyber-stalking, but it is broadly understood as a pattern of behavior involving the use of electronic communication to harass or threaten an individual. Key elements typically include repeated, unwanted contact, threats of violence, identity misuse, surveillance, and psychological intimidation via digital platforms such as email, social media, and messaging applications. In Nigeria, the Act criminalizes the sending of grossly offensive, indecent, or menacing messages online, which can be interpreted to include cyberstalking behaviors.Cyber-stalking differs from conventional stalking in its reach, anonymity, and permanence. The perpetrator can operate across borders, sometimes under pseudonyms, with messages that can be rapidly and widely disseminated and stored indefinitely, thereby amplifying the psychological harm inflicted on the victim.The Council of Europe's Convention on Cybercrime does not specifically address cyber-stalking, but the Explanatory Report acknowledges related offences under provisions on harassment and threats. National legislation varies significantly in scope. For example, the United States defines cyber-stalking under federal law as the use of electronic communication to engage in conduct that places a person in reasonable fear of death or serious injury. In contrast, the UK's Protection from Harassment Act 1997, amended by the Protection of Freedoms Act 2012, criminalizes "stalking" with illustrative examples that encompass digital communications.

1.3. The Concept of Freedom of Speech in International Law

Freedom of speech, or freedom of expression, is a foundational right in international human rights law, articulated in Article 19 of both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). It includes the right to seek, receive, and impart information and ideas of all kinds, regardless of frontiers. While international law recognizes freedom of speech as a cornerstone of democratic society, it is not absolute. Article 19(3) of the ICCPR permits restrictions that are provided by law and are necessary for the respect of the rights or reputations of others, or for the protection of national security, public order, public health, or morals. The Siracusa Principles further interpret these limitations, emphasising proportionality and necessity.The European Court of Human Rights (ECtHR) has similarly held that freedom of expression may be restricted under Article 10(2) of the European Convention on Human Rights (ECHR) when necessary in a democratic society. In *Handyside v United Kingdom*, the Court famously held that the right protects not only "information or ideas" that are favourably received but also those that "offend, shock or disturb."

1.4. Doctrinal Overlap and Conceptual Tension

At the heart of the cyber-stalking versus free speech debate lies the difficulty in drawing a principled boundary between speech that is harmful and speech that is merely offensive or unpopular. This boundary is particularly contentious online, where context is often opaque, audiences are diverse, and messages can go viral quickly. Let us consider the following conceptual questions:

1. When does repeated communication constitute a criminal offence versus legitimate expression?
2. How should courts assess the "intent" behind online speech, especially in jurisdictions requiring a subjective element for harassment or stalking?
3. Should the "reasonable person" standard apply uniformly, or should it be adapted to digital contexts where cultural norms vary?

The danger is that overly broad or vague cyber-stalking laws could chill lawful speech, especially critical, dissenting, or political speech. Conversely, insufficient regulation may leave victims vulnerable to sustained harassment that silences their own participation in public discourse. This is the

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

trend in Nigeria under the present democratic dispensation. This dual risk of overregulation and under protection presents a formidable challenge to lawmakers and courts alike.

1.5. Relevant Jurisprudence and Interpretive Issues

Courts across jurisdictions have grappled with the need to balance these competing rights. In the US, the Supreme Court's decision in *Elonis v United States* overturned a conviction under the federal anti-threat statute, holding that negligence was insufficient to prove intent in online threats.The decision underscored the importance of mental state in distinguishing true threats from protected speech.

In contrast, the ECtHR has shown more willingness to uphold restrictions where speech interferes with the rights of others. In *Delfi AS v Estonia*, the Court held that a news portal could be held liable for offensive comments posted by third parties, citing the need to balance freedom of expression with the right to privacy and dignity.The Human Rights Committee (HRC) has also emphasized that restrictions must be clear, necessary, and proportionate. In *General Comment No. 34*, the HRC warned against laws that allow arbitrary or excessive regulation of speech, including vague notions such as "cyber-bullying" or "offensive language." These cases highlight the importance of legal precision and judicial restraint in addressing cyber-stalking within constitutional and human rights frameworks.

1.6. Emerging Norms and Regulatory Trends

Efforts to regulate cyber-stalking increasingly intersect with broader debates about online content moderation and platform accountability. States and international bodies are developing frameworks to guide platform liability and user protection. The EU's Digital Services Act, for example, imposes heightened obligations on platforms to address systemic risks, including online harassment. Soft law instruments, such as the UN Guiding Principles on Business and Human Rights, also urge digital companies to respect human rights and remedy abuses on their platforms. However, the private enforcement of speech norms by technology companies raises new questions about due process, transparency, and legitimacy. In parallel, civil society organizations advocate for the inclusion of gender-sensitive standards in cyber-stalking laws, recognizing that online harassment disproportionately affects women and marginalized communities.

1.7. Analytical Framework for Legal Assessment

To evaluate whether cyber-stalking laws infringe upon freedom of speech, courts and lawmakers should employ the following structured test grounded in international human rights principles. Such a test might include:

1. Is the restriction provided for by law and formulated with sufficient clarity?
2. Does the law pursue a legitimate aim under Article 19(3) of the ICCPR?
3. Is the restriction necessary in a democratic society, and is there a less restrictive means to achieve the same aim?
4. Are there procedural safeguards to prevent abuse and avenues for redress?

This analytical framework allows for a nuanced understanding that neither trivializes the harms of cyber-stalking nor sacrifices the fundamental right to free expression.

Cyber-stalking represents a profound threat to personal security, mental health, and equality, especially in digital spaces that are increasingly central to modern life. At the same time, legal efforts to curb this conduct must not undermine the very freedoms they seek to protect. A clear and coherent conceptual framework—rooted in international legal norms, proportionality, and judicial prudence—is essential for crafting laws that are both protective and rights-respecting.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

2.0. Legal Approaches to Cyber-Stalking

Cyber-stalking represents a growing challenge for national and international legal systems. As states respond to the increasing prevalence of online harassment, they face the complex task of crafting laws that protect individuals from targeted abuse while preserving the fundamental right to freedom of expression. This section explores the diversity of legal responses to cyber-stalking across selected jurisdictions and assesses their compatibility with international human rights standards.

Results and Discussion

2.1. United States: Federalism and Constitutional Constraints

In the United States, cyber-stalking is addressed through a combination of federal and state laws. The primary federal statute is 18 U.S. Code § 2261A, which criminalises the use of any interactive computer service to engage in conduct that places a person in fear of death or serious bodily injury or causes substantial emotional distress. The statute requires proof of intent and actual harm, reflecting a high threshold that aligns with First Amendment protections.

The First Amendment's robust protection of speech, including offensive or unpopular opinions, poses significant constraints on the regulation of online conduct. In *Elonis v United States*, the Supreme Court held that negligence was insufficient to sustain a conviction under § 875(c) of the criminal code, which prohibits interstate communications containing threats [6], [7]. The Court emphasized that a showing of subjective intent to threaten is required to avoid chilling protected speech. Several states have enacted their own cyber-stalking laws, often with broader definitions than the federal statute. However, many face constitutional challenges if they are deemed overbroad or vague [8], [9]. For instance, a California law criminalising the repeated sending of electronic communications with intent to annoy or harass was partially invalidated in *People v Marquan M.* on First Amendment grounds.

Thus, while the U.S. legal framework does criminalise cyber-stalking, its application is constrained by stringent constitutional protections for speech, demanding precise statutory language and clear standards of intent [10].

2.2. United Kingdom: A More Interventionist Approach

In contrast, the United Kingdom has adopted a more interventionist legal approach. The Protection from Harassment Act 1997, initially designed to address offline stalking, was amended in 2012 to explicitly include stalking behaviours, with digital communications falling within its ambit.Section 2A of the Act criminalises a course of conduct amounting to stalking, which includes activities such as following a person, contacting or attempting to contact them, or publishing material relating to them on the internet [11], [12], [13]. The Act does not require proof of physical proximity, making it well suited to address online conduct. Moreover, the “course of conduct” requirement ensures that isolated acts of expression are not criminalised unless they form part of a broader pattern of harassment. The UK courts have generally upheld these provisions, relying on the proportionality test under the Human Rights Act 1998 to balance the right to private life under Article 8 of the ECHR with the right to freedom of expression under Article 10. In *Thomas v News Group Newspapers Ltd*, the court held that harassment could include press publications that intrude into private life, provided that the interference is significant and persistent [14], [15]. While the UK model allows greater regulatory intervention, it incorporates human rights safeguards through judicial review mechanisms and the necessity and proportionality framework.

2.3. European Union: Fragmented but Evolving

At the European Union level, there is no harmonised cyber-stalking law. However, various instruments address components of online harassment. The 2011 Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography obliges Member States to criminalise online

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

grooming and cyber-luring. Although this focuses on child protection, it reflects growing EU interest in online safety.

The 2012 Victims' Rights Directive mandates that victims of stalking, including cyber-stalking, receive protection and support from authorities. The Directive does not impose substantive criminal law obligations but aims to ensure procedural rights for victims.

Several Member States have enacted national legislation targeting cyber-stalking. For example, Germany's *Strafgesetzbuch* (Criminal Code) includes Section 238 on "Stalking," which encompasses repeated, targeted acts that infringe upon a person's lifestyle and peace of mind, including via telecommunications. France's Penal Code was amended in 2014 to define psychological harassment via digital means, punishable by up to two years in prison.

However, inconsistencies among Member States remain. A 2022 European Institute for Gender Equality report revealed that while most EU countries criminalise stalking, definitions vary, and enforcement remains uneven. The proposed EU Directive on combating violence against women and domestic violence includes provisions on cyber-stalking and could enhance harmonisation if adopted.

2.4. India: Judicial Activism and Legislative Gap-Filling

India has witnessed a surge in online harassment, prompting both judicial and legislative responses. Section 354D of the Indian Penal Code (IPC) criminalises stalking, including monitoring electronic communication used by a woman without her consent. The law was introduced in the aftermath of the 2012 Delhi gang rape case and subsequent Verma Committee recommendations.Cyber-stalking in India is also addressed under the Information Technology Act 2000. Section 66E penalises the violation of privacy, while Section 67 criminalises the publication or transmission of obscene material in electronic form. However, the now-struck-down Section 66A, which criminalised offensive messages online, was widely criticised for its vagueness and misuse. The Supreme Court in *Shreya Singhal v Union of India* declared Section 66A unconstitutional, reaffirming that laws restricting speech must be narrowly tailored and based on clear standards.

Despite legislative efforts, enforcement remains inconsistent, and many cases go unreported due to social stigma and institutional inertia. Moreover, the gendered application of cyber-stalking laws often undermines the agency of women while failing to protect other vulnerable groups.

2.5. Australia: State-Based Criminalisation and Regulatory Innovation

Australia addresses cyber-stalking primarily at the state and territory level. For instance, Queensland's *Criminal Code Act 1899* includes Section 359E, which criminalises stalking conducted through electronic means, including text, email, and social media. The law requires a "course of conduct" that causes detriment to the victim and includes examples such as surveillance, threats, and impersonation.

Victoria's legislation similarly defines stalking broadly to include cyber activities that cause physical or mental harm or arouse apprehension or fear. These provisions reflect an expansive understanding of harm, including psychological and emotional impacts.

At the federal level, the Enhancing Online Safety Act 2015 created the Safety Commissioner, an independent regulator with powers to compel platforms to take down harmful content and issue compliance notices. While not a criminal enforcement agency, the eSafety regime represents a proactive regulatory model aimed at prevention and victim support.

Australia's approach has been praised for balancing safety and expression, though concerns remain about the accountability of private platforms and potential overreach in content regulation.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

2.6. Nigeria's Legal Approach to Cyber-Stalking

Nigeria addresses cyber-stalking primarily through the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, which criminalizes various forms of cyber-related offences, including online harassment and stalking.

2.6.1. Statutory Provision

Section 24 of the Cybercrimes Act criminalizes the use of computers or network systems to send messages that are "grossly offensive," "indecent," "obscene," or "menacing," as well as communications intended to cause "annoyance," "inconvenience," or "needless anxiety." The penalty for violating this section can include fines and imprisonment of up to three years.

2.6.2. Criticism and Judicial Review

This provision has faced strong criticism for being vague, overbroad, and incompatible with constitutional and international guarantees of freedom of expression.In *SERAP v. Federal Republic of Nigeria*, the ECOWAS Court of Justice ruled that Section 24 of the Act violated the right to freedom of expression protected under Article 9 of the African Charter on Human and Peoples' Rights.

2.6.3. Practical Application

Despite the court's decision, Nigerian authorities have continued to use Section 24 to arrest journalists, critics, and activists, often on the grounds of cyber-stalking. This reflects a broader tension between the state's interest in curbing online abuse and the imperative to protect civil liberties.

2.6.4. Calls for Reform

Civil society groups, legal scholars, and international observers have called for the repeal or amendment of Section 24 to align it with constitutional protections and international human rights standards. Proposed reforms suggest narrowing the language to target genuinely harmful conduct while ensuring due process and judicial oversight.

2.6. Comparative Observations

The above legal frameworks reveal significant divergences in how jurisdictions conceptualise and criminalise cyber-stalking. While some countries adopt high thresholds to protect freedom of expression (e.g., the US), others prioritise victim protection and offer broader legal definitions (e.g., the UK, Australia, Nigeria).

From the discuss above the following few key patterns emerges:

- Jurisdictions differ on whether actual harm must be shown or whether intent alone suffices. The US leans toward a subjective intent standard, while others, like the UK, incorporate a more objective threshold.
- Most laws require a pattern of behaviour rather than isolated acts, which helps to filter out protected speech.
- Emerging models in the EU and Australia emphasize co-regulation, where states mandate compliance mechanisms for digital platforms.
- Some legal systems, notably India and the EU, have developed laws recognising the gender sensitive nature of cyber-stalking.

Legal responses to cyber-stalking illustrate a dynamic tension between personal security and expressive liberty. No jurisdiction has found a perfect equilibrium, but comparative analysis highlights best practices, such as precise statutory language, evidentiary safeguards, and proportionality reviews, that can help strike a fair balance. As online abuse continues to evolve, legal systems must remain

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

agile, ensuring that the protection of individuals from harassment does not come at the cost of silencing legitimate speech.

3.0. Freedom of Speech in International Law

Freedom of speech is a cornerstone of democratic societies and a fundamental human right enshrined in various international legal instruments. However, the advent of digital communication has introduced complexities, particularly concerning cyber-stalking—a form of online harassment that can infringe upon individuals' rights and well-being. This section explores the international legal frameworks governing freedom of speech, analyzes how they address the challenges posed by cyber-stalking, and examines the balance between protecting free expression and safeguarding individuals from online abuse.

3.1. International Legal Frameworks Protecting Freedom of Speech

3.1.1 Universal Declaration of Human Rights (UDHR)

Article 19 of the UDHR proclaims that "everyone has the right to freedom of opinion and expression," encompassing the freedom to hold opinions without interference and to seek, receive, and impart information through any media.Although the UDHR is not legally binding, it serves as a foundational document influencing subsequent treaties and national constitutions.

3.1.2 International Covenant on Civil and Political Rights (ICCPR)

The ICCPR, a binding treaty, reiterates the right to freedom of expression in Article 19, emphasizing the freedom to seek, receive, and impart information of all kinds. However, Article 19(3) permits restrictions on this right, provided they are:

- ✓ Prescribed by law;
- ✓ Necessary for respect of the rights or reputations of others;
- ✓ Necessary for the protection of national security, public order, public health, or morals.

This framework allows states to implement measures against harmful speech, including cyber-stalking, while ensuring that such restrictions are lawful, necessary, and proportionate.

3.2. European Convention on Human Rights (ECHR)

Article 10 of the ECHR guarantees the right to freedom of expression, subject to certain restrictions similar to those in the ICCPR.The European Court of Human Rights (ECHR) has developed a substantial body of case law interpreting these provisions, balancing free expression with other rights such as privacy and protection from harassment.

3.3. Balancing Freedom of Speech and Protection from Cyber-Stalking

3.3.1 The Principle of Proportionality

International human rights law mandates that any restriction on freedom of expression must be proportionate to the legitimate aim pursued. In the context of cyber-stalking, this means that measures taken to prevent or punish such behavior must not unduly infringe upon free speech rights.

3.3.2 ECHR Jurisprudence

In *Handyside v. United Kingdom*, the ECHR emphasized that freedom of expression applies not only to information that is favorably received but also to that which "offends, shocks or disturbs."However, in cases like *Delfi AS v. Estonia*, the Court upheld liability for online platforms that failed to prevent defamatory comments, highlighting the need to protect individuals from harmful speech.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

3.3.3 The African Charter on Human and Peoples' Rights

Article 9 of the African Charter affirms the right to receive information and to express and disseminate opinions within the law. The African Commission on Human and Peoples' Rights has interpreted this provision to require that any restrictions on expression must serve a legitimate interest and be necessary and proportionate.

3.4. Cyber-Stalking: A Challenge to Freedom of Speech

3.4.1 Defining Cyber-Stalking

Cyber-stalking involves the use of electronic communication to harass or intimidate individuals, often characterized by repeated and unwanted contact. While such behavior can cause significant harm, legal responses must carefully distinguish between unlawful harassment and protected speech.

3.4.2 Legal Responses and Concerns

Some jurisdictions have enacted laws targeting cyber-stalking, but concerns arise when such laws are overly broad or vague, potentially criminalizing legitimate expression. For instance, Nigeria's Cybercrime Act of 2015 has been criticized for its expansive definition of cyber-stalking, which includes sending messages deemed "offensive" or "annoying." The ECOWAS Court of Justice ruled that certain provisions of this Act violated the right to freedom of expression under international law.

3.5. Ensuring Compatibility with International Standards

3.5.1 Necessity and Proportionality Tests

To align with international human rights standards, laws addressing cyber-stalking must pass the necessity and proportionality tests. This entails demonstrating that restrictions on speech are essential to achieve a legitimate aim and are the least restrictive means available.

3.5.2 Safeguards Against Abuse

Legal frameworks should incorporate safeguards to prevent misuse, such as:

- ✓ Clear definitions of prohibited conduct;
- ✓ Requirements for intent or malice;
- ✓ Protections for journalistic and political expression.

These measures help ensure that efforts to combat cyber-stalking do not inadvertently suppress legitimate discourse. While cyber-stalking poses real threats to individuals' safety and well-being, responses must be carefully calibrated to uphold the fundamental right to freedom of speech. International legal instruments provide a framework for balancing these interests, emphasizing that any restrictions on expression must be lawful, necessary, and proportionate. As digital communication continues to evolve, ongoing vigilance is required to protect both individual rights and the broader democratic discourse.

4.0. Jurisprudential Conflicts and Doctrinal Challenges

The proliferation of digital communication platforms has amplified concerns regarding cyber-stalking and its intersection with the right to freedom of speech. While international legal instruments uphold freedom of expression, they also recognize the necessity of restricting certain forms of speech to protect individuals from harm. This duality presents jurisprudential conflicts and doctrinal challenges, particularly when addressing cyber-stalking, a phenomenon that blurs the lines between protected expression and unlawful harassment. This section examines these complexities, analyzing how various legal systems and international bodies navigate the delicate balance between safeguarding free speech and preventing cyber-stalking.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

4.1. Definitional Ambiguities and Legal Interpretations

4.1.1. The Challenge of Defining Cyber-Stalking

Cyber-stalking lacks a universally accepted definition, leading to inconsistencies in legal interpretations and enforcement. Generally, it encompasses the use of electronic communication to harass, threaten, or intimidate individuals. However, the absence of a clear, standardized definition complicates the development of coherent legal frameworks, resulting in varied approaches across jurisdictions.

4.1.2. Freedom of Speech: Scope and Limitations

International instruments like the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) enshrine the right to freedom of expression. Nonetheless, these rights are not absolute. Article 19(3) of the ICCPR permits restrictions on expression to protect the rights or reputations of others, national security, public order, or public health or morals.Similarly, Article 10(2) of the ECHR allows for limitations necessary in a democratic society. These provisions necessitate a balancing act between protecting free speech and preventing harm, a task complicated by the nuanced nature of cyber-stalking.

4.2. Jurisprudential Conflicts in Addressing Cyber-Stalking

4.2.1. The Delfi AS v. Estonia Case

In *Delfi AS v. Estonia*, the European Court of Human Rights (ECtHR) held that an online news portal could be held liable for defamatory comments posted by its readers, even if the comments were removed upon request. The Court reasoned that the portal had a duty to prevent harm caused by third-party content. This decision sparked debate over intermediary liability and its im4.2lications for freedom of expression, highlighting the tension between protecting individuals from harmful speech and preserving open discourse online.

4.2.2. The Nigerian Cybercrime Act and Its Implications

Nigeria's Cybercrime (Prohibition, Prevention, etc.) Act of 2015, particularly Section 24, criminalizes the sending of messages deemed "grossly offensive" or of "menacing character."Critics argue that the provision's vague language has been used to suppress dissent and target journalists.In *SERAP v. Federal Republic of Nigeria*, the ECOWAS Court of Justice ruled that Section 24 violated the right to freedom of expression under international law, ordering its repeal.Despite this judgment, enforcement remains inconsistent, illustrating the challenges in aligning domestic laws with international standards.

4.3. Doctrinal Challenges in Balancing Rights

4.3.1. The Principle of Proportionality

A central doctrinal challenge lies in applying the principle of proportionality—ensuring that restrictions on speech are necessary and the least intrusive means to achieve a legitimate aim. In cases of cyber-stalking, determining what constitutes a proportionate response involves assessing the severity of the conduct and its impact on victims, while also considering the potential chilling effect on free expression.

4.3.2. The Margin of Appreciation Doctrine

The ECtHR's margin of appreciation doctrine allows states a degree of discretion in implementing the ECHR, acknowledging cultural and legal differences. However, this flexibility can lead to divergent standards in addressing cyber-stalking, potentially undermining the uniform protection of rights across jurisdictions. The doctrine's application requires careful scrutiny to prevent the erosion of fundamental freedoms.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

4.4. The Role of Intent and Context in Legal Assessments

Assessing cyber-stalking cases necessitates an examination of the perpetrator's intent and the context of the communication. Distinguishing between malicious harassment and legitimate expression is complex, particularly when speech is conveyed through satire, criticism, or political commentary. Legal systems must develop nuanced criteria to evaluate such cases, ensuring that protective measures do not inadvertently suppress lawful expression.

4.5. The Impact of Technology on Legal Frameworks

The rapid evolution of technology outpaces the development of legal frameworks, creating gaps in addressing cyber-stalking. Social media platforms, encrypted messaging apps, and anonymous communication tools complicate the identification and prosecution of offenders. Legal systems must adapt to these technological advancements, incorporating digital literacy and forensic capabilities to effectively combat cyber-stalking without infringing on free speech.

4.6. Recommendations for Harmonizing Legal Approaches

To reconcile the protection of individuals from cyber-stalking with the preservation of freedom of speech, the following measures are recommended:

- Establish precise legal definitions of cyber-stalking to prevent arbitrary enforcement and ensure consistency across jurisdictions.
- Apply the principles of proportionality and necessity rigorously when restricting speech, ensuring that measures are appropriate and minimally intrusive.
- Implement safeguards to prevent the misuse of cyber-stalking laws for political or repressive purposes, including judicial oversight and transparency mechanisms.
- Foster international collaboration to develop harmonized standards and share best practices in addressing cyber-stalking while upholding human rights.
- Invest in technological tools and expertise to detect and address cyber-stalking effectively, balancing enforcement with respect for privacy and expression.

The intersection of cyber-stalking and freedom of speech presents complex jurisprudential conflicts and doctrinal challenges. Legal systems must navigate the delicate balance between protecting individuals from online harassment and preserving the fundamental right to free expression. Achieving this equilibrium requires clear legal definitions, adherence to proportionality principles, safeguards against abuse, international cooperation, and technological adaptation. By addressing these challenges thoughtfully, societies can uphold both individual dignity and the vibrant discourse essential to democratic life.

5.0. Regulatory and Policy Implications

The digital age has ushered in unprecedented avenues for communication, enabling individuals to express themselves across borders. However, this freedom has also facilitated the emergence of cyber-stalking—a pernicious form of harassment that exploits digital platforms to intimidate, threaten, or silence individuals. The regulatory and policy responses to cyber-stalking must navigate the delicate balance between protecting individuals from harm and upholding the fundamental right to freedom of speech. This section examines the international legal frameworks addressing cyber-stalking, analyzes national legislative approaches, and explores the policy implications of regulating online harassment without encroaching upon free expression.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

5.1. International Legal Frameworks

5.1.1. The Budapest Convention on Cybercrime

The Council of Europe's Convention on Cybercrime (Budapest Convention) is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. While the Convention does not explicitly define cyber-stalking, it provides a framework for criminalizing various forms of online misconduct, including illegal access, data interference, and content-related offenses. Signatory states are encouraged to enact legislation that addresses emerging cyber threats while respecting human rights and fundamental freedoms.

5.1.2. Human Rights Instruments

International human rights instruments, such as the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), enshrine the right to freedom of expression.However, these rights are not absolute. Article 19(3) of the ICCPR permits restrictions on freedom of expression to protect the rights or reputations of others, national security, public order, or public health or morals. Similarly, Article 10(2) of the ECHR allows for limitations necessary in a democratic society. These provisions provide a legal basis for regulating cyber-stalking, provided that such regulations are necessary, proportionate, and prescribed by law.

5.2. National Legislative Approaches

5.2.1. Nigeria's Cybercrime Act

Nigeria's Cybercrime (Prohibition, Prevention, etc.) Act of 2015, particularly Section 24, criminalizes the sending of messages deemed "grossly offensive" or of "menacing character." Critics argue that the provision's vague language has been used to suppress dissent and target journalists. In *SERAP v. Federal Republic of Nigeria*, the ECOWAS Court of Justice ruled that Section 24 violated the right to freedom of expression under international law, ordering its repeal. Despite this judgment, enforcement remains inconsistent, illustrating the challenges in aligning domestic laws with international standards.

5.2.2. Germany's Network Enforcement Act

Germany's Network Enforcement Act (NetzDG) requires social media platforms to remove "obviously illegal" content within 24 hours of notification.While aimed at combating hate speech and online harassment, the law has faced criticism for incentivizing over-blocking and potentially infringing upon freedom of expression. The rapid removal requirements may lead platforms to err on the side of caution, suppressing lawful speech to avoid penalties.

5.2.3. United Kingdom's Communications Act

The UK's Communications Act 2003, specifically Section 127, criminalizes the sending of messages that are "grossly offensive" or of an "indecent, obscene or menacing character" over public electronic communications networks. The provision has been used to prosecute individuals for social media posts, raising concerns about its impact on free speech. In response, the Director of Public Prosecutions issued guidelines to ensure that only communications constituting credible threats or harassment are prosecuted.

5.3. Policy Implications

5.3.1. Balancing Protection and Expression

Regulating cyber-stalking necessitates a careful balance between protecting individuals from harm and preserving freedom of expression. Overly broad or vague laws risk criminalizing legitimate speech, while insufficient regulation may leave victims vulnerable. Policymakers must ensure that legal

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

definitions of cyber-stalking are precise and that enforcement mechanisms are transparent and accountable.

5.3.2. Role of Online Platforms

Online platforms play a pivotal role in moderating content and preventing cyber-stalking. However, delegating censorship responsibilities to private entities raises concerns about due process and accountability.Regulations should establish clear guidelines for content moderation, ensuring that platforms respect users' rights while addressing harmful behavior.

5.3.3. International Cooperation

Cyber-stalking often transcends national borders, necessitating international cooperation in enforcement and policy development. Harmonizing legal definitions and standards can facilitate cross-border investigations and prosecutions. International bodies should promote the exchange of best practices and support capacity-building efforts in countries developing cybercrime legislation.

5.4. Recommendations

To effectively address cyber-stalking while safeguarding freedom of speech, the following measures are recommended:

- Legislations should define cyber-stalking with specificity to prevent misuse and ensure that only genuinely harmful conduct is penalized.
- Restrictions on expression must be necessary to achieve a legitimate aim and proportionate to the harm addressed.
- Enforcement actions should be subject to judicial review to protect against arbitrary or excessive measures.
- Online platforms should implement transparent content moderation policies and provide avenues for users to appeal decisions.
- Countries should engage in cooperative efforts to harmonize laws, share information, and support victims of cyber-stalking.

Cyber-stalking presents a significant challenge in the digital era, threatening individuals safety and well-being. Regulatory and policy responses must carefully navigate the intersection of protecting individuals from online harassment and upholding the fundamental right to freedom of speech. By enacting precise, proportionate, and transparent laws, and fostering international cooperation, societies can address cyber-stalking effectively without compromising democratic values.

6.0. Normative and Legal Recommendations

The digital age has revolutionized communication, offering unprecedented avenues for expression. However, it has also facilitated cyber-stalking—a pervasive form of harassment that exploits digital platforms to intimidate, threaten, or silence individuals. Addressing cyber-stalking necessitates a delicate balance: protecting individuals from harm while safeguarding the fundamental right to freedom of speech. This section provides normative and legal recommendations to navigate this complex intersection, ensuring that measures against cyber-stalking do not inadvertently suppress legitimate expression.

6.1. Clarify Legal Definitions and Scope

6.1.1. Precise Definition of Cyber-Stalking

A clear and precise legal definition of cyber-stalking is essential to prevent misuse of laws and to ensure that only genuinely harmful conduct is penalized. Vague or overly broad definitions can lead to

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

arbitrary enforcement and may infringe upon freedom of expression.[1] Legislators should delineate cyber-stalking to encompass intentional, repeated, and targeted online behavior that causes substantial emotional distress or fear for safety.

6.1.2. Distinguish Between Harassment and Legitimate Expression

Legal frameworks must differentiate between unlawful harassment and protected speech. For instance, criticism of public figures, satire, or unpopular opinions, while potentially offensive, are often protected under international human rights law. Laws should avoid criminalizing speech solely based on its offensive nature unless it crosses the threshold into targeted harassment or incitement to violence.

6.2. Ensure Compliance with International Human Rights Standards

6.2.1. Adherence to the Principle of Proportionality

Any restriction on freedom of expression must be proportionate to the legitimate aim pursued. Measures against cyber-stalking should be the least intrusive means necessary to achieve the intended protection, ensuring that they do not unduly burden free speech.

6.2.2. Incorporate Safeguards Against Abuse

To prevent the misuse of cyber-stalking laws for political or repressive purposes, legal frameworks should incorporate safeguards such as judicial oversight, transparency in enforcement, and avenues for appeal. These mechanisms help maintain the legitimacy of laws and protect individuals from arbitrary or discriminatory application.

6.3. Promote International Cooperation and Harmonization

6.3.1. Align National Laws with International Instruments

Countries should harmonize their cyber-stalking laws with international treaties and conventions, such as the Budapest Convention on Cybercrime, which provides a framework for addressing cybercrime while respecting human rights. Aligning national laws with international standards facilitates cross-border cooperation and ensures consistency in addressing cyber-stalking globally.

6.3.2. Foster Cross-Border Collaboration

Given the transnational nature of cyber-stalking, international cooperation is vital. States should engage in mutual legal assistance, share best practices, and participate in joint initiatives to combat cyber-stalking effectively. Collaborative efforts enhance the capacity to address cyber-stalking that transcends national boundaries

6.4. Encourage Responsible Platform Governance

6.4.1. Establish Clear Guidelines for Online Platforms

Online platforms play a crucial role in moderating content and preventing cyber-stalking. Governments should work with platforms to develop clear guidelines that define unacceptable behavior and outline procedures for reporting and addressing cyber-stalking incidents.

6.4.2. Ensure Transparency and Accountability

Platforms should be transparent about their content moderation policies and enforcement actions. Regular transparency reports can provide insights into how cyber-stalking cases are handled, fostering trust among users and stakeholders.

1

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

6.5. Support Victims and Raise Awareness

6.5.1. Provide Accessible Support Mechanisms

Victims of cyber-stalking should have access to support services, including legal assistance, counseling, and safe reporting channels. Governments and civil society organizations should collaborate to establish comprehensive support systems.

65.2. Implement Public Awareness Campaigns

Educational initiatives can inform the public about the nature of cyber-stalking, its legal implications, and available resources for victims. Awareness campaigns can also promote respectful online behavior and discourage harassment. Addressing cyber-stalking requires a multifaceted approach that balances the protection of individuals with the preservation of freedom of speech. By clarifying legal definitions, ensuring compliance with international human rights standards, promoting international cooperation, encouraging responsible platform governance, and supporting victims, societies can effectively combat cyber-stalking while upholding the fundamental right to expression.

7.0. Conclusion

The phenomenon of cyber-stalking presents a modern legal and normative challenge in the digital age, bringing into sharp focus the tension between the protection of individual rights and the preservation of fundamental freedoms. While cyber-stalking is a demonstrably harmful practice that can lead to psychological trauma, reputational damage, and chilling effects on speech, particularly for marginalized or vulnerable groups, its regulation must be carefully calibrated to avoid the unintended consequence of suppressing legitimate expression. The core of the legal dilemma lies in the dual imperative of safeguarding individuals from online harassment while upholding the principle of freedom of expression as enshrined in major international instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). The right to free speech is not absolute and may be subject to restrictions where necessary for the protection of others' rights; however, such restrictions must meet the tests of legality, legitimacy, necessity, and proportionality. Many jurisdictions have introduced cybercrime or anti-harassment laws that attempt to address cyber-stalking, but these efforts have too often resulted in overbroad statutes with vague terms such as "grossly offensive" or "annoying," which risk criminalizing a wide range of lawful speech. The judicial invalidation of such provisions in cases like *SERAP v Nigeria* and *Rynearson v Ferguson* underscores the importance of precision in legal drafting and the need for safeguards against arbitrary application.

Moreover, as cyber-stalking often transcends national boundaries, international cooperation and harmonization of standards become crucial. Instruments like the Budapest Convention on Cybercrime offer a model for cross-border collaboration, but more inclusive, rights-respecting global frameworks are needed. At the same time, online platforms—often the arenas where cyber-stalking occurs—must take proactive roles in moderating content, supporting victims, and ensuring that moderation practices are transparent, fair, and consistent with international human rights norms.

What emerges from this analysis is the need for a balanced regulatory approach that:

- Provides clear, narrowly defined legal provisions on cyber-stalking that avoid infringing on lawful speech;
- Incorporates robust procedural safeguards, including judicial oversight and rights of appeal;
- Emphasizes education and awareness to shift cultural norms and deter online harassment;
- Encourages platform accountability while maintaining room for lawful discourse;
- Fosters international cooperation in both enforcement and standard-setting.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Ultimately, the challenge of addressing cyber-stalking is not merely a matter of drafting better law,it is a test of our commitment to upholding democratic principles in the digital era. Protecting individuals from harm must not come at the expense of silencing dissent or curtailing public discourse. A human rights-centered approach, grounded in legal precision and informed by jurisprudence and digital realities, offers the most promising path forward in navigating this complex terrain.

Outline

1. Conceptual Framework

- ✓ Definition and typology of cyber-stalking
- ✓ Legal characteristics distinguishing cyber-stalking from other online abuses
- ✓ The legal definition and scope of freedom of speech under international law

2. Legal Approaches to Cyber-Stalking

- ✓ Comparative overview: United States, European Union, India, and Australia
- ✓ Statutory frameworks and criminalization
- ✓ Civil remedies and protection orders

3. Freedom of Speech in International Law

- ✓ Article 19 of the ICCPR and UDHR
- ✓ Permissible limitations under international human rights law
- ✓ Jurisprudence from international and regional courts (e.g., ECtHR, UNHRC)

4. Jurisprudential Conflicts and Doctrinal Challenges

- ✓ Case studies where cyber-stalking laws have conflicted with speech rights
- ✓ Ambiguities in defining “threat,” “distress,” and “harassment”
- ✓ Chilling effects and overbreadth concerns

5. Regulatory and Policy Implications

- ✓ The role of social media platforms in moderating speech and abuse
- ✓ Challenges in enforcement and transnational jurisdiction
- ✓ Due process and proportionality in regulatory responses

6. Normative and Legal Recommendations

- ✓ Principles for drafting balanced cyber-stalking legislation
- ✓ Enhancing safeguards for freedom of expression in enforcement
- ✓ Multi-stakeholder approaches: law, technology, and civil society

7. Conclusion

- ✓ Summary of key findings
- ✓ The future of digital speech governance in the context of rising online abuse
- ✓ The need for dynamic legal tools to mediate between liberty and security

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Reference

1. United Nations, "Universal Declaration of Human Rights," 1948. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights
2. United Nations, "International Covenant on Civil and Political Rights," 1966. [Online]. Available: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
3. U. N. Human Rights Committee, "General Comment No. 34 on Article 19: Freedoms of opinion and expression," CCPR/C/GC/34, 2011.
4. European Court of Human Rights, "Handyside v. the United Kingdom," App. No. 5493/72, 1976.
5. European Court of Human Rights, "Delfi AS v. Estonia," App. No. 64569/09, 2015.
6. ECOWAS Court of Justice, "SERAP v. Federal Republic of Nigeria," Judgment ECW/CCJ/APP/09/17, 2020.
7. Budapest Convention on Cybercrime, Council of Europe, ETS No. 185, 2001.
8. Federal Government of Nigeria, Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
9. Supreme Court of the United States, "Elonis v. United States," 575 U.S. 723, 2015.
10. Protection from Harassment Act 1997, United Kingdom, as amended by Protection of Freedoms Act 2012.
11. Government of India, Information Technology Act, 2000.
12. Supreme Court of India, "Shreya Singhal v. Union of India," Writ Petition (Criminal) No. 167 of 2012.
13. European Commission, "Proposal for a Directive on combating violence against women and domestic violence," COM(2022) 105 final.
14. Australian Government, "Enhancing Online Safety Act," 2015. [Online]. Available: https://www.legislation.gov.au/Details/C2015A00024
15. German Bundestag, "Network Enforcement Act (NetzDG)," 2017. [Online]. Available: https://www.bmj.de/EN/Ministry/NetworkEnforcementAct/NetworkEnforcementAct_node.html