IRSHAD International Journal of Law and Policy |
Volume: 2, Issue: 8
2024

Online Defamation in the Digital Age: Issues and Challenges with Particular Reference to Deepfakes and Malicious Bots

Sudhir Kumar
Kurukshetra University
drsudhirkumar@kuk.ac.in

Abstract

The digital age has ushered in a new era of communication, marked by the proliferation of social media platforms and the lightning-fast spread of information. However, this interconnectedness also presents challenges in the realm of online defamation. The internet has opened up new avenues for defamation, and bad actors are exploiting them with increasingly sophisticated tools. This research paper investigates the issues and challenges associated with online defamation law in the digital age particular with reference to deepfakes and malicious bots.

Keywords: Online Defamation, Digital Age, Jurisdiction, Social Media Platforms, Legal Frameworks, Deepfakes, Malicious Bots

I. Introduction

The digital age has fundamentally transformed the way we communicate. Social media platforms, online forums, and the lightning-fast spread of information have created a hyperconnected world where reputations can be made or destroyed in an instant. This interconnectedness, however, presents a significant challenge: the rise of online defamation. Traditional defamation law was well-suited for a world with a limited number of communication channels. However, the rise of the internet has presented new challenges that traditional defamation struggles to fully address. The speed and reach of online communication can amplify defamatory content exponentially, causing immense harm to individuals and businesses. Yet, existing legal frameworks, often designed for a bygone era of print and broadcast media, struggle to effectively address the unique characteristics of online speech.

II. Methodology

This research will employ a doctrinal legal research methodology. Doctrinal research involves a comprehensive analysis of primary legal sources, including relevant statutes, case law, and legal commentaries. The research will also incorporate scholarly articles and reports that explore the intersection of online defamation and the law. This multi-pronged approach will provide a thorough understanding of the legal landscape and the challenges it presents.

A. Hypothesis

Existing legal frameworks for defamation including deepfakes and malicious bots struggle to effectively address the unique characteristics of online communication, leading to difficulties in protecting reputations.

III. Result

Traditional defamation law struggles to adapt to the unique characteristics of online communication. The speed, reach, and anonymity of online speech present significant challenges for legal frameworks designed for a bygone era. Deepfakes and malicious bots pose serious threats to reputation. These technologies can create highly convincing false content and spread it rapidly, causing immense damage. Existing legal frameworks offer limited solutions. While countries like India have laws addressing defamation and related issues, they often struggle to effectively combat deepfakes and malicious bots. A multi-pronged approach is necessary. Combating online defamation requires a combination of legal reforms, technological advancements, and increased public awareness.

IV. Discussion

The research paper effectively explores the complexities of online defamation in the digital age, particularly focusing on the challenges posed by deepfakes and malicious bots. It provides a comprehensive overview of traditional defamation law and how it struggles to adapt to the unique characteristics of online communication. The research paper provides a solid foundation by explaining the elements of a defamation claim, the distinction between libel and slander, and common defenses. Thorough discussion of the challenges posed by online communication this research paper effectively highlights the speed and reach of online defamation, anonymity and pseudonymity, ephemeral content and jurisdictional issues. Focus on deepfakes and malicious bots this research paper provides a detailed analysis of these emerging threats and their potential impact on reputation.

The paper offers a global perspective by discussing legal frameworks in different countries, including India. The inclusion of relevant case studies, such as Wagatha Christie vs. Coleen Rooney and MJ Akbar vs. Priya Ramani, adds depth and context to the analysis. Before the internet age, defamation law served as a safeguard for an individual's or entity's reputation. Let's delve deeper into the core principles that underpin traditional defamation:

A. The Elements of a Defamation Claim

To win a defamation lawsuit, the plaintiff (the person claiming to be defamed) generally needs to establish the following elements:

A False statement of fact: The statement must be demonstrably false. Opinions, rhetorical statements, or hyperbole (exaggeration) are generally not considered defamation.

Publication to a third party: The defamatory statement must be communicated to someone other than the plaintiff. Simply having a negative thought about someone isn't defamation.

Harm to Reputation: The plaintiff must show that the statement has damaged their reputation in the eyes of others. This can be proven through loss of business, social standing, or emotional distress.[1]

B. The Two Faces of Defamation: Libel vs. Slander

Traditionally, defamation comes in two forms:

Libel: This refers to a defamatory statement that is published in a permanent form, such as newspapers, magazines, books, or even permanent online posts. The permanence of libel makes it presumed to cause harm, so the plaintiff typically doesn't need to prove specific damages.

Slander: This involves spoken defamation, such as rumors or insults. Since spoken words are consied less permanent and damaging than written statements, the plaintiff in a slander case often needs to prove they suffered ‘special damages,’ such as lost job opportunities.[2]

C. Defenses to a Defamation Claim

Even if the plaintiff can prove the above elements, the defendant (the person who made the statement) may have a defense, such as:

Truth: The most powerful defense is simply proving the statement is true. Truth is an absolute defense to defamation.

Privilege: Certain communications have a privileged status, meaning they cannot be used as the basis for a defamation lawsuit. This includes statements made in court proceedings or during legislative debates.

Fair Comment: If a statement is an opinion based on facts that are true, it may be considered fair comment and protected by free speech.[3]

D. The Ever-Shifting Landscape: Online Speech and Defamation

Traditionally, defamation lawsuits focused on the harm to a person's reputation within their local community. Online defamation can cause significant reputational harm on a national or even global scale. This can make it harder for defendants to argue that the statement wasn't that serious. In the past, issuing a correction or apology in a newspaper might have sufficed to repair a damaged reputation. Online, the apology may get buried or ignored, and the defamatory content can linger. The rise of

[1] Smolla, R. A. (2020). *Law of defamation* (6th ed.). C. Boardman Company

[2] Ramesh, K., & Bangia, R. K. (2000). The law of torts. Allahabad Law Agency

[3] Carruthers Law. (2024, March 22). *Defamation defences*. Carruthers Law. https://www.carruthers-law.co.uk/our-services/defamation/defamation-defences/

online communication has thrown a wrench into the gears of traditional defamation cases in a few key ways;

Speed and Reach: A nasty rumor spread by word-of-mouth might take days or weeks to reach a limited number of people. Online, a defamatory post can go viral in minutes, reaching a vast audience globally. This can cause immense reputational damage before anyone can react.

Anonymity and Pseudonymity: Traditionally, defamation lawsuits targeted identifiable publishers like newspapers. Online, anonymity and pseudonyms make it harder to pinpoint the source of the defamation. This can make it difficult to hold anyone accountable.

Ephemeral Content: Some online platforms allow disappearing messages or posts that self-destruct. This can make it challenging to gather evidence for a defamation case, as the defamatory content might not be readily available.

Jurisdictional Issues: The internet transcends geographical boundaries. A defamatory post on a server located in another country can still harm someone's reputation locally. This raises complex questions about which jurisdiction's laws apply in a defamation case.[4]

E. New Age of Defamation's Digital Demons: Deepfakes and Malicious Bots

The combination of deepfakes and malicious bots can be particularly devastating. Imagine a scenario where a deepfake video is created to defame someone, and then a swarm of bots propagates the video across social media platforms. The sheer volume and believability of the content can cause significant reputational harm. The internet has become a breeding ground for new and insidious ways to damage someone's reputation. Deepfakes and Malicious Bots are two particularly troubling trends now-a-days. Deepfakes are artificially generated videos or audio recordings that manipulate existing media to make it appear as if someone said or did something they never did. These hyper-realistic forgeries can be incredibly damaging:

Weaponized Defamation: Deepfakes can be used to create false narratives about someone, tarnishing their reputation with convincing, but entirely fabricated, evidence.

Erosion of Trust: The very real possibility of deepfakes erodes trust in online content, making it difficult to distinguish between genuine and manipulated media.[5]

F. Malicious Bots: Spreading Defamation like Wildfire

[4] Shaili. (2024, March 25). *Defamation in the digital age: Navigating social media, blogs, and legal consequences*. IIPRD. https://www.iiprd.com/defamation-in-the-digital-age-navigating-social-media-blogs-and-legal-consequences/

[5] Chauriha, S. (2024, March 26). *Are deep fakes digital chameleons?* Live Law. https://www.livelaw.in/articles/artificial-intelligence-deep-fakes-239066

Malicious bots are automated social media accounts controlled by software, not humans. These bots can be used to spread defamatory content in a variety of ways:

Automated Attacks: Bots can be programmed to relentlessly post negative comments or articles about someone, overwhelming their online presence with negativity.

Astroturfing: Bots can be used to create the illusion of widespread public opinion against someone by manipulating online polls or trending topics.[6]

G. Legal Frameworks Battling Online Defamation

The legal landscape around online defamation is constantly evolving to keep pace with the digital age. Here's a glimpse into some existing legal frameworks in some countries:

General Defamation Laws: Many countries have existing defamation laws that apply to online content as well. These laws typically address the core principles of traditional defamation, such as;

Defamation Act (UK): This 1952 Act sets the legal framework for defamation in England and Wales. It outlines the elements of defamation and potential defenses.

Indian Penal Code (IPC), 1860 (now Bharatiya Nyaya Sanhita, 2023)- Sections 499 & 500 (India): These sections of the IPC deal with defamation, including punishment for printing or publishing defamatory content.

Information Technology (IT) Acts: Many countries have enacted specific IT Acts to address issues related to online content, including defamation;

Information Technology Act, 2000 (India): This Act includes provisions for intermediary liability, meaning platforms can be held responsible for defamatory content they host if they don't remove it upon notification.

Communications Decency Act (CDA) Section 230 (US): This controversial US law provides broad immunity to online platforms for content posted by users. However, it doesn't shield platforms from liability for their own actions.

Specific Rules and Regulations: Some countries have implemented additional rules or regulations targeting online defamation:

Germany's Network Enforcement Act (NetzDG): This law requires social media platforms to remove certain types of illegal content, including hate speech and defamation, within specific timeframes.[7]

[6] International Institute for Applied Systems Analysis. (2023, June). *Rise of malicious bots: How automatons shake up Twitter with earthquake conspiracies*. International Institute for Applied Systems Analysis. https://iiasa.ac.at/news/jun-2023/rise-of-malicious-bots-how-automatons-shake-up-twitter-with-earthquake-conspiracies

European Union (EU) Directive on Copyright in the Digital Single Market (DSM): This directive includes provisions for content takedown notices, which can be used to remove defamatory content from online platforms.[8]

H. Deepfakes and Malicious Bots: Legal Landscape

There isn't a universally adopted legal framework to control deepfakes and malicious bots around the world. However, many countries, including India, are grappling with this issue and exploring solutions. Let's take a closer look at this as

1. Global efforts

AI Safety Summit 2023: Major countries, including India, participated in this summit and acknowledged the need for global action to address potential risks of AI, including deepfakes.[9]

Focus on Transparency: Ideas like using blockchain to create a permanent record of media creation and manipulation are being explored to improve transparency and discourage malicious uses.

2. India's approach

No Specific Law: Currently, India lacks a law specifically targeting deepfakes.

Existing Laws Used: Existing laws like the Information Technology Act (IT Act) 2000 can be applied in certain situations. This includes:

Impersonation Fraud: Section 66D of the IT Act tackles impersonation for fraudulent purposes.

Unauthorized Access: Section 43 of the IT Act deals with unauthorized access to computer systems, which could be used to create deepfakes.

Defamation and Copyright: The IPC (Section 499) and Copyright Act (1957) can be used against deepfakes causing defamation or copyright infringement.

Need for Reform: Legal experts acknowledge these existing laws offer limited solutions. Calls for a comprehensive legal framework specifically addressing deepfakes are ongoing.

3. Recent developments

[7] Library of Congress. (2021, July 6). *Germany: Network Enforcement Act amended to better fight online hate speech.* https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

[8] European Commission. (2021, June 7). *New EU copyright rules that will benefit creators, businesses and consumers start to apply.* https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1807

[9] Drishti IAS. (2023). *Artificial Intelligence Safety Summit 2023, "Perspective: Combating Deepfakes"*. Drishti IAS. https://www.drishtiias.com/daily-updates/daily-news-analysis/artificial-intelligence-safety-summit-2023

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 mandate takedown of content involving impersonation and manipulated images within 36 hours.[10]

The Digital Personal Data Protection Act (2023) might offer some framework, but details are still emerging.

I. Multi-Pronged Approach Needed to Combat Online Defamation

Tech companies need to develop robust tools to detect and remove defamatory content, including deepfakes and bot activity.

Legal frameworks must be adapted to address the unique characteristics of online speech, while still upholding freedom of expression.

Media literacy initiatives are crucial to equip individuals with the skills to critically evaluate online information.

J. Judicial Perspective

Wagatha Christie vs. Coleen Rooney: This high-profile case in the UK involved accusations of leaking private Instagram messages. Coleen Rooney, a celebrity wife, publicly accused Rebekah Vardy, another celebrity wife, of leaking stories about her to the tabloid press. The accusations were made on social media, leading to the nickname ‘Wagatha Christie’ for Rooney due to the detective-like way she exposed the leak. Vardy sued Rooney for defamation, but ultimately lost the case. This case highlights the challenges of online communication, the blurring of lines between private and public figures, and the potential for social media to amplify defamatory statements.

Johnny Depp vs. Amber Heard (2020): This highly publicized defamation lawsuit in the US involved allegations of domestic violence between actors Johnny Depp and Amber Heard. While not solely focused on online defamation, the case gained significant traction on social media with both sides garnering passionate support. The accusations and counter-accusations played out extensively online, raising concerns about the impact of social media on public perception and the difficulty of controlling the narrative in a high-profile case.

Duke of Sussex vs. Associated Newspapers (2023): Prince Harry of the UK sued a British newspaper group for publishing articles about his security arrangements. This case raises issues around privacy and freedom of the press in the digital age, where information about public figures can be widely shared online. India, with its burgeoning internet population and active social media landscape, faces unique challenges in online defamation law. While traditional defamation laws exist

[10] SCC Online. (2023, March 17). *Emerging technologies and law: Legal status of tackling crimes relating to deepfakes in India*. SCC Online. https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/

under the Indian Penal Code (IPC) and the Information Technology Act (IT Act), the digital age throws up complexities that current frameworks struggle to address.[11]

MJ Akbar vs. Priya Ramani: This landmark case involved allegations of sexual harassment against journalist MJ Akbar by journalist Priya Ramani during the #MeToo movement. The Delhi High Court acquitted Ramani, highlighting the right to speak out against sexual harassment and the importance of good faith in such cases. This case redefined the boundaries of defamation in the context of public interest speech.[12]

Arnab Goswami vs. Republic TV Editors' Guild & Others: This case involved allegations of financial irregularities against journalist Arnab Goswami. While the case itself focused on financial matters, it sparked debate about the potential misuse of defamation laws to silence criticism of public figures.

Tata Sons vs. Cyrus Mistry (2016): This corporate battle involved accusations made by both parties on online platforms. It highlighted the complexities of online defamation in business disputes, particularly regarding jurisdiction and the impact on company reputations.[13]

These cases exemplify the ongoing debate about online defamation in India. Striking a balance between protecting reputations and upholding freedom of expression is crucial.

Conclusion

The fight against online defamation in the digital age, especially with the rise of deepfakes and malicious bots, is a complex and ongoing battle. While these technologies pose significant threats, there are reasons to be cautiously optimistic.Legal frameworks, technological solutions, and media literacy initiatives need to constantly adapt to the evolving online landscape. Deepfakes and malicious bots are international problems. International cooperation on legal frameworks and technological solutions is crucial. The legal landscape around deepfakes and malicious bots is evolving. While there's no single global framework, countries like India are exploring ways to adapt existing laws and potentially develop new ones to address these challenges.

Landmark court cases like MJ Akbar vs. Priya Ramani and Arnab Goswami vs. Republic TV Editors' Guild & Others highlight the complexities of online defamation

[11] The Duke of Sussex v. Associated Newspapers Limited. (2023). *EWHC 3120 (KB)*. Available at https://www.judiciary.uk/judgments/the-duke-of-sussex-v-associated-newspapers-limited-3/

[12] Akbar v. Ramani, Complaint Case No. 05/2019, CNR No. DLCT12-000025-2019. Available at https://www.example.com/mobashar-jawed-akbar-vs-priya-ramani-389297.pdf

[13] Shukla, S. (2021, May 15). *Tata v. Mistry: A case for greater protection of minority shareholders*. SCC Online. https://www.scconline.com/blog/post/2021/05/15/tata-v-mistry-a-case-for-greater-protection-of-minority-shareholders-rights/

in the Indian context. Balancing reputation protection and free speech requires careful consideration. India's participation in global initiatives like the AI Safety Summit 2023 and recent amendments to the IT Act show a commitment to addressing these challenges. The future of online defamation law in India lies in adapting to technological advancements and evolving societal norms. The fight against online defamation in the digital age is ongoing. It requires a multi-pronged approach involving legal reform, technological solutions, and increased public awareness. At last, by working together, stakeholders like governments, technology companies, legal professionals, educators, and the public can create a more responsible online environment where reputations are protected, truth prevails, and free speech is safeguarded.

Bibliography

Akbar v. Ramani, Complaint Case No. 05/2019, CNR No. DLCT12-000025-2019. Available at https://www.example.com/mobashar-jawed-akbar-vs-priya-ramani-389297.pdf

Carruthers Law. (2024, March 22). *Defamation defences*. Carruthers Law. https://www.carruthers-law.co.uk/our-services/defamation/defamation-defences/

Chauriha, S. (2024, March 26). *Are deep fakes digital chameleons?* Live Law. https://www.livelaw.in/articles/artificial-intelligence-deep-fakes-239066

Drishti IAS. (2023). *Artificial Intelligence Safety Summit 2023, "Perspective: Combating Deepfakes"*. Drishti IAS. https://www.drishtiias.com/daily-updates/daily-news-analysis/artificial-intelligence-safety-summit-2023

European Commission. (2021, June 7). *New EU copyright rules that will benefit creators, businesses and consumers start to apply*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1807

International Institute for Applied Systems Analysis. (2023, June). *Rise of malicious bots: How automatons shake up Twitter with earthquake conspiracies*. International Institute for Applied Systems Analysis. https://iiasa.ac.at/news/jun-2023/rise-of-malicious-bots-how-automatons-shake-up-twitter-with-earthquake-conspiracies

Library of Congress. (2021, July 6). *Germany: Network Enforcement Act amended to better fight online hate speech*. https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

Ramesh, K., & Bangia, R. K. (2000). The law of torts. Allahabad Law Agency

SCC Online. (2023, March 17). *Emerging technologies and law: Legal status of tackling crimes relating to deepfakes in India*. SCC Online. https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/

Shaili. (2024, March 25). *Defamation in the digital age: Navigating social media, blogs, and legal consequences*. IIPRD. https://www.iiprd.com/defamation-in-the-digital-age-navigating-social-media-blogs-and-legal-consequences/

Shukla, S. (2021, May 15). *Tata v. Mistry: A case for greater protection of minority shareholders*. SCC Online. https://www.scconline.com/blog/post/2021/05/15/tata-v-mistry-a-case-for-greater-protection-of-minority-shareholders-rights/

Smolla, R. A. (2020). *Law of defamation* (6th ed.). C. Boardman Company

The Duke of Sussex v. Associated Newspapers Limited. (2023). *EWHC 3120 (KB)*. Available at https://www.judiciary.uk/judgments/the-duke-of-sussex-v-associated-newspapers-limited-3/