VOL 8 | Issue 1| Jan-June 2024

ISSN : 2581-6837

jims

JIMS JOURNAL OF LAW

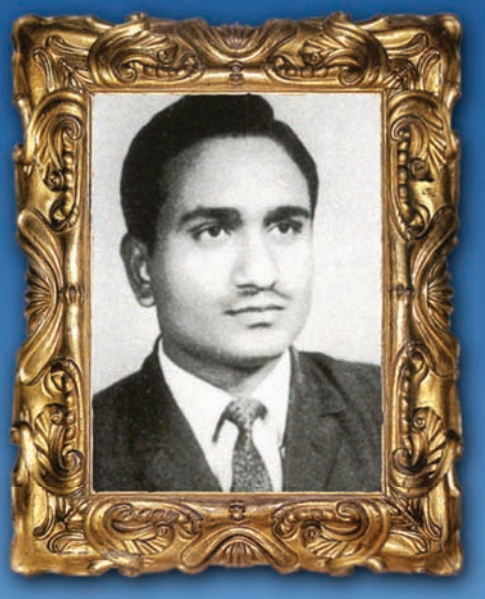
A Bi-Annual Peer Reviewed Journal

JIMS ENGINEERING MANAGEMENT TECHNICAL CAMPUS
48/4, KNOWLEDGE PARK III, Greater NOIDA 201308
www.jimsgn.org

A TRUE VISIONARY

"You see things and you say **Why***? But I dream of things that never were and say* **Why** *not?"*

- George Bernard Shaw



Shri Jagannath Gupta
(1950 - 1980)

Also a true visionary...who dared to dream!
He lives no more but his dreams live on....and on!

JIMS (Rohini)	**-**	**1993**
JIMS (Kalkaji)	**-**	**1997**
JIMS (Vasant Kunj)	**-**	**2003**
JIMS (Jaipur)	**-**	**2003**
JNIT (Jaipur)	**-**	**2004**
JIMS (Greater Noida)	**-**	**2008**
Jagannath University (Jaipur)	**-**	**2008**
Jagannath University (Bahadurgarh)	**-**	**2013**

And more dreams to come!

Editorial Office & Subscriber Service
JIMS Engineering & Management Technical Campus
48/4, Knowledge Park-III, Greater Noida, U.P. Phone #-01203819700,
lawjournal.gn@jagannath.org

From the desk of the Chief Editor

The rapid evolution of technology and digital communication has profoundly impacted legal frameworks across the world. From the influence of social media evidence in international courts to the challenges posed by artificial intelligence, the legal landscape is undergoing a transformative shift. In this issue, we present a collection of scholarly articles that critically examine these evolving dynamics and their implications for law, justice, and society.

An article titled *"From Tweets to Trials: How Social Media Evidence is Shaping International Legal Proceedings"* explores how social media evidence is shaping international legal proceedings, shedding light on the role of digital footprints in contemporary litigation.

Another offers an insightful analysis of India's *Bhartiya Sakshya Adhiniyam, 2023*, and its paradigm shift in embracing digital evidence.

In the realm of cyber law, a paper titled *"A Theoretical Analysis of Cyber Law for Women and Children in India"* provides a theoretical framework for understanding the legal protections available to women and children in India.

The paper on *"Artificial Intelligence: Examining the Benefits and Risks of AI in the Age of Social Media and its Legal Implications in India"* sheds light on the dual-edged sword of AI technologies.
The growing menace of deepfake technology and its impact on intellectual property rights is also analyzed in the paper titled *"Deepfakes and the Erosion of IP Rights: Legal Frameworks and Remedies"*, discussing existing legal frameworks and possible remedies.

Lastly, a paper titled *"Admissibility of Digital Evidence: Challenges and Perspectives in the Era of New Criminal Laws"* delves into the admissibility of digital evidence under new criminal laws, addressing the challenges and perspectives that shape modern legal proceedings.

This issue seeks to provide a thought-provoking discourse on the intersection of law and technology, offering valuable insights for legal practitioners, academics, and policymakers. I hope this compilation serves as a meaningful contribution to the ongoing dialogue on law and technology and inspires further research in this ever-evolving field. I am grateful to the authors for their insightful contributions and to our readers for their ongoing support of the journal.

Sincerely,

Prof. (Dr.) Pallavi Gupta
Thanking You

Table of Contents

FROM TWEETS TO TRIALS: HOW SOCIAL MEDIA EVIDENCE IS SHAPING INTERNATIONAL LEGAL PROCEEDINGS

Junaid Sattar
Master of Laws, AHC Member AJ&K Bar Council Muzaffarabad
Pakistan Occupied Jammu & Kashmir, Pakistan

Dr. Dalia Kadry Ahmed Abdelaziz
Assistant Professor of Criminal Law, Prince Sultan University, Saudi Arabia

ABSTRACT

The growing influence of social media on global communication has transformed the landscape of legal proceedings, particularly in relation to the role of social media evidence in international law. Platforms such as Twitter, Facebook, and Instagram have become powerful tools for both personal expression and international discourse, leaving behind a digital footprint that is increasingly being scrutinized in legal contexts. As social media content often holds critical value in criminal investigations, civil disputes, and human rights cases, its relevance in international legal proceedings cannot be understated (Butt, J. 2024a)[1]. However, significant challenges persist regarding the authenticity, admissibility, and ethical considerations of social media evidence in cross-border legal contexts. Despite its pervasive use, there remains a lack of uniformity in the ways courts and legal systems worldwide address social media data. This study aims to examine the evolving role of social media as evidence in international legal proceedings, focusing on the implications of its use for establishing truth, fairness, and justice. It addresses the gaps in current legal frameworks, especially the discrepancies in how different jurisdictions interpret and regulate the use of social media content in courts. The research employs a comparative legal analysis methodology, reviewing case studies from various countries that have integrated social media evidence into their legal proceedings. This includes examining the procedural rules, evidentiary standards, and the technical challenges associated with handling social media data in cross-border litigation. The findings reveal that while social media evidence is becoming more widely accepted, there are inconsistencies in its treatment across jurisdictions, primarily due to differences in digital forensics protocols, data privacy laws, and the evolving nature of social media platforms. International conventions and treaties have yet to establish a cohesive framework for the handling of social media evidence, leaving room for ambiguity in its legal implications. Moreover, ethical concerns regarding privacy, consent, and data manipulation continue to pose significant challenges for its use in courts. This study highlights the need for a standardized, global approach to handling social media evidence in international legal proceedings. It suggests that the legal community must develop clear guidelines and international treaties to ensure the ethical and consistent use of such evidence, while safeguarding fundamental rights such as privacy and freedom of expression. The results of this study have significant implications for the future of digital evidence law and the intersection of technology and international legal systems.

Key words: *Social Media Evidence, Digital Forensics, Cross-Border Legal Proceedings, International Law, Privacy Concerns, Legal Frameworks, Ethical Implications*

Introduction: Social Media's Legal Footprint

The digital age has revolutionized communication, transforming how individuals, organizations, and governments interact on a global scale (Yuan, Y. P., et. al., 2023)[2]. Social media platforms such as Twitter, Facebook, and Instagram have emerged as ubiquitous tools for personal expression and international discourse, bridging geographical divides and facilitating real-time communication. However, these platforms also generate vast digital footprints, leaving behind a repository of data that increasingly influences various facets of societal and legal frameworks. In the realm of international law, social media has evolved into a crucial source of

[1] Butt, J. (2024a). Data, Privacy, and the Law: Safeguarding Rights in the New Millennium. Paper presented during the 19th International Conference on European Integration - Realities and Perspectives (EIRP), Danubius International Conferences, 19(1), PP. 09–18 Retrieved from https://dp.univ-danubius.ro/index.php/EIRP/article/view/488/358 15 January, 2025.

[2] Yuan, Y. P., Dwivedi, Y. K., Tan, G. W. H., Cham, T. H., Ooi, K. B., Aw, E. C. X., & Currie, W. (2023). Government digital transformation: Understanding the role of government social media. Government Information Quarterly, 40(1), 101775. https://doi.org/10.1016/j.giq.2022.101775 15 January, 2025.

evidence, reshaping legal investigations and judicial proceedings (Hamilton, R. J. 2020)[3]. From geopolitical conflicts to transnational crimes, social media platforms now play a pivotal role in uncovering the truth and securing justice. Notable cases highlight the growing reliance on posts, videos, and interactions from these platforms to establish timelines, authenticate claims, and analyze intent. This paper explores the transformative impact of social media evidence on international legal proceedings, with an emphasis on its potential to redefine traditional legal processes. A significant body of research underscores the importance of integrating digital tools into governance and legal frameworks. For instance, (Butt, J. & Ahmed Abdelaziz. 2025)[4] highlight how digital innovation has enhanced governance systems, providing new avenues for transparency and accountability. Their studies demonstrate the broader implications of digitalization, including its role in legal mechanisms and decision-making processes. Similarly, (Butt, J. 2024b)[5] explores the intersection of digital communication and child protection in Nordic nations, shedding light on the legal challenges posed by misinformation and disinformation in the digital landscape. These findings align with the current discussion on social media evidence, as they highlight the increasing complexity and significance of digital data in legal contexts. The reliance on platforms like Twitter, Facebook, and Instagram in international legal proceedings is not without challenges. Issues such as data authenticity, privacy concerns, and jurisdictional conflicts raise critical questions about the admissibility and ethical use of social media evidence (Legros, O. 2024)[6]. Moreover, the evolving nature of digital platforms demands adaptive legal frameworks that can effectively address these complexities. As international legal systems navigate these uncharted territories, the integration of social media evidence marks a paradigm shift that underscores the intersection of technology, law, and human rights. This paper examines the role of social media in shaping international legal proceedings, focusing on its utility as evidence in trials and its broader implications for justice and accountability. By analyzing relevant case studies, legal frameworks, and academic perspectives, this study aims to provide a comprehensive understanding of how social media is redefining the boundaries of evidence and justice in the digital era.

The Rise of Social Media Evidence in International Law

The advent of social media has revolutionized how individuals and organizations communicate, creating a new frontier for criminal investigations, civil disputes, and human rights advocacy. Social media platforms such as Twitter, Facebook, and Instagram are not merely tools for personal expression but have also emerged as critical sources of digital evidence in international legal proceedings. Social media evidence has proven instrumental in high-profile international cases, where it has been leveraged to uncover the truth and achieve justice. For example, real-time posts, videos, and metadata have been utilized to document human rights violations, track the movements of individuals implicated in criminal activities, and resolve cross-border disputes. These digital footprints serve as a new class of evidence that reflects the evolving intersection of technology and law. The significance of social media evidence is particularly evident in cases involving human rights abuses, where individuals' posts can provide direct, unfiltered accounts of events that would otherwise remain undocumented. In this context, the procedural and ethical challenges surrounding the use of such evidence are immense. Questions of authenticity, data manipulation, and privacy violations frequently arise, as highlighted by (Butt, J. 2024c)[7] in his study of misinformation and disinformation in Nordic nations. Similarly, the implications of social media evidence extend beyond national borders, often requiring international collaboration to ensure its

[3] Hamilton, R. J. (2020). Social media platforms in international criminal investigations. Case Western Reserve Journal of International Law, 52, 213. Available at: https://scholarlycommons.law.case.edu/jil/vol52/iss1/12 15 January, 2025.

[4] Butt, J., & Abdelaziz, D. K. A. (2025). Sustainable governance in the digital age: E-government innovations for climate action. Journal of Recycling Economy & Sustainability Policy, 4(1), 54–69. Retrieved from https://respjournal.com/index.php/pub/article/view/58 15 January, 2025.

[5] Butt, J. (2024b). Evaluating legal measures, international conventions, and collaborative strategies to enhance child protection from misinformation and disinformation in the digital communication landscape of Nordic nations. Acta Universitatis Danubius. Communicatio, 18(1), 51–77. https://dj.univ-danubius.ro/index.php/AUDC/article/view/3147 15 January, 2025.

[6] Legros, O. (2024, January 23). The role of social media in legal proceedings. Minnesota Inventors. https://www.minnesotainventors.org/the-role-of-social-media-in-legal-proceedings/ 15 January, 2025.

[7] Butt, J. (2024c). Evaluating legal measures, international conventions, and collaborative strategies to enhance child protection from misinformation and disinformation in the digital communication landscape of Nordic nations. Acta Universitatis Danubius. Communicatio, 18(1), 51–77. https://dj.univ-danubius.ro/index.php/AUDC/article/view/3147 15 January, 2025.

admissibility and reliability in legal proceedings. The comparative study of Nordic and European economic sectors by (Butt, J. & Kousar, F. 2024)[8] demonstrates the complexity of integrating digital innovations across jurisdictions, providing a framework for understanding the challenges of harmonizing social media evidence standards globally. Despite its increasing relevance, the integration of social media evidence into international law is marked by inconsistencies. Differences in digital forensics protocols, data protection regulations, and evidentiary standards across jurisdictions pose significant hurdles. Furthermore, international conventions and treaties have yet to develop a cohesive framework for addressing the legal implications of social media content. Ethical concerns, particularly regarding user consent and the manipulation of online narratives, further complicate the use of this evidence.

Scope of Social Media Evidence in Legal Proceedings

The pervasive use of social media platforms like Twitter, Facebook, and Instagram has introduced a new dimension to legal proceedings, where digital footprints left by users can serve as crucial evidence. Social media content has found significant application in criminal investigations, human rights advocacy, and civil disputes, transforming how cases are built and adjudicated. In criminal investigations, social media evidence such as posts, geotags, and direct messages often provides leads or corroborates testimonies, as seen in cases involving cybercrime (Abdelaziz, D. K. A. 2025)[9], terrorism, and organized crime. For instance, authorities have successfully used social media posts to trace the activities of criminal networks or establish the whereabouts of suspects at specific times. In human rights cases, platforms have served as vital tools for documenting violations and amplifying voices from marginalized communities. Examples include the use of real-time videos and posts during conflicts to highlight war crimes and atrocities, subsequently presented in international courts to establish accountability. Similarly, in civil disputes such as defamation or custody battles, social media interactions have been leveraged to demonstrate intent, behavior patterns, or relationships, shaping outcomes significantly. A notable example is the case (Monica Lewinsky 1998)[10], where social media posts were instrumental in proving critical claims. Despite its transformative potential, the use of social media evidence also introduces challenges. Variations in the treatment of such evidence across jurisdictions, coupled with questions of authenticity, consent, and ethical use, complicate its integration into legal proceedings. While real-world cases highlight its value, these challenges underscore the pressing need for standardized legal frameworks to ensure the consistent, fair, and ethical application of social media evidence in international courts. The growing reliance on such evidence marks a paradigm shift in legal practice, emphasizing the critical role of digital footprints in uncovering truth and delivering justice.

Case Studies: Social Media in Courtrooms

The scope of social media evidence in legal proceedings has expanded significantly as courts grapple with the challenges of authentication, relevance, and admissibility. In *Moroccanoil v. Marc Anthony Cosmetics*[11], a federal district court ruled Facebook screenshots inadmissible due to insufficient circumstantial information to authenticate them, following the precedent set in *Internet Specialties W., Inc. v. ISPWest*[12]. Similarly, in *State of Connecticut v. Eleck*[13], Facebook comments purportedly authored by a witness were excluded when the witness claimed her account had been hacked, emphasizing the need for proof of authorship under Federal Rule of

---

[8] Butt, J., & Kousar, F. (2024). Harnessing Offshore Wind for Sustainable Economic Growth in Nordic Countries: Legal Innovations, Economic Opportunities, SDG and Policy Integration. Acta Universitatis Danubius. Œconomica, 20(2), 123–145. Published 30-04-2024 https://dj.univ-danubius.ro/index.php/AUDOE/article/view/2802 15 January, 2025.

[9] Abdelaziz, D. K. A. . (2025). Between Justice and Hidden Intent: Proving Hate Crimes in Comparative Law . Journal of Ecohumanism, 3(8), 10376 –. https://doi.org/10.62754/joe.v3i8.5648 15 January, 2025.

[10] Katyal, N. K. (2000). The public and private lives of presidents. William & Mary Bill of Rights Journal, 9(1), 1-51. Georgetown University Law Center. Retrieved from https://scholarship.law.georgetown.edu/facpub/1120 15 January, 2025.

[11] Moroccanoil, Inc. v. Marc Anthony Cosmetics, Inc. (2023). Casetext. https://casetext.com/case/moroccanoil-inc-v-marc-anthony-cosmetics-inc 16 January, 2025.

[12] Internet Specialties West Inc. v. Ispwest et al. (2005). Justia Dockets & Filings. https://dockets.justia.com/docket/california/cacdce/2:2005cv03296/173552 16 January, 2025.

[13] State of Connecticut v. Eleck. (2014). vLex. https://case-law.vlex.com/vid/state-v-eleck-no-891644252 16 January, 2025.

Evidence 901. Authentication challenges were also central in *United States v. Vayner*[14], where the Second Circuit excluded a VK.com profile as evidence, ruling that no sufficient basis was provided to link the page to the defendant beyond speculation. In *Espinoza v. State of Texas*[15] Myspace photos were admitted despite the defense's objections regarding their authenticity because additional compelling evidence supported the prosecution's case. In contrast, in *Tienda v. State of Texas*[16], Myspace content was deemed admissible due to the cumulative circumstantial evidence linking it to the defendant. Courts have also scrutinized requests for broad access to social media accounts.

For instance, in *Thompson v. Autoliv ASP, Inc.*[17], the court rejected a defense request for an exhaustive review of the plaintiff's Facebook page, citing privacy concerns. Similarly, in *Tompkins v. Detroit Airport*[18], a request for unrestricted access to a plaintiff's Facebook account was denied as overly broad, though targeted production of relevant materials was permitted. Further, in *Richards v. Hertz*[19], the court allowed selective access to social media evidence, ordering the plaintiff to turn over specific Facebook photos that contradicted claims of injury. The Stored Communications Act (SCA) also came into play in *Flagg v. City of Detroit*[20], where the court allowed discovery of text messages stored by a third-party service provider under a controlled protocol, highlighting the balance between evidence relevance and privacy. The scope of social media evidence in legal proceedings has rapidly expanded, as digital footprints increasingly play a significant role in both criminal and civil cases. Social media platforms such as Facebook, Twitter, and Instagram have become crucial sources for evidence, whether it's for proving statements made by individuals, uncovering hidden facts, or validating alibis. A key case in this area is *Bland v. Roberts*[21], where employees of a Sheriff's Department were fired for "liking" a political opponent's page on Facebook. They argued that their firing violated their First Amendment rights. Initially, the trial court ruled that "liking" something on Facebook did not amount to "speech," but the Fourth Circuit Court of Appeals reversed this decision. The court determined that a "like" on Facebook is a form of speech and is constitutionally protected, comparing it to public displays like holding a placard or verbal expression. This case highlighted the importance of social media as a form of expression that courts must now consider as protected speech under the First Amendment. In another case, *Munster v. Groce*[22], the court emphasized the necessity of using social media and online resources in legal proceedings. The plaintiff failed to perform a basic Google search to locate a defendant, which the court found surprising, as a simple search would have revealed important information about the defendant's whereabouts, such as an obituary listing relatives. This case underscored the growing importance of using digital tools like social media in legal discovery, with the court implying that failure to do so may constitute negligence on the part of legal professionals. Additionally, in *Lester v. Allied Concrete Co*[23].Social media evidence played a pivotal role in a civil suit following a tragic accident. Isaiah Lester filed a lawsuit seeking compensation after a truck accident killed his wife. However, during the discovery process, Lester's Facebook page was subpoenaed. The plaintiff's attorney advised Lester to delete certain photos from his profile, which the court later ruled as spoliation of evidence. The deletion of these photos led to sanctions against both Lester and his attorney, including an adverse-inference instruction to the jury and substantial financial penalties.

---

[14] United States v. Vayner. (2014). Casetext. https://casetext.com/case/united-states-v-vayner-1 16 January, 2025.

[15] Espinoza v. State. (2012). Court of Appeals of Texas, Amarillo. https://caselaw.findlaw.com/court/tx-court-of-appeals/1607757.html 16 January, 2025.

[16] Tienda v. State. (2012). Casetext. https://casetext.com/case/tienda-v-state-10 16 January, 2025.

[17] Thompson v. Autoliv ASP, Inc. (2012). Casetext. https://casetext.com/case/thompson-v-autoliv-asp-3 16 January, 2025.

[18] Tompkins v. Detroit Metro. Airport. (2012). Casetext. https://casetext.com/case/tompkins-v-detroit-metro-airport#:~:text=This%20is%20a%20 slip%2d And,work%20and%20to%20enjoy%20life 16 January, 2025.

[19] Bosco Legal Services. (2020). Richards v. Hertz: The court allowed selective access to social media evidence. Bosco Legal. https://www.boscolegal.org/blog/richards-hertz-corp-privacy-settings-social-media-investigations/ 16 January, 2025.

[20] Flagg v. City of Detroit. Casetext. https://casetext.com/case/flagg-v-city-of-detroit-10 16 January, 2025.

[21] Bland v. Roberts. (2013). U.S. Court of Appeals for the Fourth Circuit. https://law.justia.com/cases/federal/appellate-courts/ca4/12-1671/12-1671-2013-09-18.html 16 January, 2025.

[22] Munster v. Groce. (2005). Casetext. https://casetext.com/case/munster-v-groce 16 January, 2025.

[23] Lester v. Allied Concrete Co. (2013). Ediscoverylaw.com. https://www.ediscoverylaw.com/wp-content/uploads/2013/11/Lester-v-Allied-Concrete-Final-Order.pdf 16 January, 2025.

In *Pătraşcu v. Romania*[24], the European Court of Human Rights ruled that holding a Facebook user liable for third-party comments on their page violated their freedom of expression. Alexandru Pătrașcu, a blogger covering a scandal at the Bucharest National Opera, was held responsible for defamatory comments posted by others. The Court emphasized that social media users should not be liable for third-party comments without clear legal standards, fearing that such liability could lead to excessive self-censorship. This decision counters previous rulings, such as *Delfi AS v. Estonia*[25], where the Court held media platforms accountable for user comments, but it leaves important questions about the application of these standards unanswered. The case illustrated the legal risks associated with mishandling or tampering with social media evidence, especially when it pertains to ongoing litigation. These cases collectively illustrate the evolving role of social media evidence in legal proceedings, highlighting both its potential to influence legal outcomes and the ethical and procedural challenges it presents. As social media continues to shape modern communication, it is crucial for legal systems worldwide to develop clear guidelines and frameworks to handle such evidence effectively and ethically in the courtroom.

Challenges in Admissibility and Authenticity

In the context of using social media as evidence in international legal proceedings, determining the authenticity and admissibility of digital content presents significant challenges (Bharati, R. K. et. al., 2024)[26]. One of the primary concerns is verifying the authenticity of social media evidence, as the digital nature of these platforms allows for the easy manipulation of content. Courts often struggle to establish the validity of social media content, particularly when the data is presented without adequate supporting evidence such as metadata or verified sources (Gruce, J. (2024)[27]. The lack of standardized methods for authenticating social media content across jurisdictions exacerbates these issues, making it difficult for courts to consistently determine whether such evidence is reliable and can be trusted in the legal context. Admissibility, too, varies widely across jurisdictions. Different legal systems have distinct standards for accepting digital evidence, and this divergence often leads to complications in international cases (Aleke, N. T., & Trigui, M. 2025)[28]. Some jurisdictions have comprehensive frameworks for handling digital evidence, while others lack clear guidelines or procedures, resulting in inconsistencies in how social media content is treated in court. Procedural issues like metadata validation and the chain of custody are critical in this regard. Without proper validation of metadata or clear documentation of how the evidence was collected, stored, and transferred, the integrity of social media evidence can be easily questioned. This lack of uniformity in legal standards further complicates the use of social media evidence in cross-border litigation. Ethical concerns surrounding social media evidence also play a central role in its admissibility. Issues related to privacy, consent, and the potential for data manipulation often clash with the need for transparency and accountability in legal proceedings. In particular, the balance between using social media as a tool for truth-seeking and protecting individuals' privacy rights remains an ongoing challenge. Courts must navigate these concerns to ensure that evidence is obtained and used ethically, without violating fundamental rights such as privacy and freedom of expression (Bychawska-Siniarska, D. 2017)[29]. These complexities highlight the need for clearer and more consistent international guidelines to address the authenticity, admissibility, and ethical use of social media evidence in legal proceedings, ensuring that such evidence serves the interests of justice while respecting individual rights.

---

[24] Pătrașcu v. Romania. (2018). European Court of Human Rights. https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-171088&filename=CASE%20OF%20P%C4%82TRA%C5%9ECU%20v.%20ROMANIA.docx&logEvent=False 16 January, 2025.

[25] European Court of Human Rights. (2015). CASE OF DELFI AS v. ESTONIA (Application no. 64569/09). European Court of Human Rights. https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22001-155105%22]%7D 16 January, 2025.

[26] Bharati, R. K., Khodke, P. G., Khadilkar, C. P., & Bawiskar, S. K. (2024). Forensic bytes: Admissibility and challenges of digital evidence in legal proceedings. International Journal of Scientific Research in Science and Technology, 11(16), 24-35. https://ijsrst.com/paper/12484.pdf 16 January, 2025.

[27] Gruce, J. (2024). Social media and the court: Exploring impacts, challenges, and legal considerations in the digital age. University Honors College, (32). https://scholars.indianastate.edu/honorsp/32 16 January, 2025.

[28] Aleke, N. T., & Trigui, M. (2025). Legal and ethical challenges in digital forensics investigations. In Digital forensics in the age of AI (pp. 1-30). IGI Global. https://doi.org/10.4018/979-8-3373-0857-9.ch006 16 January, 2025.

[29] Bychawska-Siniarska, D. (2017). Protecting the right to freedom of expression under the European Convention on Human Rights: A handbook for legal practitioners. Exergue. https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814 16 January, 2025.

Ethical Considerations in Cross-Border Cases

In cross-border legal proceedings, the ethical challenges of using social media as evidence are becoming increasingly complex, especially in relation to privacy, consent, and data manipulation. Social media platforms, such as Twitter, Facebook, and Instagram, have become essential for modern communication, which has led to the blurring of the line between public and private information. This raises significant privacy concerns when social media content is utilized as evidence, particularly when the data originates from users who may not have given consent for their posts to be used in legal contexts. The issue of consent is further complicated in cross-jurisdictional cases, where differing data privacy laws across regions come into play. For example, the European Union's General Data Protection Regulation (GDPR) provides robust protections for personal data (Butt, J. 2024d)[30], but other regions may not have similar safeguards, which heightens the risk of infringing on users' privacy and freedom of expression.

Additionally, the ethical dilemmas surrounding social media evidence are exacerbated by the potential for surveillance and data manipulation. Social media content can be easily altered, edited, or misrepresented, which poses significant risks to the integrity of evidence presented in court (The Dorward Law Firm. 2024)[31]. In cross-border cases, where platforms may be governed by varying laws and regulations, it becomes difficult to verify the authenticity of social media evidence. The lack of uniformity in digital forensics practices across jurisdictions increases the likelihood of data manipulation or misinterpretation, undermining the fairness of legal proceedings (Allah Rakha, N. 2024)[32]. Surveillance methods further complicate matters, particularly when social media content is gathered without proper consent or in violation of privacy laws. These practices not only undermine the reliability of evidence but also threaten the fundamental rights of individuals involved in legal processes. As social media increasingly influences international legal proceedings, it is essential to address these ethical concerns in a manner that ensures the fair and responsible use of digital data. Establishing clear international guidelines for consent, data privacy, and surveillance practices is crucial for safeguarding justice and protecting individuals' rights in cross-border cases (Islam, M. T. 2022)[33]. A standardized global approach to the ethical management of social media evidence would help mitigate the risks of data manipulation, protect privacy, and preserve the integrity of legal processes on a global scale.

Comparative Legal Analysis Across Jurisdictions

The use of social media evidence in international legal proceedings is governed by varying legal standards and frameworks across jurisdictions (Basu, S. 2024)[34]. While platforms like Twitter, Facebook, and Instagram have become central to both individual expression and public discourse, their integration into legal processes presents substantial challenges due to the lack of uniformity in how different legal systems treat digital content. In jurisdictions like the United States, social media evidence is increasingly accepted, with courts applying conventional evidentiary standards such as relevance (Wang, X., et. al., 2024)[35], authenticity, and hearsay rules to assess the admissibility of digital content. However, in countries like the European Union, strict data privacy laws such as the (GDPR) impose significant restrictions on the collection and use of personal data, including social media posts, creating a clear tension between the need for evidence and the protection of individual privacy

---

[30] Butt, J. (2024d). The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?. Acta Universitatis Danubius. Juridica, 20(2), 7–52. https://dj.univ-danubius.ro/index.php/AUDJ/article/view/2788 16 January, 2025.

[31] The Dorward Law Firm. (2024, October 31). How social media impacts criminal cases. The Dorward Law Firm Blog. https://www.thedorwardlawfirm.com/blog/2024/october/how-social-media-impacts-criminal-cases/ 17 January, 2025.

[32] Allah Rakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review, 16(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892 17 January, 2025.

[33] Islam, M. T. (2022). A brief introduction to the right to privacy – an international legal perspective. NYU Law Globalex. Retrieved from https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html 17 January, 2025.

[34] Basu, S. (2024). Social media on trial: Can the law keep up with the times? De Penning & De Penning. Retrieved from https://www.lexology.com/library/detail.aspx?g=00a6d94b-7343-47f0-b055-17a15d62a919 17 January, 2025.

[35] Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: Exploring its evidentiary significance and procedural implications in U.S. judicial processes. Frontiers in Blockchain, 7, Article 1306058. https://doi.org/10.3389/fbloc.2024.1306058 17 January, 2025.

rights. This disparity complicates cross-border litigation, as legal practitioners and courts must navigate different thresholds for evidence acceptance and privacy protection.

A notable example of these differences can be seen in the United States versus the EU approach to data privacy and social media evidence. In the U.S., courts often prioritize the evidentiary value of social media content, allowing its use to establish facts in both criminal and civil cases. However, in the EU, the GDPR's stringent rules on data access and processing restrict how data from social media platforms can be obtained and used in legal proceedings (European Union. 2024)[36]. These regulations necessitate additional steps, including obtaining consent from data owners or ensuring that the use of such data aligns with the principles of data minimization and purpose limitation. Discrepancies in digital forensic protocols also play a significant role in shaping how social media evidence is treated (Dunsin, D., et. al., 2024)[37]. Different jurisdictions have developed varying methodologies for authenticating and preserving digital evidence, creating a lack of consistency in how social media data is handled during legal proceedings. For example, while the U.S. has well-established forensic procedures for extracting and verifying digital content, some countries, particularly in the Global South, face challenges due to limited access to advanced forensic tools and expertise (Goodison, S. E., et. al., 2015)[38]. This gap can result in the use of unverified or improperly handled evidence, undermining its integrity in international litigation. Furthermore, case studies from countries such as Brazil and India illustrate the complexities of integrating social media evidence in different legal systems. In Brazil, the courts have started to embrace social media evidence in cases ranging from defamation to electoral fraud, but there remains uncertainty over how to handle data privacy issues and the scope of consent required for its use. In contrast, India's judicial system has faced hurdles in reconciling the increasing use of social media content with the need to respect privacy rights, often leading to lengthy legal debates on whether digital evidence was obtained through legitimate means. These disparities in legal protocols highlight the need for clearer procedural rules and evidentiary standards in handling social media evidence across borders. A lack of cohesive international conventions governing the collection, use, and admissibility of social media content contributes to the challenges in cross-border litigation. Differences in technical capabilities, such as the availability of digital forensic tools and expertise, further exacerbate these challenges, creating an environment where the application of social media evidence may vary significantly depending on the jurisdiction. In light of these discrepancies, there is an urgent need for a global approach to the use of social media evidence in legal proceedings (Silver, L. A. 2020)[39]. Establishing standardized protocols for data authentication, cross-border data transfer, and privacy protection would not only enhance fairness and consistency in international legal processes but also safeguard individuals' fundamental rights. This comparative analysis underscores the importance of international cooperation and the creation of unified frameworks that address the evolving nature of social media and digital forensics in the context of international law.

International Treaties and the Need for Standardization

The growing reliance on social media evidence in international legal proceedings underscores a critical gap in the global legal framework (Amoo, O. O. et. al., 2024)[40]. Despite the widespread use of platforms such as Twitter, Facebook, and Instagram in criminal investigations, civil disputes, and human rights cases, there is no universally accepted standard for handling and interpreting social media content in courtrooms. This lack of global standards leads to inconsistencies in the admissibility, authenticity, and use of digital evidence across

[36] European Union. (2024). Data protection under GDPR. You're Europe. Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm 17 January, 2025.

[37] Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation, 48, Article 301675. https://doi.org/10.1016/j.fsidi.2023.301675 17 January, 2025.

[38] Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence. RAND Corporation. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf 17 January, 2025.

[39] Silver, L. A. (2020). The unclear picture of social media evidence. Manitoba Law Journal, 43(3), 111. Retrieved from https://canlii.ca/t/sxm6 17 January, 2025.

[40] Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205–217. Retrieved from https://doi.org/10.30574/wjarr.2024.21.2.0438 18 January, 2025.

jurisdictions. Different countries have varying procedural rules, evidentiary standards, and technical protocols for dealing with social media data, resulting in significant ambiguity (Digital Wellbeing Organisation. 2021)[41]. This fragmentation is further exacerbated by the absence of cohesive international conventions or treaties specifically addressing social media evidence. While international law has evolved to handle traditional forms of evidence, social media content presents unique challenges that current treaties and conventions fail to address adequately. For example, discrepancies in data privacy laws, differing approaches to digital forensics, and the evolving nature of social media platforms make it difficult to establish a uniform framework for cross-border legal proceedings. Without such a framework, courts are often left to navigate these challenges on a case-by-case basis, leading to uneven legal outcomes. Moreover, ethical issues surrounding privacy, consent, and data manipulation remain largely unregulated, raising questions about the protection of fundamental rights such as privacy and freedom of expression. To address these gaps, it is essential that international legal bodies develop standardized frameworks for handling social media evidence in legal proceedings. Clear guidelines, supported by international treaties, would ensure a more consistent and fair approach to the use of social media content in courts (United Nations Office on Drugs and Crime. 2018)[42]. These frameworks should balance the need for technological advancement with the protection of individuals' rights, ensuring that social media evidence is used ethically and in accordance with international human rights standards. Establishing such a cohesive global framework would not only streamline the handling of digital evidence but also promote fairness, transparency, and justice in international legal systems.

Implications for Truth, Fairness, and Justice

The increasing integration of social media evidence into international legal proceedings presents both significant opportunities and challenges in safeguarding fundamental rights, including privacy and freedom of expression. As platforms like Twitter, Facebook, and Instagram become key tools for legal investigations, the need for a balance between the use of digital footprints and the protection of individual rights becomes paramount (Bokolo, B. G., & Liu, Q. 2024)[43]. While social media can provide critical insights into criminal investigations, civil disputes, and human rights cases, it also raises serious concerns regarding data manipulation and consent violations. The potential for altering, fabricating, or misinterpreting social media content poses risks to the accuracy of legal outcomes, jeopardizing fairness in trials (The Dorward Law Firm. 2024)[44]. The use of social media as evidence must be approached with caution to prevent the infringement of privacy rights and the exploitation of personal data without consent. In many cases, individuals may unknowingly expose sensitive information, and this information can be misused in legal proceedings without proper safeguards. To ensure justice, legal systems must develop rigorous protocols to verify the authenticity of social media evidence and prevent data tampering. This includes establishing clear guidelines on obtaining consent for the use of social media data and ensuring that privacy protections are not undermined in the process.

Furthermore, social media evidence has the potential to uncover truth in ways that traditional forms of evidence may not (Epstein, Z., et. al., 2023)[45]. Posts, messages, and multimedia content can provide real-time, unfiltered insights into events, offering a fresh perspective in cases where other evidence may be unavailable or unreliable. In human rights cases, for instance, social media can act as a crucial tool for documenting violations and providing a voice to marginalized groups, ensuring that the pursuit of justice is not constrained by traditional barriers. However, the application of social media evidence in legal disputes also raises concerns about fairness.

---

[41] Digital Wellbeing Organisation. (2021). International regulation of social media. https://digitalwellbeing.org.au/wp-content/uploads/2021/12/International-Regulation-of-Social-Media.pdf 18 January, 2025.

[42] United Nations Office on Drugs and Crime (UNODC). (2018). Non-binding guidelines on the use of social media by judges. Retrieved from https://www.unodc.org/res/ji/import/international_standards/social_media_guidelines/social_media_guidelines_final.pdf 18 January, 2025.

[43] Bokolo, B. G., & Liu, Q. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. Electronics, 13(9), 1671. Retrieved from https://doi.org/10.3390/electronics13091671 18 January, 2025.

[44] The Dorward Law Firm. (2024, October 31). How social media impacts criminal cases. Retrieved from https://www.thedorwardlawfirm.com/blog/2024/october/how-social-media-impacts-criminal-cases/ 18 January, 2025.

[45] Epstein, Z., Sirlin, N., Arechar, A., Pennycook, G., & Rand, D. (2023). The social media context interferes with truth discernment. Science Advances, 9(9), eabo6169. Retrieved from https://doi.org/10.1126/sciadv.abo6169

Given the variations in how different jurisdictions regulate the admissibility of social media content, there is a risk that its use could be skewed by local legal standards or biases. Inconsistent practices across borders further complicate matters, as courts may not be equipped to handle the technical intricacies of social media data, leading to potential injustices in cross-jurisdictional cases. As technology continues to evolve, the role of digital evidence in international legal systems will expand, reshaping how justice is delivered (Barraclough, G. 2024)[46]. The rise of artificial intelligence, blockchain, and digital forensics will likely revolutionize how social media data is handled, authenticated, and analyzed. Yet, this transformation must be guided by strong ethical and legal frameworks to prevent abuses and to ensure that these advancements serve the broader goals of truth, fairness, and justice.

Findings

The analysis of social media evidence in international legal proceedings reveals several key findings that underscore both the transformative potential and the challenges it presents. First, while social media platforms such as Twitter, Facebook, and Instagram are increasingly recognized as valuable sources of evidence, the way in which social media content is treated varies significantly across jurisdictions. These platforms leave a digital trail that is crucial in criminal investigations, civil disputes, and human rights cases, but the lack of uniformity in legal frameworks creates inconsistencies in their admissibility and treatment in courts worldwide. One of the most notable findings is the variation in digital forensic practices and standards across different legal systems. In some countries, social media evidence is meticulously scrutinized through established forensic methods, while in others, such practices are still evolving. The lack of standardized protocols for verifying and handling social media data in legal contexts contributes to challenges in establishing authenticity, which is essential for ensuring the integrity of legal proceedings.

This paper also highlights the ongoing issues related to data privacy laws and the protection of individual rights in the context of social media evidence. While the use of social media content as evidence has grown, significant ethical concerns persist, particularly regarding consent, data manipulation, and the privacy of individuals. This raises important questions about the balance between the need for truth and the protection of fundamental rights such as privacy and freedom of expression. Furthermore, the study found that international conventions and treaties addressing digital evidence are insufficient in providing a cohesive and globally accepted framework for handling social media data in cross-border legal proceedings. The absence of clear, universally agreed-upon guidelines exacerbates the ambiguity surrounding the legal implications of using such evidence in court. Overall, the findings suggest that the legal community must adopt a more standardized, global approach to the use of social media evidence in international legal proceedings. There is an urgent need for international treaties and clearer legal guidelines to address the technical, ethical, and procedural challenges associated with social media data. This would ensure the consistent and fair use of digital evidence while safeguarding fundamental rights in the evolving landscape of international law.

Conclusion: Toward a Digital Evidence Future

Social media has undeniably transformed the landscape of international legal proceedings, offering both vast opportunities and complex challenges. As platforms like Twitter, Facebook, and Instagram continue to shape global communication, they leave behind digital footprints that increasingly serve as pivotal evidence in criminal, civil, and human rights cases. This manuscript has highlighted the growing importance of social media evidence in legal contexts, emphasizing its potential to uncover truth and promote justice. However, significant hurdles remain in the consistent and ethical integration of such evidence across borders, as discrepancies in legal frameworks, digital forensics protocols, and data privacy laws continue to hinder the global harmonization of social media evidence standards. To address these challenges, a collaborative, global approach is urgently needed. Legal systems worldwide must work together to establish clear, standardized guidelines for the handling

[46] Barraclough, G. (2024, November 12). The future of digital forensics: How technology is transforming investigations. TechUK. Retrieved from https://www.techuk.org/resource/the-future-of-digital-forensics-how-technology-is-transforming-investigations.html 18 January, 2025.

of social media evidence. This requires international treaties and frameworks that ensure the ethical use of social media content while protecting fundamental rights, such as privacy and freedom of expression. By fostering cross-jurisdictional cooperation, the legal community can navigate the complexities of digital forensics, address concerns about data manipulation, and uphold the integrity of international legal proceedings. The future of social media evidence in international law holds transformative potential, enabling a more dynamic and transparent approach to justice. However, without coordinated efforts to harmonize legal systems and develop a unified framework, the effective and ethical use of social media evidence may remain an elusive goal. The findings from this study underscore the need for continued dialogue and collaboration to shape the future of digital evidence law, ensuring that it aligns with the evolving nature of technology while safeguarding the principles of fairness, truth, and justice.

Future Directions: Bridging the Gaps

To effectively address the challenges posed by the use of social media evidence in international legal proceedings, it is essential to establish cohesive and standardized global frameworks. As the study indicates, the current lack of uniformity in how jurisdictions handle social media content leaves room for ambiguity and potential misuse, particularly when it comes to the authenticity, admissibility, and ethical considerations of such evidence (Butt, J. 2024a). One actionable step toward bridging these gaps is the development of international conventions or treaties that set clear standards for the handling of social media data. These frameworks should provide guidelines for the proper collection, verification, and presentation of digital evidence in courts, taking into account the diverse legal systems and cultural contexts that may affect the interpretation of social media content.

In addition to legal frameworks, it is crucial to balance technological advancements with ethical and legal principles. Social media platforms evolve rapidly, and the legal community must adapt by addressing concerns related to privacy, consent, and data manipulation. This requires careful consideration of fundamental rights, such as the protection of personal data and freedom of expression, while ensuring that digital evidence is used in a fair and transparent manner. Therefore, any global framework should include provisions to safeguard these rights and prevent the misuse of social media evidence for purposes that could undermine justice. Moreover, clear guidelines should be developed for the consistent and ethical use of social media evidence in courts. Legal professionals, including judges, prosecutors, and defense attorneys, must be educated on the unique challenges posed by digital evidence, particularly in cross-border cases where data privacy laws and digital forensics protocols may differ. Establishing these guidelines will help ensure that social media evidence is handled in a way that promotes fairness and justice, while avoiding potential biases or inconsistencies in its interpretation. Ultimately, the legal community must work together to create an environment where the use of social media evidence in international legal proceedings is both standardized and ethically sound. By developing clear frameworks and guidelines, it is possible to bridge the current gaps and ensure that social media evidence can be effectively integrated into legal systems without compromising fundamental rights or the integrity of the judicial process.

Limitation

While this study provides a comprehensive analysis of the role of social media evidence in international legal proceedings, there are several limitations to consider. First, the scope of this research is confined to the examination of case studies and legal frameworks within a select number of jurisdictions. As such, the findings may not fully represent the global landscape, particularly in countries with less-developed legal systems or those where the use of social media evidence is minimal. Second, due to the rapidly evolving nature of social media platforms, this study may not capture the most current developments in the digital forensics field or the latest changes in data privacy laws and regulations. Third, this research primarily focuses on the legal and procedural aspects of social media evidence, and does not delve deeply into the technological complexities involved in the collection, preservation, and analysis of social media data, which could provide additional insights into the practical challenges faced by legal practitioners. Additionally, the ethical concerns related to the use of social

media evidence, such as privacy and consent, are considered but not exhaustively addressed in terms of their long-term societal impact. Lastly, the lack of cohesive international treaties and conventions on this matter limits the scope of recommendations for global standardization, leaving significant room for further research and development in this area.

Authors Biography

Junaid Sattar Butt is an accomplished legal professional and researcher based in Lahore, Pakistan, with extensive experience in law and governance. Currently practicing as an Advocate at the High Court under the AJK Bar Council and serving as a Corporate Tax Practitioner under the Lahore Tax Bar Association, he has expertise spanning constitutional, international, and administrative law. Committed to advancing the protection of fundamental rights, his work involves research, settlements, arbitration, and court representation. He holds a Master of Laws (LL.M) with honors from the University of Lahore, specializing in International and Comparative Laws, alongside a Master of Arts in Political Science from the University of the Punjab. Additionally, he possesses a Bachelor of Laws (LL.B) and a Master's in Business Administration (Finance), reflecting his diverse knowledge base in both legal and business fields. In addition to his legal practice, he has taught International Law, Administrative Law, and Human Rights at various institutes. Actively engaged in academic and research circles, he has published extensively on topics related to law, digital governance, human rights, artificial intelligence, and sustainable development. As a passionate advocate for justice and human rights, he is dedicated to bridging the gap between theory and practice, focusing on the intersection of law, technology, and governance. His future vision is centered on advancing the rule of law, promoting sustainable governance, and contributing to global policy through ongoing research initiatives.

Dr. Dalia Kadry Ahmed Abdelaziz is an Assistant Professor of Criminal Law at Prince Sultan University, Saudi Arabia. She holds a Ph.D. in Criminal Law and has a strong academic and research background in the field of law. Dr. Dalia's research interests focus on various aspects of criminal law, with an emphasis on legal reforms and the intersection of law and society. She is an active contributor to academic discussions and has published works in her area of expertise.

TRANSFORMING JUSTICE: EMBRACING DIGITAL EVIDENCE AND THE PARADIGM SHIFT UNDER BHARATIYA SAKSHYA ADHINIYAM, 2023

Dr. Caesar Roy
Assistant Professor of Law, Surendranath Law College, University of Calcutta

ABSTRACT

In this era of digitalization we are not only experiencing e-governance but communication, education, e-commerce and other transactions are also carried on through online platforms. This technological growth and advancement also impacted on countries' legal systems affecting legal rules and regulations. In our day to day life while dealing with technology we face many odds which ultimately led to legal obligations due to this the importance of electronic records are felt necessary. A gap was observed between the present laws and growing societal complexity backed by technological use and abuse. Owing to this gap a need was felt to frame laws relating to information technology and also amend the rules of admissibility of evidence by including electronic evidence both in civil and criminal justice system. This necessitated the requirement to update the laws governing information technology and the criteria for the acceptance of digital evidence in both criminal and civil proceedings. Different sorts of evidence are now accepted by courts, reflecting the significant changes in the law of evidence in recent years. This development has also affected India, where the law has undergone several changes. In order to address this issue, the Information Technology Act of 2000 was passed and accordingly the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023 were passed and the Banker's Book Evidence Act of 1891 was amended. This article aims to examine and analyze the extent to which the Indian Judiciary has recognized and appreciated the admissibility and relevance of digital evidence, while also providing some suggestions for improvement.

Key words: *Electronic evidence, digital evidence, Evidence Act, Information Technology Act, 2000, relevancy, admissibility*

Introduction

In this 21st century we are a part and parcel of two parallel worlds one is the physical world and another is the virtual world. The use of information and communication technologies, such as computers, mobile phones, printers, digital cameras, etc., is essential to the virtual world. In contrast to the physical world, there are many possibilities for crimes like phishing, identity theft, child pornography, hacking, etc. to be committed in the virtual world. Electronic information often serves as evidence before the court and can be used to prove or disprove a fact or fact in issue. These electronic information or data are immensely important and valuable in the eyes of law especially during dispute or crime as because those electronic information or data related with any crime or illegal activity will gain the recognition as evidence in the court of law during court proceedings. Electronic records are volatile and fragile in nature and are easily alterable. Being intangible it is necessary to protect and preserve such electronic records or digital documents. Now whether these electronic records will further be rejected or accepted as a piece of evidence in the court of law depends upon the authenticity of the electronic evidence. These electronic records which are stored or transmitted digitally can be treated as electronic evidence or digital evidence.

“Electronic or Digital evidence” is one kind of piece of evidence produced by some mechanical or electronic means. Emails, text documents, spreadsheets, photos, graphics, database files, deleted files, data backups, and other types of files stored on floppy discs, zip discs, hard drives, tape drives, CD-ROMs, mobile phones, microfilm, pen drives, and other devices are included but not limited to. The Indian Evidence Act, 1872 did not contain any particular provisions acknowledging the admissibility and relevance of digital evidence until 2000. In order to address this issue, the Information Technology Act of 2000 was passed. Accordingly, the Banker's Book Evidence Act of 1891 and Indian Evidence Act, 1872 were amended. Later, the Information Technology Act was amended and the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023 were passed primarily to recognise transactions made using

Electronic Data Interchange (i.e., computer-to-computer communication) and other types of communication.

Meaning of Digital Evidence

Evidence is something which tends to prove or disprove an fact or conclusion. Evidence in ordinary speech is the means by which something is proved or disproved. According to Black Law Dictionary evidence means something (including testimony. documents, and tangible objects) that tends to prove or disprove the existence of an alleged fact; anything presented to the senses and offered to prove the existence or nonexistence of a fact[1]. According to Blackstone evidence signifies that which demonstrates, makes clear or ascertains the truth of the very fact or point in issues, either on the one side or on the other[2]. According to Halsbury, evidence is the usual means of proving or disproving a fact or matter in issue. The law of evidence indicates what may properly be introduced by a party and also what standard of proof is necessary[3].

According to Bharatiya Sakshya Adhiniyam, 2023, "Evidence" means and includes (i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence[4]. So the word "evidence" in the Act signifies only the instruments by means of which relevant facts are brought before the court. The instruments adopted for this purpose are witnesses and documents. The term "Evidence" as defined in the Act is by no means exhaustive. The word 'evidence' connotes the instruments by which relevant facts are brought before the court so that it can come to a right decision[5].

According to Black Law Dictionary computer-generated evidence means evidence created by using a computer to provide a re-creation, simulation, or reconstruction of an event (usu. a crime scene or accident), esp. as it may be used as substantive evidence or as demonstrative evidence. To be introduced as substantive evidence, it must be relevant, sufficiently reliable, and probative to a degree that outweighs the danger of unfair prejudice. As demonstrative evidence, it need only be helpful to understanding a witness's testimony and not be based on erroneous or misleading information[6].

According to Black Law Dictionary, digital evidence means any probative information that has been produced, stored, or transmitted in electronic form and might be usable at trial. It is also termed electronic evidence[7].

Before passing Bharatiya Sakshya Adhiniyam, 2023, the Indian Evidence Act, 1872 was amended by virtue of Section 92 of Information Technology Act, 2000 (Before amendment). Section 3 of the Indian Evidence Act, 1872 was amended and the phrase *"All documents produced for the inspection of the Court" was substituted by "All documents including electronic records produced for the inspection of the Court"*.

According to IT Act, 2000, "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche[8]. "Electronic form" with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device[9]. "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or

---

[1] Garner, B. A. (2019). Black's Law Dictionary (11th ed.). Minnesota: Thomson Reuters.

[2] Singhal M.L & Chitaley (2000). The Indian Evidence Act. Nagpur: All India Reporter Pvt. Ltd.

[3] *Ibid*, p. 38

[4] Section 2(1)(e), Bharatiya Sakshya Adhiniyam, 2023

[5] Sengupta S.P (1988). Law of Evidence. Calcutta: Kamal Law House

[6] Garner, B. A. (2019). Black's Law Dictionary (11th ed.). Minnesota: Thomson Reuters

[7] Ibid.

[8] 2(t) of Information Technology Act, 2000

[9] 2(r) of Information Technology Act, 2000

computer generated micro fiche[10].

As per the Explanation to Section 79A of the IT Act, "electronic form of evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines. Courts can thus permit the use of digital evidence such as e-mails, digital photographs, word processing documents, instant message histories, spreadsheets, internet browser histories, databases, contents of computer memory, computer backup, secured electronic records and secured electronic signatures, Global Positioning System tracks, Logs from a hotel's electronic door, Digital video or audio etc., during the course of trials of a civil or criminal case.

"Digital evidence or electronic evidence" can be found in electronic digital form and it must comply with all the requirements of evidence. Digital evidence is substantiating information that is kept or sent digitally and can be used as evidence by one or more parties in a judicial proceeding. Prior to using digital evidence, the court must determine its relevance, validity, and originality and determine whether the information is hearsay or whether a copy is preferable to the original. Evidence may also be collected on digital devices like telecommunication or electronic multimedia devices, therefore it is not just limited to those found on computers. Emails, digital photos, ATM transaction logs, word processing, spreadsheets, instant message histories, files saved from accounting software, internet browser histories databases, contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files are all examples of digital evidence. Digital evidence is prone to be more numerous, harder to destroy, simple to alter, simple to copy, maybe more expressive, and more quickly accessible. Computer forensics is another category of forensic science relating to legal evidence which deals with computers and digital storage mediums.

Significance of Digital Evidence

During the nascent stage of digitalization and technological growth the availability, usage of electronic device and the services provided thereto was very limited when compared with today's world. Throughout the globe technology has penetrated in such a way that we are not just experiencing smart phones and computers, tablets, external hard drives, but smart homes having internet-enabled home appliance(e.g. smart televisions, smart watches, refrigerators, vacuum & mopping robots, laundry-folding robots, Toilet Cleaning robots, Pool cleaning Robot, Window Cleaning Robots, Effie Smart Iron, fitness bands etc) so now we have more choice with smart devices parallel smart choices of doing crimes with the help of these smart electronic devices like cyber extortion (demanding money to prevent a threatened attack), malware creation, possession and distribution, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, website defacement(i.e. a form of online vandalism targeting the e-content of related websites), hacking, spoofing, phishing, identity theft, pornography, cyber stalking. Crime committed or any criminal activity targeting or using a computer, a computer network or a networked device as a tool is addressed as cybercrime. The present impact of digitalization and the technological interference in every aspect of our lives made the need and importance of digital evidence more felt especially when we experience the severity of the attached threats of cybercrime. Thus digital or electronic information is very much needed during judicial proceedings as a piece of evidence to prove or disprove the existence of an alleged fact. Electronic evidence unlike traditional evidence are more vulnerable to alteration, tampering, excision, transposition etc. if not preserved with utmost care and expertise by digital forensics experts apart from first responders, investigators, crime scene technicians. Digital evidence being volatile needs to be properly identified, handled, collected and sealed by digital forensics experts to save guard its authenticity, reliability, admissibility in the court of law during judicial proceedings or trial.

Relevancy and admissibility of digital evidence in India

Relevant means which is logical probative, on the other hand, admissibility is not based on logic but on law and strict rules. Many facts having no bearing on the facts to be proved are admissible. The question of relevancy has

[10] 2(v) of Information Technology Act, 2000

been dealt with under sections 4 to 50 of Bharatiya Sakshya Adhiniyam, 2023 (previously sections 5 to 55 of the Indian Evidence Act, 1872) whereas admissibility has been dealt with under section 56 onwards (previously section 56 onwards). The rules of relevancy declares a certain fact relevant, rules of admissibility lays down as to whether a certain form of evidence about a relevant fact may be allowed or excluded. Strictly speaking relevancy or relevant fact and admissibility are quite synonymous with each other but in legal language they denote entirely different conceptions.

The Supreme Court in *Ram Bihari Yadav v. State of Bihar*[11], explained the differences between relevancy of evidence and its admissibility. The court observed that more often the expressions 'relevancy' and 'admissibility' are used as synonyms but their legal implications are distinct and different because facts which are relevant are not admissible; so also facts which are admissible may not be relevant, for example, questions permitted to be put in cross-examination to test the veracity or impeach the credit of witnesses, though not relevant are admissible. The probative value of the evidence is the weight to be given to it which has to be judged having regard to the facts and circumstances of each case.

The Bhartiya Sakshya Adhiniyam (BSA) 2023 signifies a pivotal change in India's legal framework, especially regarding its clauses on electronic evidence, often called e-evidence. In an era dominated by digital technology, where significant quantities of information are produced, saved, and shared electronically, the acknowledgment and governance of e-evidence are essential. This article examines the primary provisions concerning e-evidence in the Bhartiya Sakshya Adhiniyam 2023 and analyzes the consequences these provisions hold for the Indian legal system.

According to *Bharatiya Sakshya Adhiniyam, 2023*, “document” means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records[12]. The definition of “document” has been broadened to encompass electronic or digital records such as emails, server logs, files on computers, laptops or smartphones, messages, websites, cloud storage, location data, and voicemail messages saved on digital devices. This revision recognizes the transition from traditional paper documentation to electronic communication and data storage in modern India. It ensures that the legal system is prepared to address cases involving digital evidence. It will furnish legal professionals, law enforcement, and the judiciary with a thorough framework to manage digital evidence stored across various platforms.

According to *Bharatiya Sakshya Adhiniyam, 2023*, “Evidence” means and includes (i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence[13]. So the word “evidence” in the Act signifies only the instruments by means of which relevant facts are brought before the court. The instruments adopted for this purpose are witnesses and documents. The term “Evidence” as defined in the Act is by no means exhaustive. The word 'evidence' connotes the instruments by which relevant facts are brought before the court so that it can come to a right decision[14].

The definition of 'evidence' now encompasses all forms of electronically provided information. This change will allow witnesses, defendants, experts, and victims to present their testimonies through digital methods. Additionally, it recognizes 'digital records' as valid documentary evidence. This amendment in the BSA reflects a technology-neutral stance by acknowledging the legitimacy of electronically submitted information and treating electronic communication as equivalent to traditional in-person statements.

---

[11] AIR 1998 SC 1850 : (1998)4 SCC 517

[12] Section 2(1)(d), *Bharatiya Sakshya Adhiniyam, 2023*

[13] Section 2(1)(e), *Bharatiya Sakshya Adhiniyam, 2023*

[14] Sengupta S.P (1988). *Law of Evidence*. Calcutta: Kamal Law House

Coercion' has been added to Section 22 of BSA, 2023 as one of the acts causing a confession to become irrelevant. Under Section 39 of BSA, the scope of an expert has been expanded to include persons especially skilled in 'any other field'. An Explanation has been added to Section 24 of BSA, 2023 that clarifies that in a case when multiple people are tried jointly, if the accused who has absconded or who failed to comply with the proclamation issued against him under Bharatiya Nagarik Suraksha Sanhita, is absent during the trial, the trial will be conducted as a joint trial.

Under Section 57 of the BSA, dealing with primary evidence, new Explanations have been expanded to include –

(i) an electronic or digital record which is created or stored, either simultaneously or sequentially in multiple files, then each such file is an original.
(ii) an electronic or digital record is produced from proper custody, it is sufficient to prove its contents unless it is disputed.
(iii) a video recording is simultaneously stored in electronic form and transmitted or broadcast to another, each of the stored recordings is an original.
(iv) an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is an original[15].

These enhancements create a structure for the legal handling of electronic or digital records, focusing on their appropriate management and confirming their authenticity across different storage contexts. It simplifies the process of validating and authenticating electronic material.

Section 58 of the BSA broadens the definition of secondary evidence. It now incorporates both oral and written acknowledgments, along with testimony from experts skilled in analyzing complex or extensive documents that are difficult to assess. Furthermore, this provision permits the admission of matching hash values (#) of original records as valid evidence, highlighting the integrity of particular files rather than the complete storage device. This revision seeks to improve the admissibility and dependability of evidence.

Section 61 establishes equality in the acceptance of electronic or digital records alongside other types of documents. Henceforth, electronic or digital records will hold the same legal significance, validity, and enforceability as traditional documents.

There was a new section 22-A under the Indian Evidence Act, 1872 that permits the relevance of oral testimony with regard to the substance of electronic documents. Though this section was removed from the Bharatiya Sakshya Adhiniyam, 2023.

The IT Act was enacted to regulate transactions through the electronic medium[16]. As one of its objectives, it amended the Indian Evidence Act by introducing Sections 65A and 65B the Indian Evidence Act, 1872 to acknowledge the growing influence of electronic evidence in Indian courts[17].

Section 6 of the IT Act provides that electronic records and electronic signatures can be used in Government and its agency. Hence they are admissible in a court of law. So, whenever a dispute regarding online contracts or e-crimes is to be adjudicated by a court, production of admissible evidence becomes necessary to decide the merits of the case. Section 141 of the Bharatiya Sakshya Adhiniyam, 2023 (136 of the Indian Evidence Act, 1872) empowers a judge to decide on the admissibility of the evidence.

Section 59 of the Indian Evidence Act, 1872 was amended to exclude electronic records from the probative force of oral evidence. However, for the documentary evidence to test the secondary evidence was in section 63 and 65 the Indian Evidence Act, 1872, new section 65A and 65B the Indian Evidence Act, 1872 was added for

[15] Section 57, *Bharatiya Sakshya Adhiniyam, 2023*
[16] Preamble, Information Technology Act, 2000
[17] *Ibid*, Schedule II, Entry 9

evidentiary rules of electronic records. Since, due to the size of computer/server, the evidence in electronic form cannot always be presented in the court of law, these section were introduced the provision for technical nature of it requiring the interpreter to read the same[18].

The word "document or content of documents" is not replaced by the word "Electronic documents or content of electronic documents" under the provisions of Section 61 to 65 of the Indian Evidence Act, 1872. This makes it clearly clear that the legislature did not wish to apply to electronic documents the applicability of sections 61 to 65 the Indian Evidence Act, 1872. It is the cardinal principle of interpretation that the assumption is that the omission is deliberate if the legislature has failed to use any term. It is well settled that no term is overly used by the Legislature[19].

Section 3 of the Bharatiya Sakshya Adhiniyam, 2023 provides that evidence can be given regarding only facts in issue or of relevance. Whereas, section 62 of Bharatiya Sakshya Adhiniyam, 2023 provides that the contents of electronic records may be proved in accordance with the provisions of Section 63 of the BSA, Section 63 of the BSA provides that notwithstanding anything contained in this Adhiniyam, any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

The special law for digital evidence now includes section 62, and further evidence of the validity of digital documents must be provided in accordance with the requirements of section 63. Similar to how Section 61 handles documented evidence, Sections 62 and 63 handle electronic evidence. A new procedure is devised to guarantee that the adduction of electronic documents conforms to the hearsay rule under these sections. Additionally, it protects additional rights including the authenticity of the program and the reliability of the information retrieval procedure. But because section 62 is a specific law that differs from the documentary evidence procedure in sections 58 and 60, it is further distinguished from other parts of law.

Before a computer output is admissible in evidence, the following conditions as set out in Section 63(2) must be fulfilled –

(a) the computer output containing the information was produced by the computer or communication device during the period over which the computer or communication device was used regularly to create, store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer or communication device;
(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or communication device in the ordinary course of the said activities;
(c) throughout the material part of the said period the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer or communication device in the ordinary course of the said activities[20].

[18] Dubey V (2017). Admissibility of Electronic Evidence: An Indian Perspective. *FRACIJ,* 4.
[19] *Ibid.*
[20] Section 63(2), Bharatiya Sakshya Adhiniyam, 2023

Where over any period, the function of creating, storing or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by means of one or more computers or communication device, whether in standalone mode; or on a computer system; or on a computer network; or on a computer resource enabling information creation or providing information processing and storage; or through an intermediary, all the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly[21].

In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely:

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3);
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule[22].

Digital evidence in India: some judicial observations

The Delhi High Court for the first time in *State v. Mohd. Afzal And Ors*[23] considered the test for determining the admissibility of electronic evidence under Section 65B of the Indian Evidence Act. In this case, the Division Bench of the High Court had to decide whether the call records of the accused had been legally permitted in conformity with Section 65B. The High Court in this case agreed with the prosecution's argument and noted that adherence to Sections 65B (1) and (2) was adequate justification for the admission of electronic evidence. The most important thing to remember from this case is that the necessity of a certificate, as stated in Section 65B (4), is just one of several alternative methods that can be accepted to authenticate electronic evidence[24].

The observation of this case was further affirmed by the Supreme Court in State *(N.C.T. Of Delhi) v. Navjot Sandhu @ Afsan Guru*[25]. In this case, the Supreme Court pointed out that the Section 65B (4) certificate was not a mandatory condition. Moreover, the disputed electronic record might be admitted in accordance with Sections 63 and 65 even in the absence of a certificate. This led to questions about whether the Supreme Court's decision violated the principle of *generalia specialibus non derogant*, which states that the special law must prevail over the general law[26]. Therefore, after the Navjot Sandhu case, there was a significant relaxation of the criteria for authenticating electronic evidence across the High Courts. However, there have been a number of cases when courts have chosen to disregard the finding in Navjot Sandhu case by which imposed the certificate under Section 65B (4) as a mandatory condition[27].

---

[21] Section 63(3), Bharatiya Sakshya Adhiniyam, 2023
[22] Section 63(4), Bharatiya Sakshya Adhiniyam, 2023
[23] (2003) 107 DLT 385
[24] *Ibid*, at 276
[25] (2005) 11 SCC 600
[26] *Ibid.*
[27] *Aniruddha Bahal v. CBI*, (2014) 210 DLT 292

In order to resolve this question, nine years after the *Navjot Sandhu* case, in *Anvar P.V. v. P.K. Basheer & Ors*[28], the Supreme Court had the opportunity to formulate a unified standard for interpreting the authentication requirement under Section 65B. The court held that the computer output is not admissible without compliance of 65B. This judgment has put to rest the controversies arising from the various conflicting judgments and thereby provided a guideline regarding the practices being followed in the various High Courts and the Trial Court as to the admissibility of the Electronic Evidences. The legal interpretation by the court of the following Sections 22A, 45A, 59, 65A & 65B of the Evidence Act has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate u/s 65 B(4) of Evidence Act and further clarified that in absence of such a certificate, the oral evidence to prove existence of such electronic evidence and the expert view under section 45A Evidence Act cannot be availed to prove authenticity thereof.

The Supreme Court in *Shafhi Mohammad v. State of Himachal Pradesh*[29], held that a party who is not in possession of the device from which the document is produced is not required to produce a certificate under Section 65B(4) of the Indian Evidence Act,1872, and that the application of the certificate requirement, which is procedural, could be relaxed by the Court whenever the interest of justice so warrants. The Supreme Court further over ruled the position of law and reiterated the same principle as was laid down in the *Anvar* case.

In *State of Karnataka v. M.R. Hiremath*[30], the Court emphasized that non-production of a certificate under Section 65B on an earlier occasion is a curable defect. It further held that "the High Court erred in coming to the conclusion that the failure to produce a certificate under Section 65B(4) of the Evidence Act at the stage when the charge-sheet was filed was fatal to the prosecution. The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise."

The Supreme Court in the *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and others*[31] held that "the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4)".

The Court further held that "We may reiterate, therefore, that the certificate required under Section 65B(4) is a condition precedent to the admissibility of evidence by way of electronic record, as correctly held in *Anvar P.V. (supra)*, and incorrectly "clarified" in Shafhi Mohammed (supra). Oral evidence in the place of such a certificate cannot possibly suffice as Section 65B(4) is a mandatory requirement of the law. Indeed, the hallowed principle in Taylor v. Taylor (1876) 1 Ch.D 426, which has been followed in a number of the judgments of this Court, can also be applied. Section 65B(4) of the Evidence Act clearly states that secondary evidence is admissible only if lead in the manner stated and not otherwise. To hold otherwise would render Section 65B(4) otiose.

Anvar P.V. (supra), as clarified by us hereinabove, is the law declared by this Court on Section 65B of the Evidence Act. The judgment in *Tomaso Bruno (supra)*, being per incuriam, does not lay down the law correctly. Also, the judgment in SLP (Crl.) No. 9431 of 2011 reported as *Shafhi Mohammad (supra)* and the judgment dated 03.04.2018 reported as (2018) 5 SCC 311, do not lay down the law correctly and are therefore overruled.

---

[28] (2014) 10 SCC 473

[29] (2018) 2 SCC 801

[30] (2019) 7 SCC 515

[31] (2020) 3 SCC 216

The clarification referred to above is that the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4)."

The aforementioned decision has resolved the issues raised by the numerous contradictory judgements and has given Trial Courts a set of guidelines about the procedures to be followed with regard to the admissibility of electronic evidence. The legal interpretation by the court of the following Sections 22A, 45A, 59, 65A & 65B of the Evidence Act has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate u/s 65 B(4) of Evidence Act. It has also clarified that in the absence of a certificate, oral testimony to establish the existence of such electronic evidence and expert testimony under section 45A of the Act cannot be used to establish its authenticity.

Recently in *Ravinder Singh @ Kaku v. State of Punjab*[32], the Supreme Court observed that the electronic evidence produced before the Court should have been in accordance with the statute and should have complied with the certification requirement, for it to be admissible in the court of law. Oral evidence in the place of such a certificate cannot possibly suffice as Section 65B(4) is a mandatory requirement of the law.

In *State of Maharashtra v. Dr. Praful B. Desai*[33], the question involved was whether a witness can be examined by means of a video conference. The Supreme Court observed that "video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence". The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.

In *Amitabh Bagchi v. Ena Bagchi*[34] ,the court held that the physical presence of a person in Court may not be required for the purpose of adducing evidence and the same can be done through mediums like video conferencing.

In *Twentieth Century Fox Film Corporation v. NRI Film Production Associates (P) Ltd.*[35], certain conditions have been laid down for video recording of evidence. They are as follows –

(i) The person who examines the witness on the screen shall file an affidavit/undertaking before examining the witness with a copy to the other side with regard to identification.

(ii) The witness has to be examined during working hours of Indian Courts. Oath is to be administered through the media.

(iii) The witness should not plead any inconvenience on account of the time difference between India and USA.

(iv) Before examination of the witness, a set of plaint, written statement and other documents must be sent to the witness so that the witness has acquaintance with the documents and an acknowledgment is to be filed before the Court in this regard.

(v) Learned Judge is to record such remarks as is material regarding the demeanour of the witness while on the screen.

---

[32] (2022)7 SCC 581

[33] AIR 2003 SC 2053

[34] AIR 2005 Cal 11

[35] AIR 2003 Kant 148

(vi) Learned Judge must note the objections raised during recording of witness and to decide the same at the time of arguments.
(vii) After recording the evidence, the same is to be sent to the witness and his signature is to be obtained in the presence of a Notary Public and thereafter it forms part of the record of the suit proceedings.
(viii) The visual is to be recorded and the record would be at both ends. The witness also is to be alone at the time of the visual conference and notary is to certificate to this effect.
(ix) The learned Judge may also impose such other conditions as are necessary in a given set of facts.
(x) The expenses and the arrangements are to be borne by the applicant who wants this facility.

In the matter of *State of Punjab v. Amritsar Beverages Ltd*[36], due to the same issue a copy of hard disk was taken but there has been no seal and signatures where court held that in such cases, the data must be copied or hard disk must be taken, a hard copy is to be made and the seal and signature should be affixed on the hard copy and a copy of it must be given to the person it is seized from. Thus, the procedure relating to the seizure of electronic evidence is provided.

In the matter of *Bodala Murali Krishna v. Smt. Bodala Prathima*[37] the court held that "the amendments carried to the Evidence Act by introduction of Sections 65A and 65B are in relation to the electronic record. Sections 67A and 73A were introduced as regards proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85A, 85B, 85C, 88A and 90A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence."

In *Jagjit Singh v. State of Haryana*[38], the Hon'ble Supreme court admitted the electronic evidence in the form of interview transcripts from the Aaj Tak television channel, Zee News television channel and the Haryana News of Punjab Today television channel. The court heavily depended on the digital evidence produced and held that the decision taken by the speaker was based on the voices recorded on the CD and these voices are proved to be of the member, the conversation is relevant and hence the conclusion reached by him regarding the disqualification is correct.

However, in the case of the recording of the transcripts of the interviews, the courts have made it clear that without the actual recording of the audio being made available for inspection, no reliance can be placed on the recording of audio recordings[39].

In the case of *Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke*[40] the Apex Court relied on the judgement of the *Anvar* case and held that there is no point in relying on the translated version if the voice recorder itself is not subject to analysis. Without the source, the translation does not have authenticity. The two main variables for electronic proof are source and authenticity.

In *Abdul Rahaman Kunji v. The State of West Bengal*[41], while deciding the admissibility of an electronic record that is an email it was stated that an email which can be downloaded and printed directly from the email account of an individual can be proved by Section 65B along with Section 88A of the Indian Evidence Act, 1872. The High Court of Calcutta passed a judgment that the testimony of a witness to carry out certain procedures to download and print the same is sufficient enough to prove the electronic communication and can be termed as electronic or digital evidence if it satisfies other factors of admissibility.

---

[36] AIR 2007 SC 59
[37] AIR 2007 (2) ALD 72
[38] (2006) 11 SCC 1
[39] *Sanjaysinh Ramrao Chavan v Dattatray Gulabrao Phalke*, (2015) 3 SCC 123
[40] (2015) 3 SCC 123
[41] 2016 CriLJ 1159 (Cal)

Comparative Study with UK, USA and Australia on Digital Evidence

In the United Kingdom, electronic evidence is subject to different rules for admissibility than traditional documentary evidence. Both the Police and Criminal Evidence Act of 1984 and the Civil Evidence Act of 1968 contain these clauses. In the UK, Section 5 of the Civil Evidence Act, 1968 governs the admissibility of electronic evidence. This provision, which is the same as Section 65B of the Evidence Act, permits the admission of "a statement included in a document created by a computer," provided that it satisfies the requirements of Section 5 (2). Moreover, the conditions mentioned under Section 65B (2) have also been closely adopted from Section 5 (2).

Section 69 of the Police and Criminal Evidence Act, 1984 provides that computer-produced evidence is admissible in criminal proceedings as long as there exists no reasonable grounds for believing that the statement it contains is inaccurate because of improper use of the computer and that, at all material times, the computer was operating properly or that the malfunction did not affect the production of the document or the accuracy of the statement. Finally, section 69 of the Police and Criminal Evidence Act 1984 requires that the Rules of Court concerning giving notice are satisfied.

Rules 901 and 902 of the Federal Rules of Evidence, 2015, deal with authenticating electronic evidence in the USA. These two provisions provide the authentication of physical evidence through a variety of methods, such as oral testimony, expert testimony, public reports, etc. In 2007, the District Court of Maryland in *Lorraine v. Markel American Insurance Co*. extended the applicability of Rules 901 and 902 to electronic evidence as well[42]. This helped create a flexible framework for courts and parties to admit electronic evidence through multiple means[43].

Documentary evidence must first be authenticated in accordance with the Federal Rules of Evidence before it may be admitted into evidence in court. Without making a distinction between computer-generated evidence and other types of documented evidence, the Federal Rules of Evidence address authentication. The logical conclusion is that computer-generated evidence is subject to the same standards as traditional documentary evidence.

The laws in Australia relating to authentication of electronic evidence are quite better than the laws of the UK stated above. This is because, in addition to the four requirements under Section 5(2), Section 59B of the South Australian Evidence Act, 1929 adds three additional conditions through sub clauses (e), (f), and (g), which serve as a safeguard against any tampering or manipulation of the electronic record[44].

These additional requirements are given below – a

(i) There must have been no interference with the computer that would have jeopardized the accuracy of its output[45].
(ii) A reasonable person must keep track of every change made to the computer[46].
(iii) There must be no reason to believe that utilizing the computer without adequate security measures has adversely affected the accuracy of the output[47].

Conclusion and Suggestions

In order to stay up with international trends, India still has a long way to go in terms of the issues with regard to the admissibility and appreciation of electronic evidence. Though the amendments were made to reduce the burden of the proponent of records, they are not absolute. It is obvious that India has not yet developed a strategy to

[42] 241 FRD 534 (2007)
[43] Federal Rules of Evidence, 2015, Advisory Committee's note to Rule 901(b).
[44] Section 59B, South Australian Evidence Act, 1929
[45] *Ibid,* 59B(e)
[46] *Ibid,* 59B(f)
[47] *Ibid,* 59B(g)

ensure the veracity of the information included in electronic records, which is susceptible to manipulation by anybody who has access to the server or location where it is stored.

Along with advantages, the admissibility of electronic evidence can sometimes be challenging. Courts must determine whether the evidence satisfies the three fundamental legal standards of veracity, reliability, and integrity. Following the Supreme Court's decision in the *Anvar P.V*. case, which established the guidelines for the admissibility of electronic evidence, it may be anticipated that the Indian courts will take a consistent stand and implement all feasible precautions for admitting and appreciating electronic evidence.

Considering the present position in India and other three countries as mentioned above, some suggestions are put forward to make the digital evidence more effective –

(i) The UK model provides us an opportunity to start because Section 65B (2) is an exact adaptation of the requirements outlined in Section 5 (2) of the Civil Evidence Act. Moreover, we may continue using the certificate-based authentication mechanism for admitting electronic evidence, which has been recognised in the UK.

(ii) The three new conditions under Section 59B of the South Australian Evidence Act must, however, be added to the existing conditions under Section 65B (2). This provision will minimize the scope of deliberate attempts for tampering or manipulating the electronic evidence.

(iii) To guarantee that the anticipated lack of an accompanying certificate does not affect its admission, Section 65B has to be amended to provide an exception for evidence obtained illegally.

(iv) To make the requisite of a certificate mandatory when admitting electronic evidence, Section 65B (4) should be adequately amended. This is due to the fact that, in the absence of a certificate, information relevant to the authenticity of an electronic record can become rather difficult for judges to understand.

(v) When a certificate is required, the barrier for judging the authenticity of electronic evidence is very low. As a result, Section 65B may follow the American model by permitting courts to seek additional forms of authentication if they have a reasonable grounds for believing that the certificate does not satisfy the requirements of Section 65B (2). The advantages would be as follows in this regard –

(a) it will support in authenticating the data provided in the certificate and help in boosting its accuracy and reliability.

(b) Future improvements in authentication techniques will inevitably result from technological progress. Pre-empting such a scenario would assist us in preventing a situation in which courts are unable to use advanced authentication techniques because of a mandatory certification requirement.

The ruling in *Arjun Panditrao Khotkar* endorsed the idea that the rules regarding the admissibility of electronic evidence constitute a self-contained and thorough “complete code,” effectively avoiding the emergence of two separate procedural pathways within the current legal framework concerning electronic evidence. The methods proposed in previous judgments, such as *Anvar P.V* and *Shafhi Mohammad*, were considered inconsistent, which positioned the verdict in *Arjun Panditrao Khotkar* as a crucial move towards consistency in this legal domain – a development that is now in question following the recent introduction of the BSA, 2023.

A THEORETICAL ANALYSIS OF CYBER LAW FOR WOMEN AND CHILDREN IN INDIA

Banashree Ghosal
Research Scholar, Department of Sociology, SKBU, Purulia, West Bengal

Dr. Chandrani Chattopadhyay
Assistant Professor, Department of Sociology, SKBU, Purulia, West Bengal

ABSTRACT

Cybercrime refers to criminal activities conducted through the internet, mobile devices, computers, and various gadgets. These technologies often keep individuals busy and distracted, but some people misuse them for personal gain or malicious intent. We inhabit a world that is interconnected through both the internet and physical interactions. In today's fast-paced environment, the internet provides a quick route to success in acquiring information, but this can sometimes involve illegitimate tactics such as exploitation and manipulation.

Furthermore, users often share personal information online, and with the right skills and a criminal mindset, offenders can exploit this data. Women and children, in particular, have experienced severe incidents of cybercrime, and the past few years have seen a significant increase in such offences against these vulnerable groups. As we navigate both the virtual and physical worlds, it raises the critical question: how can individuals protect themselves in the cyber world from molestation, harassment, and other threats? Cyberlaw addresses issues related to cyberspace and information technology. This research paper will analyze the protective measures of Indian law concerning the virtual world.

Key words: *Cybercrime, Virtual world, Cyberstalking, Pornography.*

Introduction

Women and children are often observed as the most vulnerable segments of our society. Unfortunately, they are also the most targeted group for offenders. Perpetrators not only attack them physically but also digitally. In the 21st century, we navigate both the physical and digital worlds, making it essential to consider incidents that occur online as well. Through social media, we communicate, build trust, and connect with people in virtual spaces, which have become a new reality. When it becomes challenging to harm someone physically, the cyber world provides an alternative way to inflict damage. As a result, many individuals experience mental and emotional torment through online interactions. Cybercrimes, such as cyberstalking and bullying, have been on the rise. With the conveniences of modern life, society has become increasingly dependent on the digital world. Many tasks are now performed using laptops, mobile phones, and the Internet. For those pursuing education alongside a job, online classes have become essential.

1.1. Different types of cyber crimes against women-

In the past year, women have encountered several common cybercrimes, including:

Cyberstalking- Threatening through messages, constantly bombarding the victim with direct messages, phone, chats, etc.

Blackmailing for sexual favours – Offenders try to blackmail the victim with morphed images. The offenders blackmail for sexual favors.

Cyber hacks – with the help of fake news and information links, those will capture personal data and private images[1].

[1] Halder, D., & Jaishankar, K. (2016). Cyber crimes against women in India. SAGE Publications India.

Cyberbullying – Here to defame someone abusive statements will be written on social media. The victim will be threatened with rape threat. Offender sometimes morphs the picture of the victim for pornography.

Cybersex trafficking – This is one kind of sex trafficking in the cyber world. Here perpetrator streams photos and videos of the performance of sexual and intimate acts and sells this online. Blackmailing, manipulation, and coercion are also there[2].

Cyber Crimes against women in India –

Crimes	At the year 2017	In the year 2018	In the year 2019	In the year 2020
Cyber threatening	132	113	113	74
Cyber Pornography	271	862	1158	1655
Cyber Stalking	555	738	791	887
Morphing	50	62	61	251
Fake Profile	147	207	289	354
Others crime	3087	4048	5967	7184

Source: Cyber crimes against women (ncrb.gov.in)

The distinction between the physical and virtual worlds has become increasingly blurred in today's society. Reality and hyper-reality are closely intertwined, reflecting the ideas of sociologist Jean Baudrillard, particularly his concept of simulacrum, which refers to representations that replace reality[3]. We now encounter false images that often obscure our ability to distinguish between what is real and what is not. Morphed pictures serve as prominent examples of this phenomenon.

In our current age, sexual crimes in the virtual world encompass actions such as unwanted sexual advances, demands for sexual favours, the distribution of pornography against someone's will, and the creation of sexually morphed images. Such crimes can cause both physical and mental trauma in the physical world, and they inflict similar mental distress in the digital realm. While cyber assaults may result in less physical harm, the mental anguish and stress experienced are equally severe. The threat of criminal activity exists in both the physical and digital worlds and is becoming increasingly prevalent. Trust in sharing personal information in cyberspace is growing, facilitated by smartphones, laptops, tablets, and other devices.

Cybercrime against children

Children are not abandoned in this digital world. The online environment and social media platforms are easily accessible to them. This world is particularly fascinating, especially after the pandemic. During the lockdown, when education moved to the home setting, children gained access to tablets, phones, and laptops. However, this increased access also made children more vulnerable to bullying and harassment. Parents, while allowing children to use technology for learning and leisure, may not have foreseen the consequences. Consequently, children have become accustomed to these devices and the various forms of entertainment available, such as gaming, videos, and shows.

Many children unfortunately do not have the knowledge needed to stay safe online. They are especially at risk when they are unsupervised by their parents. The digital world often comes with fewer restrictions, making it

[2] Singh, J. (2015). Violence against women in the cyber world: a special reference to India. International Journal of Advanced Research in Management and Social Sciences, 4(1), 60-76.

[3] Baudrillard, J. (2019). Simulacra and simulations (1981). In Crime and Media (pp. 69-85). Routledge.

easier for perpetrators and cyber offenders to infiltrate and manipulate young users. Children, with their immature judgment, may not recognize which websites, videos, or images are unsafe or inappropriate. As a result, they become easy targets for cyber offenders[4].

Cyber Crimes against children in India-

Crimes	At the year 2017	In the year 2018	In the year 2019	In the year 2020
Cyber threatening	01	04	03	03
Fake profile	03	03	01	01
Cyber Pornography	07	44	102	738
Cyberstalking	07	40	45	140
Internet crimes through online games	00	00	01	00
Other crimes against children	70	141	153	220

Source: Cyber-crimes against children (ncrb.gov.in)

2.1. Different types of cyber crimes against children-

Pornographic content – The dark side of the cyber world is it can misuse our trust. Sexual abuse of children is one kind of activity of that. Child pornography, images, videos, and online sexual exploitation of a child through call and video can damage the innocent mind of the viewer. A video like children is coerced into performing sexual acts harmful to one immature mind.

Cybersex trafficking – The abuser streams some images and videos performing the child's intimate acts. This can be done with morphed images also.

Child grooming – Here the offender becomes friends with the child by using his or her loneliness. The child starts to keep trust in the offender. By manipulating the child, cyber offenders force him or her to perform sexual acts[5].

Indian Laws for cyber crimes

India has several laws in place to combat cybercrime, particularly concerning women and children. Victims, along with their parents, can file complaints online through the National Cybercrime Reporting Portal, where they can also upload relevant evidence. Additionally, victims can track the status of their reports online. An offline, written complaint method is also commonly used. The Information Technology Act of 2000 addresses various cybercrimes. Specifically, Sections 66E and 67 outline the punishment for offenders who intentionally capture images of a person's private areas. Penalties for such offences can include imprisonment for up to seven years, along with potential compensation[6].

[4] Kumar, P. V. (2016, March). Growing cyber crimes in India: A survey. In 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE) (pp. 246-251). IEEE.

[5] Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 305-326.

[6] Shah, M. R. (2019). Cyber Crimes in India: Trends and Prevention. IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 6(1), 25-37.

In today's digital age, the prevalence of cybercrime is alarming activities that would have been unimaginable a few years ago have become common. While the IT Act 2000 has provisions addressing various online offences, it lacks strong, specific measures that deal exclusively with crimes against women, as the Indian Penal Code does. For instance, the IT Act does not clearly define cyber defamation. However, it does prohibit child pornography under Section 67B, and the Protection of Children from Sexual Offences (POCSO) Act also addresses child safety issues[7]. Individuals are well aware of the severe penalties associated with cybercrimes, such as cyber pornography, which are defined under Sections 66A, 66E, 67A, and 67B of the IT Act 2000. Despite these efforts, there remain inadequate legal provisions regarding the viewing or storing of pornography[8].

Conclusion

In today's era, we live in an information–communication society. The famous sociologist Manuel Castell[9] outlines this as a 'Network Society'[10]. Through technology, we are now connected to the digital world, cyberspace. This is one kind of historical change. We also trust people in the cyber world like the contemporary physical world. This is increasing our risk, especially issues related to safety. It is a new type of space. Internet-based network society has become the basic unit of the modern era. Then why are the definitions of crime and punishments not the same in cyberspace? The mental trauma for the victim is the same for both worlds. Why the definition of molestation, rape, sexual abuse, and punishment are not the same?

[7] Singh, S. (2020). Cyber Crime against school children: Challenges & Solutions. International Journal of Home Science, 6(3): 264-267.

[8] Sankhwar, S., & Chaturvedi, A. (2018). Woman harassment in digital space in India. International Journal of Pure and Applied Mathematics, 118(20), 595-607.

[9] Castells, Manuel; Ince, Martin (2003). "Manuel Castells: Life and Work". Conversations with Manuel Castells. Cambridge: Polity Press. pp. 8–9

[10] Stalder, F. (2006). Manuel Castells: The theory of the network society. Polity Press, Cambridge.

ARTIFICIAL INTELLIGENCE: EXAMINING THE BENEFITS AND RISKS OF ARTIFICIAL INTELLIGENCE IN AGE OF SOCIAL MEDIA AND ITS LEGAL IMPLICATIONS IN INDIA

Anita
Research scholar, Department of Law, Kurukshetra University, Kurukshetra

Dr. Manjinder Gulyali
Associate Professor, Institute of Law, Kurukshetra University, Kurukshetra

ABSTRACT

The introduction of artificial intelligence into social media platforms has transformed user interaction, content distribution, and communication in the digital age. However, these changes raise important ethical and legal issues and challenges. The regulatory frameworks controlling AI applications on social media are the focus of this paper, which explores the nexus between AI and social media, addressing key topics such as content moderation, algorithmic transparency, data privacy, and disinformation, as well as major legal ramifications and issues associated with the use of AI in social media. It is crucial to carefully assess the use of AI, as it has the potential to impact public opinion and behavior. AI algorithms are being utilized more to recognize and eliminate offensive content, including explicit material, disinformation, and hate speech. But these algorithms' opacity begs questions about responsibility, transparency, and possible biases. Legal frameworks must address how to protect free speech while maintaining an appropriate balance in content regulation. Key legal concerns include the possibility of over-censorship, which could lead to the unwarranted removal of legitimate content and the exaggeration of preexisting prejudices in AI systems. Ethical implications of AI in social media are finally being considered. This paper emphasizes the need for ethical standards that focus on the well-being of users and the overall benefit to society.

Key words: *Artificial Intelligence, social media, Digital Age, legal implications.*

Introduction

Artificial intelligence (AI) is leading a technological revolution that is radically changing the face of contemporary society. Social media is the one area where this change is most noticeable. AI has been ingrained in online interactions due to its unmatched ability to digest large volumes of data, identify complex patterns, and make judgments on its own.

In recent years, AI has dramatically changed how content is created, filtered, and consumed on social media sites. AI technologies are improving user experiences and streamlining marketing tactics with anything from automatic moderation and real-time data analysis to tailored content recommendations. For example, chatbots offer real-time customer support, picture recognition tools assist with photo organization and labeling, and algorithms evaluate user behavior to recommend relevant material.

The ethical ramifications of AI-driven decision-making, algorithmic prejudice and privacy are some of the important issues that this integration also brings up. Concerns about AI's ability to reinforce preexisting biases or introduce new ones, as well as its potential to violate user privacy through mass data gathering and analysis, are substantial. Furthermore, there are still arguments for stronger legislative frameworks to guarantee the ethical application of AI, and the accountability and transparency of AI systems continue to be controversial topics.

This research seeks to investigate the complex relationship between artificial intelligence (AI) and social media, looking at both the advantages and drawbacks. We want to comprehend how artificial intelligence (AI) is changing the social media landscape and what this means for consumers, content creators, and society at large by examining existing uses and potential future developments. This research will offer insights into the changing dynamics of AI and social media through a review of the literature and case studies. It will also provide recommendations for striking a balance between innovation and ethical issues.

AI-DRIVEN SOCIAL MEDIA: ENHANCING CONNECTIVITY AND CONTENT

Nowadays we are living in a digital world. It changes our way of living, mindsets, with the advancement of information communication of technology Artificial Intelligence came into existence. There is hardly any sector which remains untouched from Artificial Intelligence and social media is one of them. Social media has become the most powerful means of communication in the digital age. Websites, apps, and other digital platforms that facilitate content sharing, interaction, communication, and teamwork are collectively referred to as social media. Social media is used by people to maintain relationships with friends and family. Social media offers countless opportunities for human connection and interaction; Above all, social media has made it possible to converse and connect instantly through real-time texting. Utilizing a variety of multimedia formats, such as text, pictures, emoticons, audio, and video. This has made communication easier to reach and more efficient, especially considering that many people now hold cell phones with remote access capabilities for social media apps. Social media and artificial intelligence are closely related, as AI is crucial to improving user experiences and maximizing marketing tactics. Artificial intelligence (AI) has many positive effects on social media like Personalization, efficiency, and content suggestions are among the advantages of implementing AI in social media platforms[1]; yet, there are a number of ethical problems, including those related to privacy, algorithmic bias, disinformation, job displacement, and mental health. Effectively utilizing AI in the social media realm requires striking a balance between these benefits and drawbacks.

5 "I" CONCEPT[2]

PM @narendramodi presented his vision of maximizing digital technology for society benefit in his intervention at G20 on Digital Economy & AI. The 5 'I's are -- Inclusiveness, Indigenization, Innovation, Investment in infrastructure & International cooperation, At G-20 Summit Prime Minister of India called the international Co-operation for Artificial Intelligence advancement and to deal with the concerns associated with the Artificial Intelligence. The Prime Minister of India said, we are living in the digital world and digital advancement is important not only for individual development but also for international development.

Union Minister of Electronics and Information Technology, Ashwini Vaishnaw, said, "Ethical issues in artificial intelligence (AI) and spread of fake news are global concerns and India is committed to addressing these challenges through robust debate and responsible innovation, while fixing accountability on social media platforms[3]"

The minister emphasized the need for strong legislative frameworks, social media accountability, and the significant difficulties presented by the developing AI landscape. The minister emphasized how crucial it is to strike a balance between the right to free speech and the need to prevent false news and guarantee truthful stories in the digital era.

AI TOOLS IN SOCIAL MEDIA ARE GAME CHANGER

Artificial intelligence is still revolutionizing a lot of areas in our lives. One area where this effect is most noticeable is in the social media space. Artificial intelligence (AI) is changing how we connect and interact online, from the advertisements we watch to automated content moderation and personalized suggestions, big data analytics, sentiment analysis, and content creation will help your social media approach. Artificial intelligence (AI) tools assist in improving the features of social media platforms and leading social media operations at scale. In a variety of use cases, such as the generation of text and visual content, social media monitoring, ad management, influencer research, brand awareness campaigns, and more. This will improve your decision- making, help you comprehend your audience, and free up time for other, more important tasks

[1] Mohamed, E. A. S., Osman, M. E. & Mohamed, B. A. (2024). The Impact of Artificial Intelligence on Social Media Content. Journal of Social Sciences, 20(1), 12-16. https://doi.org/10.3844/jssp.2024.12.16

[2] The Economic Times, June 29, 2019, 08:24:00 AM IST

[3] Addressing ethical challenges of AI, making social media accountable on fake news: Ashwini Vaishnaw,.ibtimes.co.in,11 dec, 2024

Some examples of AI tools: StoryChief, AICarousels, Typeframes, TweetGen, Canva, Typefully, BlogToPin, Perplexity AI, ChatGPT, Xnapper[4].

Artificial Intelligence (Ai) In social media Can Make Life Significantly Easier

● **Personalized Content Recommendations:** Algorithms with artificial intelligence (AI) are made to learn from user behavior and provide recommendations and tailored information. AI is used, for instance, by social networking sites like Facebook, Instagram, and Twitter to recommend pages, groups, and posts that you might find interesting. Your prior activities with the site, such as your likes, shares, and comments, are the basis for these recommendations. Social media companies may enhance user engagement and lengthen users' stays on their platforms by leveraging artificial intelligence to tailor content.

● **Enhanced User Experience:** Social media networks are employing AI to enhance the user experience by providing a more fluid and intuitive interface. For example Chatbots with artificial intelligence (AI), can assist customers with their questions, and image recognition technology can enhance the precision of photo and video tagging. Additionally, AI can assist platforms in recognizing and eliminating spam and fraudulent accounts, improving user safety and dependability.

● **Recognition of Images and Videos:** These days, AI systems can identify photos and videos that have been posted to social media sites. Because of this, social media companies are now able to provide additional features like automatic tagging, which recognize objects and individuals in pictures.

● **Trend Evaluation:** Social media data can be analyzed by AI systems to find trends and patterns. Because of this, social media platforms can now offer marketers and businesses insightful information. For example, Twitter's, Instagram, Facebook AI algorithms can identify hot topics and hashtags, allowing businesses to stay up to date with the newest trends and modify their marketing tactics appropriately.

Business and marketing: Social media influencers may now be found using AI algorithms based on parameters like followers, engagement rates, and other data. Because of this, it is now simpler for companies to find influencers who fit in with their target market and brand.

● **Chatbots:** Another area on social media where AI has had a big impact is chatbots. Computer programs that mimic human dialogue are called chatbots. They are frequently employed in customer service, where their ability to reply to questions and offer solutions promptly is valued. For instance, Facebook Messenger leverages chatbots to let companies automate sales and customer support queries[5].

● **Time-Saving:** Artificial intelligence (AI) frees up time for more creative and strategic endeavors by automating repetitive chores like scheduling postings, moderating comments, and answering frequently asked questions.

● **Accessibility:** AI makes social media more inclusive for people with diverse needs by enhancing accessibility features like automatic captioning and translation.

● **Effective Customer Service:** AI-driven chatbots instantly respond to consumer questions, addressing problems and raising customer satisfaction levels.

[4] Ai Social Media tools, https://www.insidr.ai

[5] Yage Liu 2023, AI Chatbots in social media: Ethical Responsibilities and Privacy Challenges of Information and Communication Technology, IMMS '23: Proceedings of the 2023 6th International Conference on Information Management and Management Science, https://doi.org/10.1145/3625469.3625483

RISKS OR CHALLENGES OF USE OF AI TECHNOLOGY IN SOCIAL MEDIA PLATFORMS:

Use of Artificial Intelligence technology in social media: a hub of cyber crime

Increasingly, individuals of all ages and genders are creating profiles on online social networks so they can communicate with one another in this virtual environment. Some people have thousands or even hundreds of friends and followers split over several accounts. However, the expansion of phony profiles is also occurring at the same time. Oftentimes, fraudulent profiles bombard authentic people with offensive or unlawful stuff. Additionally, false profiles are made, portraying well-known individuals to harass them.

The most popular targeted websites/apps used to create Fake Profiles are: Facebook, Instagram, Twitter, LinkedIn, WhatsApp, Snapchat.

Use of AI technology in social media is responsible for emergence of cybercrime like-

Online Threats, Stalking, Cyber bullying:

The most often reported and observed crimes on social media are individuals making threats, harassing, stalking, and intimidating others online.

Hacking and fraud:

Even while posting a humiliating status update on a friend's social media account could be okay among friends, it is technically illegal. Furthermore, depending on the activities taken by the person using a fake or impersonation account, creating a fake account or impersonating someone else in order to deceive others may also be punished as fraud[6].

Artificial intelligence and social media: privacy concerns:

Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, and several other international and regional human rights accords all acknowledge the right to privacy as a fundamental human right. The right to life, including privacy, is guaranteed by Article 21 of the Indian Constitution. A person's right to privacy is essential to their ability to live in safety and dignity.

The right to privacy and data protection may be infringed upon as algorithms utilize personal data to select the material that will be given to each individual and skew their ability to make independent decisions.

Using AI technology in social media creates privacy issues, particularly about personal data. Large amounts of data are frequently used by AI systems and social media to train their algorithms and enhance performance. This data may contain sensitive information like social security numbers as well as private information like names, residences, gender, age, and financial frauds. User information may be at danger when utilizing social media due to data protection concerns and gaps in privacy safeguards. Accounts on social media might not be as private as people believe. For instance, if a user reposts anything they shared with a friend, the friend's friends will also be able to view it. The material that was originally uploaded by the user is now seen by an entirely different audience. Since posts in closed groups can be searched, including comments, they could not be entirely private. Malware that attacks users with advertisements, slows down computers, and steals confidential data can be distributed over social networking networks. Hackers take control of the social media account and spread malware to all the user's friends and contacts as well as the compromised account.

Deepfake technology:

The term "deepfake" describes the creation of textual, audio, visual, or video content (SMS or written content)

[6] Danny D'Cruze, Jan 18, 2024,AI is making cyber criminals dangerous with tools like FraudGPT, https://www.buinesstoday.in

using cutting-edge artificial intelligence and machine learning technologies. Technology can create media that mimics the voice and appearance of people. Deepfakes are artificial intelligence (AI) and deep learning algorithm-generated synthetic media, frequently presented as images, audio, or movies. These algorithms seamlessly superimpose the likeness of one person over another by altering or replacing existing content using enormous databases. Shallow fakes are a kind of misleading media that is comparable to but maybe less well-known than artificial intelligence (AI) in that the media is edited using basic editing tools rather than AI. It can be difficult to distinguish between real and false content due to the intricacy of this procedure.

Online controversy has erupted around a purported video of actress Rashmika Mandanna entering an elevator. What looks real at first is actually a "deepfake" of the actress. Zara Patel, a British Indian girl, was featured in the original video; however, Mandana's face was substituted for Zara's. The Union Minister for Electronics and Technology, Rajeev Chandrasekhar, responded to the video by saying on the social networking platform X that deep fakes are the newest and a "more dangerous and damaging form of misinformation" that social media platforms should be handling. He also mentioned ITdata. Concerns over the data's usage and accessibility may arise from its gathering and processing. The biggest privacy concerns surrounding AI is the potential for data breaches and illegal access to personal information. Because there is so much data being gathered and processed, there is a chance that it could be misused through hacking or other security flaws. It is possible to abuse generative AI to modify photos or make up profiles. Scammers can obtain enough information from user social media accounts to spy on users, steal identities, and launch regulations concerning digital deception and social media companies' legal responsibilities[7].

The 73-year-old victim, Radhakrishnan, got a WhatsApp contact from a person posing as Venu Kumar, a former colleague. The caller's appearance and voice were an exact replica of Venu Kumar due to deepfake technology. The caller claimed to be in dire need of money and begged Radhakrishnan for a ₹40,000 loan. With complete confidence that the caller was, in fact, his old colleague, Radhakrishnan sent the money[8].

According to a ToI report from November 30, thieves used a video that had the voice and face of a retired IPS officer from the UP Police to extort a 76-year-old man. The senior citizen ended up making repeated payments to the thieves out of concern that authorities would take action against him[9].

Violence and Indecent Representation of women and children by using AI tools in social media:

AI technology used in online platforms to create illicit, obscene, and pornographic content. Artificial intelligence (AI) has been linked to violence and abuse. For example, a person's face could be digitally merged into already-existing pornographic photos or films using AI-assisted applications and tools to produce so-called "deep fake" imagery, as demonstrated in Image- Based Abuse. Because we still live in a society where outdated ideas about a woman's sexual reputation or character still determine her value and appropriateness as a worker, mom, or friend, fake sexual imagery can still be immensely destructive to women.

- In a case, two siblings in Maharashtra's Palghar district are suspected of using artificial intelligence (AI) to produce and share obscene and pornographic videos of women and girls on social media[10].

Will and preferences of the social media users are controlled by the marketing companies using Artificial intelligence technology:

AI is significantly changing the way businesses utilize social media. Facebook, Instagram, Twitter, LinkedIn, and other social media platforms are more than just instruments for communication. They are now an essential part of

---

7 Ankita Deshkar, Deepfake' video showing Rashmika Mandanna, THE INDIAN EXPRESS JOURNLISM OF COURAGE November 7, 2023 12:03 IST

8 Kerala's deep fake Fraud, Indian cyber squad Nov 27, 2023

9 Times of India report, November 30, 2023

10 Mayank Kasyap, AI generated obscene videos circulated on social media by sons of Mumbai cop, News24, Aug 24, 2023 06:55 IST

any company's marketing toolkit for those looking to build a significant internet presence. In order to properly utilize these dynamic platforms, businesses need to stay up to date on the latest advances in social media trends, which are always evolving. Using social media to interact with people for business purposes or to purchase products or services that are lawful may be entirely acceptable. Nonetheless, it is most likely unlawful to use social media to purchase narcotics or other regulated, controlled, or prohibited goods. In one the report it is stated that digital data collected by unauthorized agencies is a big concern as they control the mind and activities of the user of social media. Collected data is used for the purpose of profit earning as they show their product and sell on online platform according to the interest of individual[11]. Sometimes business companies share and transfer collected data even across boundaries for profit earning.

Artificial technology and the spread of fake, misinformation, and disinformation:

Artificial intelligence Technology poses a challenge to democratic representation, democratic accountability, and social and political trust because of its capacity to spread false information and misinformation at large. It is true that social media sites and artificial intelligence (AI) are major contributors to the propagation of hate speech, rumors, and false information. AI techniques exacerbate the disinformation phenomenon online AI methods are opening new possibilities for text creation and manipulation, as well as for image, audio, and video content. The efficient and quick spread of misinformation online is greatly aided by the artificial intelligence (AI) algorithms that internet platforms design and implement to increase user engagement.

Artificial intelligence and social media: threat to democratic values:

The rapidly developing field of generative AI revolutionizes the fields of journalism, economics, and medicine, and also has a significant impact on politics. WhatsApp, YouTube, Instagram, and other social media channels are now essential to Indian political campaigns. By utilizing these channels, political parties may communicate with voters directly and go beyond traditional news gatekeepers like journalists. On social media, falsehoods, twisted messages, malevolent assertions, and artificial intelligence-powered fabrications are commonplace. These components are frequently employed with little accountability in order to malign opponents and sway voter opinions. Deepfake films, AI-generated memes, and other synthetic media are being used more frequently to spread misinformation and sway public opinion. Election Commission rules[12] pertaining to the use of AI and social media in campaigns are difficult to implement. It is challenging to control hate speech and false information online due to the large volume of activity and the usage of shadow accounts.

Artificial intelligence and social media: threat to national security:

The application of AI in the field of national security presents unique difficulties because of its evolutionary consequences. With the rise of hybrid warfare, cyber security threats like ransomware, and the development of technologies like the Internet of Things (IoT), artificial intelligence (AI) has caused disruption in the context of the evolving security landscape. Cyber- physical systems have complicated the situation.

Non-state actors have easier and greater access to AI-based technologies because of the dual use of AI (military and civil applications), which has further complicated efforts to regulate the technological flow. Furthermore, as social media has grown in popularity, artificial intelligence (AI) has become a fundamental component of these platforms, where it is being exploited to propagate hate speech, radicalization, and false information, hence increasing national security risks[13].

---

[11] Clodagh O'Brien, AI in social media, digital marketing institute, May 01, 2024

[12] https://www.eci.gov.in/eci-backend/public/api/download?url=LMAhAK6sOPBp%2FNFF0iRfXbEB1EVSLT41NNLRjYNJJP1KivrUxbfqkDatmHy12e%2FztfbUTpXSxLP8g7dpVrk7%2FeVrNt%2BDLH%2BfDYj3Vx2GKWdqTwl8TJ87gdJ3xZOaDBMndOFtn933icz0MOeies xvsQ%3D%3D

[13] Sharma Sanur, AI and National Security: Major Power Perspectives and Challenges, Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi September 12, 2022

Artificial Intelligence and social media: threat to human rights and values

Human rights are the inherent, unalienable rights that all people have, irrespective of their gender, ethnicity, nationality, religion, or any other distinction. They include economic, social, and cultural rights like the right to work, health care, education, and culture, as well as civil and political rights like the right to life, liberty, privacy, expression, and participation[14]. Numerous people's human rights have continued to be infringed and abused as the use of AI has risen. Some of the rights like right to privacy and data protection, right to freedom of speech and expression, right to profession and right to livelihood, right against indecent representation of women in online platforms using AI tools and right against defamation. The advancement of AI technology in India has given rise to grave concerns over human rights. The human rights of women, children, migrants, and refugees have been negatively impacted by AI, which frequently results in bias, discrimination, inequality, and privacy abuses. Artificial intelligence technologies provide significant obstacles to India's well-established human rights law frameworks. The swift advancements in artificial intelligence have often left conventional laws in India behind, leading to substantial legal issues due to uncertainty and confusion over legal personality, responsibility, accountability, and liability.

Ethical implications:

The digital ecosystem's AI techniques provide up new avenues for efficiently and widely manipulating people, rising or exacerbating several ethical issues.

Human dignity is a first ethical value that is challenged by the current digital ecosystem. AI algorithms are programmed to adapt what is shown to individuals based on their profile created through datafication to optimize engagement, regardless of the content's quality, those individuals are considered as mere means for economic purposes. AI techniques present in the digital ecosystem change reality in most cases unbeknownst to the individuals, expanding opportunities for effective manipulation of their opinion. Indeed, targeted individuals are rarely aware of the current digital ecosystem, and they usually think that the disinformation they see online is objective and universally encountered by other users.

Secondly, the difficulty to access information alongside the pervasiveness of disinformation online drastically impairs the individuals' capacity to make free and informed decisions, which is an essential prerequisite for their autonomy. The value of autonomy “refers to the capacity of individuals to construct their own identity, to determine their own 'good', their own vision of a good life in respect of others' similar capacity, and therefore to contribute fully to collective deliberation[15].

LEGAL IMPLICATION OF AI IN CONTENT MODERATION AND CENSORSHIP

Monitoring, evaluating, and controlling user-generated information on websites and social media platforms are referred to as content moderation and censorship. Content moderators are essentially in charge of making sure user-posted content conforms to community standards and legal requirements, including those pertaining to hate speech, harassment, violence, and nudity. Content moderation and censorship are significant because they are essential to preserving a polite and safe online environment. They aid in stopping the dissemination of damaging information that might encourage hatred, prejudice, and violence. Additionally, they safeguard the privacy and rights of users of social media platforms and websites,

The rapid expansion of social media and the democratization of content production in recent years have increased the urgency of the need for efficient content filtering. It is nearly difficult to manually examine and control all of the content on social media platforms, as billions of individuals create and share content every day. The need for automated solutions that can instantly scan and filter massive amounts of data is therefore growing.

[14] Universal Declaration of human right 1948

[15] Goutham Krishnan and Adv Rebecca Sara George, THE IMPACT OF AI ON HUMAN RIGHTS”, Academic

Important moral and legal questions are also brought up by content moderation and restriction. For instance, there are worries about how censorship affects the right to free speech as well as the possibility of prejudice and discrimination in automated content moderation. Therefore, it is critical to find a balance between shielding people from damaging content and making sure that their freedom of speech isn't unfairly curtailed.

Role of judiciary

The judiciary plays a crucial role in analyzing the advantages and dangers of artificial intelligence (AI), especially in the age of social media.

- The Indian Supreme Court affirmed the right to privacy as a basic right guaranteed by the Indian Constitution in the historic decision of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[16]. This decision highlights how important it is to protect personal information from AI-based systems.

- In the case of Gramophone Company of India Ltd. v. Super Cassettes Industries Ltd[17], the Delhi High Court determined that AI-generated music produced by a computer program lacks human creativity and, therefore, is ineligible for copyright protection. This case clarifies the copyrightability of AI-generated content in India.

- The Prajwala v. Union of India[18] case revolves around the alarming issue of child sexual abuse material (CSAM) being widely circulated online, which brought to light the insufficiencies of the existing legal framework, particularly the Protection of Children from Sexual Offenses (POCSO) Act. Prajwala, an NGO based in Hyderabad, took a proactive step by addressing a letter to the Supreme Court of India, which was subsequently converted into a Public Interest Litigation (PIL). This case emphasizes the need for more stringent laws to combat the online sexual exploitation of children, an area where the POCSO Act was found lacking.

  The Supreme Court, upon hearing the case, observed that the POCSO Act, as it stood, was not adequately equipped to deal with the challenges of cybercrimes involving children.

  The Court noted the necessity of adopting a comprehensive approach that would include stricter regulations, improved technology for tracking and removing illegal content, and greater accountability for internet intermediaries.

  Recognizing the growing threat of online child exploitation, the Court directed the government to establish a committee to develop policies aimed at preventing and combating these crimes more effectively.

- Arijit Singh v. Codible Ventures LLP, COM IPR SUIT (L) NO.23443 OF 2024[19], the Bombay High Court upheld the singer's personality rights, ruling that unauthorized use of his name, voice, and image by the defendants, including AI-generated replicas, violated his rights. The court emphasized that celebrities have the right to control it

- In Anil Kapoor vs Simply Life and Others 30 April 2024[20], the defendants were found misappropriating Anil Kapoor's personality rights using generative artificial intelligence to superimpose his face on other famous actors' bodies and creating cartoon characters, which led to the Court granting an interim relief to Mr. Anil Kapoor for protection of his name, likeness, voice, persona, and other attributes of his personality against unauthorized commercial use.

---

[16] AIR 2018 SC (SUPP) 1841

[17] 2010 SCC Online Del 4743]

[18] https://indiankanoon.com.org

[19] https://www.livelaw.in

[20] Ipandlegalfilings.com

Laws related to AI technology in India

Information Technology Act, 2000 (IT Act)

India's primary legislation governing cyber security, digital governance, and electronic commerce is the Information Technology Act of 2000. Even though the IT Act was enacted before AI technology gained popularity, a few of its restrictions still apply to actions involving AI.

Digital personal data protection act 2023

India has a thorough framework for securing personal data thanks to the Digital Personal Data Protection Act, 2023, which was signed into law on August 11, 2023. The Act is extremely pertinent to AI systems that manage vast amounts of personal data since it addresses the collection, storage, processing, and sharing of data.

- Data Protection Principles: These principles mandate that AI platforms obtain user consent before processing personal data, ensure transparency, and allow users to withdraw their consent.
- Data Localization: The Act requires certain sensitive data to be stored within India, which impacts AI systems that rely on cross-border data transfers.
- Data Breaches: Companies deploying AI must report data breaches to regulatory authorities within a specific timeframe, further ensuring accountability.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021)

Intermediaries including social media sites, digital news outlets, and over-the-top (OTT) services are governed by the IT Rules 2021. These regulations require intermediaries to make sure that their platforms don't host, show, or send illegal content, which is relevant for AI systems that produce content like automated media or deep fakes.

Rule 3(1) (b): "This rule specifically mandates that intermediaries should not allow users to upload or share any information that is "grossly harmful, harassing, or defamatory." AI platforms that fail to comply with these provisions may lose their intermediary "safe harbour" protections and face legal penalties".

Principles for Responsible AI (2021)

In 2021, NITI Aayog published the Principles for Responsible AI. These guidelines, which emphasize ethical issues, direct AI development in India.

The society concerns center on how AI will affect the automation of industries and the generation of jobs, while the system considerations address concepts like accountability, transparency, and inclusion in decision-making. By establishing rules for AI governance, this paper makes sure that AI systems follow morally righteous and open procedures.

Digital Advertisement Policy, 2023[21]

The Ministry of Information and Broadcasting has approved a path-breaking Digital Advertisement Policy, 2023 on November 10, 2023. It aims to enable and empower the Central Bureau of Communication (CBC) which is the advertising wing of the GOI to undertake campaigns in the Digital Media Space. The Policy will enable CBC to empanel agencies and organizations in the OTT and Video on Demand Space.

[21] Principle of Responsible AI, NITI Aayog, https://www.niti.gov.in

Bhartiya Nyaya Sanhita, 2023

Section: 196, 197, 353etc, which deals with the creation, dissemination, or publication of false assertions, false statements, rumors through electronic means that cause public harm and mischief.

Solutions for Addressing the Benefits and Risks of AI in Social Media

Enhanced Privacy Protection: Use strong data encryption techniques to safeguard user information, and anonymize data to prevent the disclosure of personal information.

Regulation Compliance: Verify that AI systems abide by data protection laws like the GDPR and the Personal Data Protection Act of India. Establish clear guidelines for data collection, storage, and usage.

Regular Audits: Conduct regular audits and assessments of AI algorithms to detect and correct biases. Implement transparent reporting mechanisms to track the performance and fairness of AI systems.

Combating Misinformation by fact checking

Create and integrate artificial intelligence (AI) techniques that can recognize and highlight misleading material. Work together with fact-checking groups to ensure the accuracy of the content.

Public Awareness: Educate users about the risks of misinformation and the importance of verifying sources before sharing content. Promote digital literacy programs that teach users how to critically evaluate information online

Comprehensive AI Legislation: Develop comprehensive AI legislation that addresses ethical, legal, and social implications. Ensure that the legal framework covers data protection, algorithmic accountability, and user rights.

Multi-Factor Authentication (MFA): Promote the adoption of MFA to strengthen user accounts' security and make it more difficult for hackers to access them without authorization.

Biometric Authentication: To improve security and confirm user identities, use biometric authentication techniques like fingerprint scanning and facial recognition. Never divulge private information to somebody you've only spoken to on the phone or online.

Conclusion

It seems sensible to infer that artificial intelligence (AI) is currently one of the most important factors in a person's life after taking into account all of its features and how it relates to social media platforms. Artificial intelligence is the foundation of modern technology, which affects social networking sites. Since this is a relatively young industry, the majority of Indian consumers are not aware of the implications. AI has the potential to be just as harmful as it is helpful; it might interfere in some way and disturb a person's daily life and tranquility.

India is leading the way in the development of AI. But developing a strong legal framework for AI remains a difficulty for the nation. The framework for regulating AI is provided by current laws such as the IT Act, Digital Personal Data Protection Act, and IT Rules; but, in order to handle the intricacies and moral dilemmas of AI technologies, legislation tailored to AI is obviously required. as AI continues to change sectors and societies India must find a balance between encouraging innovation and guaranteeing acceptable, ethical AI practices comprehensive legislation that address bias, discrimination, accountability, and privacy issues while promoting AI's enormous potential to propel economic growth and societal advancement are probably going to be a part of India's future AI regulations. These days, social media and artificial intelligence permeate every aspect of our life. All we can do is be vigilant and proactive, and cautious enough to steer clear of any scams or damage that can arise from using these online portals.

REFERENCES

1. Sharma Sanur, AI and National Security: Major Power Perspectives and Challenges, Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi (September 12, 2022).
2. Basin Punit, Law Relating to Social Media Crimes, Intermediaries; Digital Media, and OTT Platforms' (edition 2022).
3.
4. Dr. Malhotra, Rajiv. (10 January 2021), 'Artificial intelligence and the future of power' Publisher: Rupa publication house, (Edition: 1, 2021).
4. Dr. Manaswini, Pradhan. (2022), 'fundamental of artificial intelligence and machine learning' Publisher DPS publishing house, (edition: 1, 2022).
5. Dr. Zolich, M, (4, January, 2023), The AI Advantage Chat GPT, AI and their role in the disruption of industries and creation of opportunities for businesses and individuals (Edition: 1, 2023).
6. James Irvin, AI for social media marketing in 2024: An In-Depth Guide, BOCNRT5GF5, (20 November 2023).
7. Nunez Christopher, Next Level Social media Harnessing AI for marketing Success,(24 November 2023)
8. Artificial Intelligence in Social Media, Publisher Introbook ISBN 9781393345206 (28/4/2020) (EBOOK).
9. M.B. Chatfied, Unraveling the impact of Artificial Intelligence on Social Media, ASIN: B0CQGS9X3N, (15/12/2023).
10. Singh Chanderveer, AI in Social Media Exploring Use Cases, Challenges, and Strategies, SocialPilot, (11/01/2024) https://www.socialpilot.com
11. Mohamed, E. A. S., Osman, M. E. & Mohamed, B. A. (2024). The Impact of Artificial Intelligence on Social Media Content. Journal of Social Sciences, 20(1), 12-16. https://doi.org/10.3844/jssp.2024.12.16
12. Yage Liu 2023, AI Chatbots in Social Media: Ethical Responsibilities and Privacy Challenges of Information and Communication Technology, IMMS '23: Proceedings of the 2023 6th International Conference on Information Management and Management Science, https://doi.org/10.1145/3625469.3625483
13. Ministry of Information and Broadcasting approves Comprehensive “Digital Advertisement Policy, 2023, https://pib.gov.in

DEEP FAKES AND THE EROSION OF IP RIGHTS: LEGAL FRAMEWORKS AND REMEDIES

Mr. Suresh
LLM Student, Christ Deemed to be University, Delhi NCR

ABSTRACT

Deepfakes, AI-generated content that simulates reality, pose a significant threat to individual privacy, as they can be used to create convincing but false digital content that damages reputations, invades personal boundaries, and manipulates public opinion.Deep fakes cause reputational harm to the targeted personalities and the creator of such activities definitely does it with malice. For this reason it is necessary to have a law to regulate.This research explores the privacy implications of deepfakes, including identity theft, reputational damage, and emotional distress. Critically analyzing and evaluating the notable deep fake scams . This can be illustrated with some following instances, targeting famous personalities, such as Rashmika Mandanna, Priyanka Chopra, Sachin Tendulkar, , Barack Obama, Donald Trump and a critical evaluation of existing privacy frameworks in the US, Europe, and India, this study identifies gaps in protection and proposes regulatory solutions to mitigate deepfake risks.The existing legal framework in India, primarily governed by the Information Technology Act, 2000, and the Draft Personal Data Protection Bill, 2019, provides limited provisions to address deepfake concerns. This research aims to contribute to the development of effective privacy countermeasures against this emerging threat.

Key words: *Deepfakes, Artificial Intelligence(AI), Emotional Distress, Copyright infringement, Trademark dilution, Intellectual property rights, Misappropriation of identity, Digital manipulation.*

Literature Review

Eleonora Rosati, 'Infringing AI: Liability for AI-Generated Outputs Under International, EU, and UK Copyright Law' (forthcoming, European Journal of Risk Regulation, 2024)[1].

Footer Detail missing

In the article, Eleonora Rosati discusses the difficulties of attributing copyright liability in the context of content that is created by AI and looks into the legal standards from the international and the EU and UK copyright laws as well. In addition, she investigates the TDM ({, affectionately TDM — text and data mining} exceptions, which permit AI systems to incorporate copyrighted material into training provided that specific conditions are met, and which do not extend the scope of these permissions to the production of outputs. Copyright omission has been described by Rosati as one of the baseline of uniqueness, whereas the related sub norms are investment protection modules. Another part of her analysis seems to point out that liability might not only be determined by the end users of the AI but also the developers and providers of the AI who may, under certain circumstances, be defined as secondary infringers, and in some cases, even primary infringers. Moreover, Rosati notes other possible justifications such as fair dealing, which are, within the context of the present dispute, more convenient for users rather than developers and makes the point that liability should be proportionate to the role of the actor within the AI system. This study advocates for the need to include references to AI outputs within the scope of copyright in order to enhance both the rule of law and the further development of AI.

S. Alex Yang and Angela Huyue Zhang, 'Generative AI and Copyright: A Dynamic Perspective' (forthcoming, manuscript, London Business School and University of Hong Kong)

In the article "Generative AI and Copyright: A Dynamic Perspective," S. Alex Yang and Angela Huyue Zhang[2] describe the relationship between copyright law and generative AIs with regard to the standards of 'fair use' and 'AI-copyrightability:' Do such legal norms stimulate or hamper the flourishing of AI technologies? The co-authors develop a dynamic perspective to assess the economic aspects of these legal regulations, particularly how they influence AI model advancement and profitability, as well as user satisfaction. In the Key sections like the Introduction or Model, the authors create a contact between AI's skeptics, the most content creators in regard to copyright infringement, and AI companies, establishing the economic struggle between the two. For AI-

Footer Detail missing

generated content, fair use, and copyright issues are in the center of that struggle. The research brings about strong contributions by describing two regimes of data: “data abundant” and “data scarce” which determine the algorithms of a majority AI-company–content creator interactions depending on the amount of training data at hand. The analytical strength of the paper is that it first provides the ability to depict complicated, real life situations and explains how creator's choices and AI evolution would depend on regulatory alternatives. The findings also offer practical recommendations for regulators, encouraging industry-based regulation. This paper makes it to this list due to its innovative empirical models that highlight the importance of policy considerations, which is appropriate for policy makers working in the sphere of artificial intelligence.

Wenqing Zhao, 'AI Art, Machine Authorship, and Copyright Laws' (2020) 12 American University Intellectual Property Brief 1[3]

Footer Detail missing

The article titled "AI Art, Machine Authorship, and Copyright Laws” by Wenqing Zhao examines how copyright laws may be applied to an artwork created by AI. It questions AI-generated art and if it has a creator, among other considerations. Early on, Zhao explains the controversy regarding a portrayal of Edmond de Bellamy, who was a picture created by AI and was bought for quite a sum which led to many claims regarding ownership and creativity in the field of AI. As the paper concludes, Zhao believed that machines create the art but the ones who warrant artistic recognition are the developers and artists who formulate and work with these AI tools. Zhao cites such AI projects as GAN and AICAN, and analyzes how AI art fits into the market. The focus is on the issues of originality and attribution. In general, Zhao maintains that, through some patients of AI, the copyright system could fuse with the AI-generated works and enforce them as works of art created by a human, armed with an AI tool. Such policy, Zhoa asserts, will drive creativity and will help meet an objective of arts promotion.

Amy B. Cyphert, 'Generative AI, Plagiarism, and Copyright Infringement in Legal Documents' (2024) 25 Minnesota Journal of Law, Science & Technology 49[4]**.**

Footer Detail missing

Amy B. Cyphert explains in her article titled 'Generative AI, Plagiarism, and Copyright Infringement in Legal Documents' how copyright and professional ethics, as well as their legal applicability, get into conflict with generative AI. All these worries sit well with Cyphert, who focuses on the large language models' (LLMs) other obvious risk: the potential of reproducing more than just inscribed literal words. The research is grounded in empirical evidence, demonstrating in training data the AI's “memorization” and its potential reproduction of original materials, which raises interrelated legal issues of its own. Focusing on several recent cases against Meta and Open AI, for instance, the author allows herself to suggest that derivative works will probably be viewed by courts in copyright infringement litigation against AI results from Openai and other entities. Significantly, the authors precede the previous discussion with a mentioning of the necessity of ethical behavior in the workplace, addressing the potential risks of AI usage in professional practices that are not checked and validated properly. More importantly, Cyphert's research reveals the hurriedness of current copyright regimes to truly grasp the functioning capabilities of generative AI, providing plausible and reasonable ways to deal with this emerging opportunity.

Dana Subia Espinoza, 'The Future of Art and Copyright in the World of AI' (2024) 32 Catholic University Journal of Law & Technology 189.

The Future of Art and Copyright in the World of AI[5], Dana Subia Espinoza addresses the question of whether the law of copyright can be deployed to protect AI-generated art by examining the difficulties of using conventional intellectual property principles in connection with newly emerging AI-based technologies. The main point in spinning of such a narrative is that, even though American copyright can be said to have adapted itself historically to the development of new kinds of mediums such as photography, today's expansion of art in the form of AI generation brings about the questions of a legal nature pertaining to issues such as ownership or infringement,

[5] https://heinonline-org-christuniversityncr.knimbus.com/HOL/PDFsearchable?handle=hein.journals/cconsp32&collection=usjournals&section=20&id=&print=section&sectioncount=1&ext=.pdf&nocover=&displa

especially in instances of works that have copyrighted datasets for training without prior consent. With the focus on such key cases as Sawyer Corp. v. Universal City Studios and Campbell v. Acuff-Rose Music, Inc, which have developed AI contours of the present paper, the paper explores the problems of the courts in modern cases involving AI – in identifying transformative and derivative works. The author observes that since LLMs and ISMs produce speech and graphics at speeds which are impossible for humans, the scope of the questions concerning fair use, potentially contributory infringement, and ownership extends wider than the modern legislative framework can resolve. This paper makes the point regarding legal adaptation so as to be able to ensure the protection of the various interests of the artists, the AI creators as well as the consumers without stifling creativity altogether.

INTRODUCTION:

Letting one's guard down in the Digital Age where Truth is Hard to Find

There is hardly any doubt that the world is currently undergoing a great digital transformation, which is being driven by advances in the world of Information and Communication Technologies (ICT). It can be stated that shopping is much easier now more than ever thanks to e-commerce and social interaction more connected than before due to social media, but the importance of the internet reaches far beyond that[6].The combination of globalization, the spread of the internet among the masses, and the rapid development of [7] Social networks and content-sharing sites have created a new reality, even a new information ecosystem that is flooded with content.

Moreover, the high penetration of low-cost mobile devices, including smartphones, tablets, laptops, and digital cameras, has driven up the growth in the production and the distribution of multimedia content even further. In a remarkable way, social networks in the last decade give an opportunity for ordinary users to upload their multimedia works and as a result, such content comes and is accessed in huge numbers each day (Masood et al., 2021). It is, however, one thing to have this degree of access, and quite another to do so returning any useful content as the volume of available information and multimedia content increases, so too do the challenges of differentiating what is real from what is false, thus posing grave threats to public confidence and the quality of information available (Girgis et al., 2018). The inability of most humans to distinguish lies from the truth is not surprising. Studies show that people have merely a 54 percent accuracy of distinguishing between lies or truths (Girgis et al., 2018). The progression of deepfake devices creates a further challenge to the protection of personal privacy, as AI-enabled content manipulation devices can be abused to create highly realistic forgeries. Only recently, the Delhi High Court[8] raised concerns on the “serious menace” posed by deep fake technologies, calling on regulatory action by the government concerning their misuse. Deepfakes have been known to violate people's intellectual property rights, for instance, by depicting someone's image, voice or any other unique identifiers without their consent and claiming the image as theirs. An alteration of an individual's likeness, voice, or other biometric associated with his personality without the consent of the person, deep fakes violate moral rights such as rights of reproduction, distribution, and personality Deep fakes are heavily compounded by techniques coming from newer communication patterns including: fake news such as constructional content which generates false information for the objective of mass element alteration in a context where rise mutual beliefs targeting similar social groups. Journalism, which often times lies at the core of democratic rights, and free speech in general is under legislative siege. Deepfakes provide tools for further erosion of democracy through propaganda techniques empowered by AI: social media convinces millions that these techniques work A neural network that specializes in deepfakes Fakes operates on deep learning models called GANs, which stands for Generative Adversarial Networks[9]. To construct genuine content, GANs[10] involve two networks units: one is

---

[6] Masood et al, 'Social Media and Deepfake Technologies' (2021) *Journal of Media and Communication Studies.*

[7] Girgis et al, 'The Role of Digital Media in the Spread of Misinformation' (2018) Journal of CyberPsychology.

[8] Delhi court,'The Role Of Digital Media in the Spread of Misinformation'(2018) Journal CyberPsychology

[9] See Girgis et al (n 2).

[10] Generative Adversarial Networks (GANs) are dual neural network models widely used in the creation of deepfakes. For an overview, see Ian Goodfellow et al, 'Generative Adversarial Nets' (2014) Proceedings of the International Conference on Neural Information Processing Systems.

producer, to develop artificial information secondly[11] An appraiser - oversees what the creator builds and approves substandard creations if the end target deviates from the acceptable standard. Repeated practices refine the result closer to the target of generating a believable outcome deep fakes hardly retain any features from the original media content while slowly growing up integrated into them from various angles producing a believable original look Despite the neutralization of security this is believed that the time of deep fake may begin the exposure of scripted concepts these concepts always operate on three planes, narrating ideas, analyzing sub graphs, generating new beliefs and creating new conceptual ideas encompassing them for future awakening. Deepfake advocates often argue that the technique can be used positively such as voice fillers in video edit WhichIntegrated into tools makes it possible to drastically alter society for the worse.The ramifications are far-reaching and impact public confidence in the media, open new doors for identity theft, and legal systems that seem unable to adapt to the pace of technological change.

RESEARCH PROBLEM:

The problem that is the focal point of this paper, on the other hand, is the threat that deepfakes pose on the intellectual property (IP) and privacy laws. Deepfakes which are made with the help of advanced artificial intelligence algorithms such as generative adversarial networks enable people to create hyper-realistic audios and videos of other people without their permission. This is especially problematic to the existing IP systems as it creates copyright thresholds to be crossed since synthesized material has the potential of using existing or pre-existing works without permission[12]. Furthermore, deepfake technology's implications with the use of an individual's[13] likenesses without consent is also detrimental in that it creates an avenue for identity theft, reputation tarnishing, and emotional abuse[14]. Existing laws, such as the Information[15] The Technology Act of India and privacy statutes of Europe and the U.S. countries, are not well positioned to deal with such issues. In this study, these weaknesses, the current legal framework and its shortcomings will be reviewed, as well as how deepfake technology could be curtailed, will be discussed.

RESEARCH QUESTION:

1. Whether there are clear guidelines defining the responsibilities and rights of AI developers and users when it comes to copyright infringement involving AI-generated works?

2. Whether deepfakes contribute to the erosion of intellectual property rights and copyrights, undermining creators' protections and challenging the integrity of original content in the digital landscape?

3. Whether current IP and privacy laws have significant limitations in effectively managing the challenges posed by deepfake technologies?

OBJECTIVE AND SCOPE OF STUDY:

This paper seeks not only to highlight existing problems posed by deep fakes but also to examine how the existing intellectual property (IP) as well as privacy regimes may have relevant but unexplored regulatory gaps. More specifically, it intends to examine the legal protection measures that have been put in place in regard to creations, individuals, and public figures and establish if they are adequate. The concept in this research includes, literature review, literature review of cases as well as legal frameworks around the world including the US, Europe and India. These issues include how copyright is disturbed by deepfake technologies and whether deepfake

[11] See Masood et al (n 1).

[12] European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[13] On the application of AI in digital manipulation and its social impacts, see Hannah Fry, Hello World: Being Human in the Age of Algorithms (Penguin Books 2018).

[14] (General Data Protection Regulation) [2016] OJ L119/1

[15] On the application of AI in digital manipulation and its social impacts, see Hannah Fry, Hello World: Being Human in the Age of Algorithms (Penguin Books 2018).

technologies can be adequately protected within the common legal frameworks of copyright existing today. The paper will analyze current privacy laws to determine whether they are sufficient to protect people against the misuse of their images through deepfake applications. In order to meet these objectives, the paper suggests various proposals. The first proposal relates to the enactment of special legislation targeting deep fakes that will provide definitions, standards for consent and measures for abuse of deep fakes. Unquestionably important is the need to revise the law and reinforce copyright provisions which will prevent the generation by unauthorized AI of content which amounts to reproduction of original works as well as the need to review the fair use doctrine in line with AI technologies. Additionally, there is a need to strengthen privacy risks with the regulation of the usage of people's images in the digital space for commercial purposes without permission being made mandatory. Awareness campaigns among the individuals to sensitize them on the dangers posed by deepfakes as well as how to legally protect themselves from the technology should also be put in place. Finally, the promotion of cooperation between jurisdictions will facilitate the engagement of jurisdictions in the development of regulations that are consistent with the understanding of the global nature of digital items including deepfakes and efficient enforcement and access to justice across borders. These objectives, in so far as these solutions are also implemented, this research seeks to address, will assist in the development of appropriate legal and administrative measures that will guarantee the protection of intellectual property and privacy rights in the face of the growing dominance of AI content generation in all areas of life.

SIGNIFICANCE OF STUDY:

Confronting the legal implications surrounding deepfakes is a matter that can be relevant to the improvement of international legal frameworks and policy formulation for one reason which is very critical. Technology is ever improving and deepfakes are a potential threat not only to the right to privacy and right to identity but also the concept of intellectual property rights. There is however the threat of the use of deepfakes that has been developed to create close to perfect representation of people for purposes where entertainment or art is not the intended goal, rather it is to spread disinformation and other forms of maltreatment in the digital space. Thus, non-adjustment of the august legal frameworks to these developments can drastically reduce the trust of people over the information and communication systems which in return has the potential to undermine democracy, societal order, and violation of IP rights. This current research borrows heavily from previous works as it stresses the urgent action that is needed to enforce law that needs to match the rapid growth of AI technologies. Most of the present legal frameworks in a good number of jurisdictions including US, Europe, and India were never crafted to deal with the challenges imposed by the presence of deepfake technologies. In the absence of legal protection, copyright hacking, and impersonation is likely to become the order of the day for many creators and individuals which will greatly affect digital content creation.In addition, abuse of deepfakes can cause further damage through stalking and political interference which requires comprehensive regulation and understanding of the policymakers. As this survey highlights the interdependence of localized digital networks, it too brings to light the need for cooperation among states in crafting legal solutions to the deepfake issue, whose scope is predominantly international in character. Policymakers can actively participate and work together towards the development of consistent regulations that would allow protecting individuals and at the same time allow innovation in a just and non-infringing manner. Focusing on the relationship between the practice and the regulatory governance, this study demonstrates how legal and policymaking processes respond to the challenges posed by a particular technological progress, to ensure that the resulting systems and policies are relevant even in the face of future changes. In the end, however, the paper proposes a different legislative policy which accommodates the influence of AI and digital content alteration on society – that of creativity, consumers' needs and societal norms.

RESEARCH METHODOLOGY:

This study is analytical and focused on comparative research in order to understand how deepfake technologies impact intellectual property (IP) rights and privacy laws. As the focus is on qualitative scholarship, the study studies legal texts, the experiences of cases, and literature to analyze the situation with regulations concerning the deepfake and their efficiency. Rather, the research compares the approaches undertaken in different regions

including the United States, Europe and India and the challenges faced in relation to the legal aspects of deepfakes, with the view of making suggestions on what works and what does not. Beyond these, the research will seek to use knowledge obtained from webinars covering issues such as digital twins, deepfake, and risks to personality rights from a legal perspective as well as the concept of digital afterlife and fraud prevention. Such webinars will provide up to date views of the audience from legal, technological and ethical perspectives enhancing the analysis of the study with practical implications and recent developments. Primary data sources will include legislative documents such as Indian Information Technology Act 2000, and EU General Data Protection Regulation (GDPR) and other case laws that illustrate both the practice and the shortcomings of the law.Different angles on the role of deepfakes in the infringement of IP rights and privacy will also be sought out in secondary sources including, but not limited to, legal articles, commentaries, and academic papers. Adopting this approach allows for considering the relationship between the development of technology and the response of law to such advancement which in turn helps in the search for effective ways to strengthen the safeguards of creators and people against the abuse of deepfake technology.

LIMITATION OF STUDY:

There are several limitations of this study which may influence the extent and the application of its results. Firstly, the case studies concentrate on the United States, Europe, and India; making the findings not readily transferable since legal approaches to deepfake technologies may differ across jurisdictions. Also, this study may be limited in certain respects due to the absence of definite empirical data on the effects of deepfakes in practice since many problems are still developing and complete studies measuring the risk to intellectual property rights and privacy, for example, are quite rare. Thirdly, it is true that the analysis employs relevant statutes and case law, but these are most probably not the latest changes or interpretations of the courts which may have an effect on the legal regulation. Finally, the fast pace of advancements in AI devices and deepfake technologies also renders the application of such legal frameworks ineffective because they would not be able to catch up with the changes in technology. All these limitations notwithstanding, this research hopes to help in offering meaningful insights and suggestions in the improvement of the legal measures for dealing with the misuse of deepfake technologies.

DEEPFAKES:

The Legal and Ethical Issues

Deepfakes are media outlets that create realistic-looking but fake images of a person's likeness through digital modifications. The technology that underpins this phenomenon is predominantly artificial intelligence (AI) algorithms[16] like Generative Adversarial Networks (GANs)[17]. A GAN is made up of two neural networks: one called the generator and another called the discriminator and these two networks enhance one another's ability to produce realistic images or videos. The generator's role is to construct fake material while the discriminator's role is to measure authenticity, and through reiterations of improvement, the fakes are almost identical to the genuine media. Though this technology can generate creative works, it also has dire ramifications for one's intellectual property (IP) and personal privacy.

Privacy Issues Related to Deepfakes

In this regard deepfakes depict a new threats for privacy these include, impersonation, emotional suffering and alteration of someone's reputation[18]. One of the well-known cases is the recent distribution of deepfake nudes these are used in blackmail and harassment scenarios that have increased against already marginalized women.To illustrate, the National Center for Digital Investigations (NCDOI) provides ample evidence of cases where abusers have placed the faces of people on pornographic images without their consent which leads to the

[16] Hannah Fry, *Hello World: Being Human in the Age of Algorithms* (Penguin Books 2018).

[17] Ian Goodfellow et al, 'Generative Adversarial Nets' (2014) Proceedings of the International Conference on Neural Information Processing Systems.

[18] National Center for Digital Investigations, 'Report on the Misuse of Deepfake Technology in Digital Harassment Cases' (2023).

exposure of them on the public forums causing severe distress. Because, in some jurisdictions, such as the USA, such actions may result in legal action for defamation, undesired emotional distress, and violation of privacy laws. For example, the[19] BC Intimate Images Protection Act provides a cause of action for nudity or near nudity, even when such depictions have been modified, which is the area of law available to plaintiff's victimized in law. In India[20], while the protective mechanisms are not exhaustive, there is a gradual shift towards being aware of the need for such regulatory structures to address these novel challenges. Despite these challenges, the FBI has revealed instances when con artists operated using the photographs and videos in the public domain for deepfakes in order to further their blackmail schemes[21]. With this level of digital manipulation, the public can be led to believe that individuals were captured in compromising positions that could severely damage their reputation and cause emotional pain[22]. These instances urgently point to the existence of an effective comprehensive plan of legal reliefs that would be able to combat the violations of the deepfake technology on the privacy of individuals.

Ethical Issues

The legal issues surrounding the generating and circulating of deepfakes do not constitute the major ethical issues involved in the use of the technology.The alteration of people's appearances raises fundamental issues with respect to consent, agency and the ethical role of the artists and distributors of such content. The use of AI to create sexual material in the absence of a person's consent violates the social concept of private circles and respect. Furthermore, the making of deepfakes adds another layer to the crisis of trust where still pictures and moving images are not genuine representations of the truth[23]. The lack of trust in what deep fakes are increases the issues which are tilted towards journalism, citizen engagement and democratic systems. The legal frameworks within which the creators of deep fakes operate should be more than just laws, the ethical considerations extend to the protection of individuals from violation of rights and protecting the content from distortion. In a nutshell, it is important to note that the use of deepfakes raises legal and ethical challenges which are crucial in as far as safeguarding intellectual property of individuals and privacy matters. The call for regulation is required because as technology advances, the legal means of addressing the concerns posed by deep fakes ought to ensure stability in ingenuity pertaining to AI. The subject seeks to address the issues of lack of regulation and how they can be dealt with in order to protect both the creators and the individuals in the myriad realities of the digital world

ANALYSIS OF CURRENT LEGAL FRAMEWORKS:

Comparison of Relevant Laws and Their Implementation within Legal Systems of Member States Analysis of Current Legal Frameworks International and Regional Laws United States In the United States, the prevailing conditions concerning deepfakes, as well as the associated practices in IP (intellectual property) are fundamentally embedded in copyright and its legislative systems such as the Copyright Act enacted in the year 1976[24]. With the advancement of deepfake technology, the concern regarding the loss of IP rights gradually increases,since the likeness of people can be used to create derivative works without their consent. Courts are held in view of IP rights and new technologies such as in the case of Brown v. Electronic Arts[25], where athletic imagery was used without consent, so the defense is a right of publicity. Yet the depolarized legal networks have no definitive clauses which can address the issues related to deep fakes, hence protection for content and sometimes individual creators is missing. Nevertheless, according to California's AB 730[26],it is unlawful to misuse, abuse or use deepfake inappropriately, as well as without consent of the people involved in the legislative

[19] BC Intimate Images Protection Act, SBC 2021, c 20 (Canada).

[20] Information Technology Act 2000 (India), amended in 2008

[21] Federal Bureau of Investigation (FBI), 'Cyber Crime Report 2023' (2023).

[22] See Fry (n 2).

[23] On ethical concerns with AI-generated deepfakes, see Shashi Tharoor, 'Copyright and Ethical Standards in the Age of AI' (2023) International Journal of Intellectual Property Law.

[24] Copyright Act 1976 (US), Pub L No 94-553, 90 Stat 2541.

[25] *Brown v Electronic Arts*, Inc No 2:09-cv-01598-FMC-RZ (CD Cal Sept 23, 2009).

[26] California AB 730 (2019) (prohibiting the use of manipulated media without consent for purposes of deception in political or commercial contexts)

frame. Interestingly, although these initiatives are a positive development, so far we lack federal laws that best deal with the complexities involved and copyright infringement aspects related with the deepfake technology. In the European Union[27], the copyright directive (2019) along with the GDPR has derivative legislation that addresses copyright infringement and issues between copyright and data.

The aim behind the Copyright Directive is to enhance the creators' rights and assist in coping with the problems created by the online content sharing platforms. But the developing technology of deepfake makes it possible to use video clips and likenesses of real people in a way that infringes upon the principles of fair and transformative use. For example, if a deepfake transfer film places a person's face on another body but the source remains not too distant,such work would be likely infringing copyright. Other real cases, such as the case of Kraftwerk v. Tobias R. (2012), provide evidence of the enforcement of copyright principles, more precisely, anti-sampling principles. In this situation, the German electronic musical group Kraftwerk was able to win a court judgment in which it claimed that its song had been illegally used in the composition of a hip-hop performer. This case illustrates the legal difficulties that creators encounter when their original works are distorted or utilized without permission and points to the urgent need for new laws concerning deepfake technology. India's khmer workings. India's intellectual property regime to the deepest fake is the copyright act 1957, which gives protection to original literary, dramatic, musical and artistic work[28]. However, as deepfake technology becomes more sophisticated, the laws that are currently in place become outdated and do not address the issues that are associated with it in the first place.

The unauthorized artificial alteration of materials by means of AI that allows fake content to be created using an individual's likeness without consent constitutes a violation of their possible copyright and moral rights[29], which might have the effect of bringing them damage to their reputation, etc[30]. One such case is the recent evidence involving the generation of more than one video deepfake of a person without consent, leading to claims that there should be more measures designed to deal with such atrocities. Additionally, the Draft Personal Data Protection Bill 2019, Although it aims at augmenting data protection rights, it does not provide adequate attention to the issues of copyright that arise from AI content[31]. Such intricacies of deepfake technology amplify the need for the relevant changes to be made to the copyright laws in India so as the perpetration of such infringements that stem from the manipulation of digital images does not occur.

Comparative Analysis

A comparative analysis of the legal frameworks in the United States, the European Union countries and India for the same issue of using deepfake and other technologies shows that there is no or very little provision for IP rights. The US legal framework has to a reasonable extent been able to progress through focused legislation, however the splintered nature of the laws has failed to address many concerns[32]. The efforts of the EU through the Copyright Directive is a step in the right direction, however, deepfake technology is likely to be adversely complicated by the various complexities that it will bring about. In India, there is a need for more provisions to be made in the existing Copyright Act so that deeper technologies further aggravate the existing challenges brought about by AI generated content.

---

[27] Directive (EU) 2019/790 on Copyright and Related Rights in the Digital Single Market [2019] OJ L130/92.

[28] *Kraftwerk v Tobias R* (2012) German Federal Court of Justice (addressing the unauthorized sampling of Kraftwerk's music).

[29] Copyright Act 1957 (India), as amended 2012.

[30] Draft Personal Data Protection Bill 2019 (India).

[31] National Center for Digital Investigations, 'Report on Deepfake Technology and Privacy Concerns' (2023).

[32] European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

Social Engineering Scams and Copyright Erosion

The sinking of IP rights and copyright is even more deepened by the social engineering scams that use the images of the people who fell as their subjects through the utilization of deepfake technology. There are numerous ways in which this type of fraud is committed. A scammer can, for instance, forge documents with the assistance of AI and create a realistic environment where this fraud will go unnoticed[33]. Scalper B can impersonate vendor A seeking payment by overly assisting the vendor, which will expose B into wire transfer fraud in which vendor impersonation drives the fraudster to redirect payments to themselves instead of receiving payment for goods via shipment. As deepfake technology becomes more accessible and advanced, the potential for the breaching of copyright or even utilizing a person's likeness for commercial purposes will increase significantly. Legal responses to these threats need to be forward looking and factor new trends of deepfake technologies in content creation and distribution. Remember, deep fakes have a lot of impact, here strengthening verification procedures, heightening penalties for the violations, and consumer education on the dangers of using deep fakes will provide great efforts towards countering loss of IP rights and ensuring stronger legal response to the issues of the digital world. In conclusion, as the terrain of digital content continues to expand, the circumstances of deepfakes, copyright, and IP will need continual scrutiny to ascertain their place within the law.Practical cases, as well as new emerging threats, point out the dire need for efficient mechanisms that protect individual and creator rights in this ever-manipulated ZETA space.

IPR AND DEEPFAKE COPYRIGHT ISSUES:

The development of deepfake technology poses serious problems to the established copyright law, especially with respect to generative AI, as some scholars such as Cyphert and Rosati discuss. It is important to note, however, that the very core of copyright law is based on the existence of an originality concept. But then, the gray area of deepfakes often creates uncertainty on the issues of originality and authorship[34]. A deep fake is usually said to involve the processes of editing existing media (images, video, sound) by means of algorithms to create new content that may be altered from the original. This begs the question of how far can deep fakes go and still be regarded as original content which can have copyright protection.Cyphert's investigation brings to attention what seems to be a paradox with AI generators; they only consider inputs which are derived from other existent content which tends to negate the idea of authorship. The majority of these deepfakes created do[35], on the other hand, depend on large databases containing copyright materials, and therefore copyright violation does come into consideration. A copyright deep fake that closely resembles an original work may violate the right holder's exclusive rights. In addition, Rosati's remarks underline more strongly that the change of the original subject matter in question shall reach quite a degree of originality to qualify for the protection under the copyright law[36]. This presents a difficulty that deepfakes can distort content so that it does not fulfill the definition of originality yet at the same time, reproduce new forms that can be considered as violating the rights of the original creators.

Trademark and Right of Publicity

Above the copyright matters, it has been established that deep-fakes are also an intrinsic hazard to trademark rights as well as the right of publicity. The right of publicity enables an individual to earn either money or income from the commercial utilization of his/her photo, name or even persona and that can be violated through deep-fakes. If one deep-fake video uses likeness of a star without permission to promote a product or service, then such a depiction is not only identity theft of the superstar but also could mislead the customers and encroach on the trademark rights for the respect of the brand. Hannah Montana and the deepfake videos where Miley Cyrus's image has been misused and without authorization are perfect examples of these kinds of manipulations

---

[33] Amy B Cyphert, 'Generative AI, Plagiarism, and Copyright Infringement in Legal Documents' (2024) 25 Minn J Law Sci & Tech 49.

[34] Eleonora Rosati, 'Infringing AI: Liability for AI-Generated Outputs Under International, EU, and UK Copyright Law' (forthcoming 2024) European Journal of Risk Regulation.

[35] Shashi Tharoor, 'Copyright and Ethical Standards in the Age of AI' (2023) *International Journal of Intellectual Property Law*

[36] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 UC Davis L Rev 399.

adversely affecting the publicity rights as well as the trademark rights. The creation of false endorsements using Deep fake technology is also problematic because it creates brand confusion, which is a primary objective of trademark law. Currently, there is indeed a new accelerating tension that is brought about by technology evolution, which is the need for legislation to catch up with the new needs on defining the relationship that exists between these deep fakes and the existing trademark or right of publicity.

Legal Liability

As it pertains to a major issue, there is the question of who is liable for the wrongful acts of deepfakes: only those who created the images or else it should be those who manufactured and propagated the deepfake-generating software[37]. As the availability of deepfake technology increases, its possible abuse increases and thus, there are ethical and legal concerns for the software developers of the creation of such tools. The question is raised: what is the limit of responsibility for those who provide means of production of deepfakes? On one hand, holding deepfake software creators liable will incentivize them to act responsibly and enforce limits on their designs. On the other hand, the fears of inhibiting innovative development and basic freedom of speech are real. The current elements of compliance of the existing legal frameworks are likely to contain some limitations regarding the specifics of the liability in this case leading to a lack of accountability concerning adverse use of deepfake technology. This calls for a review of the laws in place and perhaps the introduction of new laws to be set out which highlight the obligations of parties engaged in the production and dissemination of deep fake material.

PROPOSED LEGAL AND POLICY SOLUTIONS:

Strengthening Existing Frameworks

Revisiting some existing legal structures such as copyright and privacy laws would be necessary with their apparent deficiencies in addressing the role of AI in content generation. In particular, it has been noticed that in the U.S., the existing Copyright Act of 1976 only applies to those works that are composed by a natural individual[38]. However, this allows substantial loopholes when it comes to works such as a novel or a painting created by an AI program. Reviewing regulations of this kind would open the door for joint or co-creation whereby humans are actively involved in the creative process. For instance, in the Thaler v. Copyright Office case, an AI's work is not copyrighted simply due to the fact that it does not have human authors, therefore, proponents of legislation should try to enforce laws that will establish criteria for assigning authorship to works that use artificially assisted creation.

International Coordination

Because of the global character of digital media, it is necessary to have an international approach if reasonable regulation is to be achieved[39]. This is partly evident when considering the image of the Berne Convention which makes it possible for countries that signed it to enjoy some level of equality in their countries'[40] copyright levels but doesn't extend to AI or synthetic content yet. For example, it seems appropriate to broaden such frameworks to address AI-related issues so that if deepfake technology used in one part of the world encroaches the rights of an actor in another, there are frameworks in place that both parties can use to deal with the matter. This type of cooperation could stop offenders from taking advantage of jurisdictional loopholes in order to distribute harmful content around the world.

---

[37] Authors Guild v OpenAI (2023) 1st Circuit Court Case No. 23-1122.

[38] Sam Mishra, 'Human Authorship in AI-Generated Content and Copyright Law' in Panda Law Review (2024) 18 *Panda Law Journal*

[39] Anupam Pandey, 'Legal Implications of AI in Content Creation under the Copyright Act of India' (2023) 13 Indian Journal of Intellectual Property Law 112.

[40] Anupam Pandey, 'Proposed Legislative Reforms for AI and Copyright in India' (2024) Indian *J IP Law.*

Technological Countermeasures:

Technological solutions can assist in the management and detection of deepfake content. For example, tools like the ones used by Deepware or Truepic come in handy when aiding in the spotting of altered videos as well as images among their customers. Microsoft's Project Origin, a form of digital watermarking, embeds markers in media claiming its source so that tampering is apparent. A similar form is in blockchain as it can record the history of a digital asset creation and even modifications, such as verifying an NFT's history[41]. All of these tools work together to provide a seamless transition for the verification process in guaranteeing more complicated structures in regards to content legitimacy against fake media for the safety of consumers and creators.

FUTURE DIRECTIONS:

The evolution of the new generation technologies undoubtedly has an impact on the growing erosion of trust in digital content, yes, such changes in society in combination with the processes of the evolution of technology can also have a negative impact on democracy possibilities through the spreading of misinformation[42]. The legal order is under pressure to shift the paradigm to be able to promote innovative systems, whilst maintaining avenues of accountability. A possible future impact suggests a wider occurrence of litigation over rights of the digital realm whilst suggesting a stronger influence of the judiciary over law making relating to this area.

REVIEWS AND INSIGHTS:

Human Authorship and Copyright: Mishra at Panda Law explains that in many Western jurisdictions, including the US and EU, for a person to enjoy the protection of copyright there must be human authorship of the work[43]. India's position on this matter is on the same lane as it does not recognize AI as an author when contemporary copyright statutes are applicable. This begs the question of how is the right to be assigned if AI creates the content to a greater degree.

Fair-Use Considerations: As Mukherjee points out, AI users are perhaps the most exposed when it comes to terms most AI's terms of service where so many responsibilities are placed on the users not to infringe. This burden may transfer to those who are creating the AI thereby creating a more responsible framework when the AI is being trained. Anupam Pandey underlines that currently[44] section 14 and section 51 of the Copyright Act of India exposes the frameworks on how AI agnostic limitations can be infringed; the only problem is application of these limitations to AI content generation.

Judicial Precedents and Global Perspectives: Other countries appear to have differing views on this so such cases as Authors Guild v Open AI and China's enabling AI authorship but does provide for human supervision. The above situations indicate India and other jurisdictions should explore if laws should be modified to recognize hybrid authorship models or retain the current requirement as per the person's involvement.

Ethical and Universal Standards: Shashi Tharoor an expert opinion maker asserts that it is necessary for a standard copyright that not only deals with AI related concerns but also all other fields to protect creators at a wider scale. Ethical instructions that should be implemented include obtaining consent, being transparent, fair licensing payments for AI training using copyrighted material and empower economic considerations in ensuring that creations rights are observed.

Compensation and Licensing Models: With regard to AI training, AI developers, users, and AI content creators' interests should be protected. Copyright fees and licensing fees practiced in other creative fields could reflect those used in publishing and generate funds for creators.

---

[41] Microsoft, 'Project Origin: Digital Content Provenance Initiative' (2023) https://www.microsoft.com/projectorigin accessed 3 November 2024.

[42] Berne Convention for the Protection of Literary and Artistic Works (9 September 1886, as amended on 28 September 1979).

[43] Deepware, 'AI-Powered Deepfake Detection Tools' (2023) https://deepware.ai accessed 3 November 2024.

[44] See Cyphert (n 10); Rosati (n 11); Mishra (n 15)

Clear Legislative Reforms: Senior IP practitioner Anupam Pandey recommends the introduction of an Act on AI with provisions on the rights and obligations of AI developers, users and content authors. Doing so would provide faster resolution alternatives and reduce the need for an exhaustive court process.

CONCLUSION AND RECOMMENDATIONS:

To conclude, this research work has emphasized the major threats that deepfake technology brings to the intellectual property (IP) rights and privacy laws. The analysis indicated that the present legal provisions existing in jurisdictions such as the US, Europe, and India are insufficiently dealt with the advanced nature of deepfakes and hence there are deficiencies in legal protection against uses desconocidos which encompass the use of an individual's image and the infringement of copyright. The study stressed on the likelihood of harm that creeps in including impersonation, unfair loss of good name and the violation of rights of the creators. Last but not least, the current acts for example that of US Copyright Act of 1976 and the Indian Copyright Act of 1957 bear glaring gaps by not able to cover the concept of AI and its generate content thereby justifying the need for change in the law.It is clear that there is a need to promote legislative and regulatory developments. In the same context, technologically enhanced deception has been evolving with time leading to more danger towards the people and truthfulness of the digital world. There is a gap that desperately needs to be filled with appropriate laws that would define the scope of AI creators and users' roles and obligations, enhance IP protection, and establish the requirements of consent and responsibility. Comprehensive, pro-active legal and policy changes are, therefore, the best way through which societies can prevent the abuse of deepfakes while allowing space for development that is consistent with human rights and confidence in digital media.

REFERENCES:

Eleonora Rosati, 'Infringing AI: Liability for AI-Generated Outputs Under International, EU, and UK Copyright Law' (forthcoming, European Journal of Risk Regulation, 2024).

S. Alex Yang and Angela Huyue Zhang, 'Generative AI and Copyright: A Dynamic Perspective' (forthcoming, manuscript, London Business School and University of Hong Kong).

Wenqing Zhao, 'AI Art, Machine Authorship, and Copyright Laws' (2020) 12 American University Intellectual Property Brief 1.

Amy B. Cyphert, 'Generative AI, Plagiarism, and Copyright Infringement in Legal Documents' (2024) 25 Minnesota Journal of Law, Science & Technology 49.

Dana Subia Espinoza, 'The Future of Art and Copyright in the World of AI' (2024) 32 Catholic University Journal of Law & Technology 189.

Masood et al., 'A review on emerging artificial intelligence (AI) techniques for air pollution forecasting: Fundamentals, application and performance' (2021) Elsevier https://www.sciencedirect.com/science/article/abs/pii/S0959652621032613

Girgis et al., 'Efficacy and safety of anti-inflammatory agents in treatment of psychotic disorders – A comprehensive systematic review and meta-analysis' (2018) [Elsevier]https://www.sciencedirect.com/science/article/pii/S0889159120311557Mishra at Panda Law, 'AI's Right to Copy',https://law.asia/generative-ai-copyright-law

Shashi Tharoor, 'When AI Shashi Tharoor Interviewed MP Shashi Tharoor Deepfakes to possibilities,know what happened,

https://tech.hindustantimes.com/tech/news/when-ai-shashi-tharoor-interviewed-mp-shashi-tharoo r-deepfakes-to-possibilities-know-what-happened-71707640298072.html

ADMISSIBILITY OF DIGITAL EVIDENCE: CHALLENGES AND PERSPECTIVES IN THE ERA OF NEW CRIMINAL LAWS

Keshav Jha
Assistant Professor, Medicaps University, Indore M.P

Dr. Priyamvada Tiwari
Associate Professor & HOD Medicaps University, Indore M.P

ABSTRACT

The old criminal laws have been replaced with new ones, making the handling of digital evidence in legal cases more important than ever. Digital evidence, like emails, text messages, social media posts, and digital files, plays a big role in both crimes and law enforcement today. For digital evidence to be used in court, it must meet traditional rules such as being relevant, authentic, and trustworthy.

However, there are many challenges when it comes to digital evidence. For example, it's important to maintain a proper chain of custody, which means tracking who has handled the evidence to make sure it hasn't been tampered with. Verifying the authenticity of digital files, like checking metadata or timestamps, is also a challenge. Sometimes, the evidence is stored in another country, creating jurisdictional problems and the need for international cooperation to retrieve and verify it. Privacy laws, like the GDPR, add complexity by requiring a balance between accessing digital evidence and protecting personal privacy.

The fast pace of technological advancements makes things even harder, as courts and law enforcement have to keep up with new devices, platforms, and encryption techniques. Additionally, expert testimony in digital forensics is often needed, but experts may have different opinions on how to interpret the evidence.

To address these issues, new criminal laws and standards for digital forensics are being created, offering clearer guidelines for handling digital evidence. This paper will look at the challenges and different views on the admissibility of digital evidence, especially with today's technology and the new criminal laws in place.

Key words: *Digital Evidence, Technology, Criminal Law, Admissibility, Privacy.*

Introduction

The introduction of computers in India in 1969 marked the beginning of a digital revolution that has transformed every aspect of society. The widespread availability of computers, smartphones, and internet connectivity has not only facilitated convenience but has also introduced new forms of criminal activity. Just as criminals leave physical traces at crime scenes, they also leave digital footprints, which can be used as evidence in legal proceedings.

To regulate digital transactions and ensure the admissibility of electronic records, the Information Technology Act of 2000 was enacted. This law, along with amendments to the Indian Evidence Act, the Indian Penal Code, and the Banker's Book Evidence Act, laid the foundation for recognizing digital evidence in Indian courts. Over time, digital evidence has gained prominence in investigations, as data from electronic devices, cloud storage, and social media platforms often play a crucial role in legal cases.

For digital evidence to be considered valid in court, it must meet three essential criteria:

1. **Relevance** – The evidence must be directly connected to the case.
2. **Authenticity** – It must be proven that the evidence has not been altered or manipulated.
3. **Integrity** – The evidence must be preserved in its original state without unauthorized modifications.

As technology continues to evolve, legal systems worldwide face the challenge of ensuring that digital evidence is handled with fairness and accuracy while maintaining public trust.

Digital Evidence Under Previous Criminal Laws

Section 65B of the Indian Evidence Act

Previously, Section 65B of the Indian Evidence Act governed the admissibility of electronic records. According to this provision, digital evidence had to meet specific conditions to be accepted in court. One such requirement was obtaining a certificate under Section 65B(4), confirming the authenticity of the electronic record and detailing the system used to generate it.

The Supreme Court has issued significant rulings regarding digital evidence. In **State (NCT of Delhi) v. Navjot Sandhu**[1], the court initially allowed electronic evidence even without a Section 65B certificate. However, this ruling was later overruled in **Anvar P.V. v. P.K. Basheer**[2], which emphasized that electronic records must strictly comply with Section 65B to be admissible. The court clarified that oral testimony cannot be used to validate digital evidence unless the requirements of Section 65B are fulfilled.

The principle established in **Anvar** remains binding, reinforcing that compliance with Section 65B is a mandatory prerequisite for admitting electronic records in court.

Digital Evidence Under New Criminal Laws

With the introduction of the Bharatiya Sakshya Adhiniyam (BSA), significant changes have been made to the legal framework governing electronic evidence. Some of these changes provide clarity, while others introduce new complexities.

Key changes include:

1. **Expanded Definition of Documents** – Section 2(1)(d) of the BSA now explicitly includes electronic and digital records as documents, broadening their legal recognition.

2. **Revised Procedural Requirements** – Sections 61 to 63 of the BSA correspond to Sections 65A and 65B of the Indian Evidence Act, ensuring that electronic records have the same evidentiary value as physical documents. However, conflicting provisions in Section 57 of the BSA create ambiguity regarding the classification of certain digital records as primary evidence.

3. **Proper Custody Concerns** – Explanation 5 of Section 57 suggests that digital records may be considered primary evidence if retrieved from "proper custody," but the term remains undefined, leading to uncertainty in its legal interpretation.

Challenges in Admitting Digital Evidence

Despite the revised legal framework, several challenges persist:

1. **Limited Technical Expertise** – Many forensic labs lack adequate resources and trained personnel to handle digital evidence efficiently.

2. **Managing Large Data Volumes** – The increasing use of digital devices in criminal activities results in vast amounts of data that must be examined, verified, and certified, posing logistical difficulties.

3. **Timely Certification** – Requiring expert certification for all digital evidence may slow down legal proceedings. It has been suggested that certification should be mandatory only when the authenticity of the evidence is disputed.

---

[1] AIR 2005 11 SCC 600

[2] AIR 2015 SCW 5695

To address these issues, a two-pronged approach is necessary:

- Strengthening forensic capabilities and resources.
- Conducting training programs for private organizations and law enforcement agencies on digital evidence management.

Conclusion

Digital evidence is playing an increasingly vital role in modern legal proceedings. While new laws like the BSA, BNS, and BNSS aim to align legal practices with technological advancements, challenges related to procedural clarity, jurisdiction, and technical expertise remain. To ensure the fair and effective use of digital evidence, legal professionals, lawmakers, and forensic experts must collaborate to develop standardized practices. By embracing innovation and enhancing digital forensic expertise, the judicial system can maintain procedural integrity while adapting to the evolving digital landscape.

Printed, Published and owned by Amit Gupta. Printed at Shubham Enterprises, 129, DSIDC Sheds, Okhla Indl. Area, Phase-I, New Delhi - 110020.
Published at JIMS Engineering Management Technical Campus 48/4, Knowledge Park-III, Greater Noida. Editor: Amit Gupta