Asst. Prof. Sanya D. Kishwar, Jindal Global Law School

Sadqua Khatoon, Student, Faculty of Law, Aligarh Muslim University

By Lex Vedika Blog

Date:- 01 April 2025

Large Language Models have brought with them an onset of technological revolution. Be it OpenAI’s ChatGPT, Google’s PaLM 2 or Microsoft’s Copilot, all of them have find their way into the field of academic and miscellaneous writings. Be it a text that we need to drop to our friend or an essay that we need to turn in overnight, LLMs turn to our rescue. There is certainly a limit with regard to efficiency in some fields of research that LLMs face owing to hallucinations, where AI produces false or misleading information. Particularly in legal and academic contexts, reliance on LLMs for research and drafting is cautioned against. However, we still end up witnessing instances where judges rely on Chat-GPT for drafting bail orders or there are instances of ‘jailbreaking’ where the bypass of an LLM’s ethical safety restriction results due to leaking of confidential legal information.[1]

While such automated content generation is undoubtedly helpful, the increased usage of LLMs give rise to a very creator. Additionally, another important legal question pertains to whether AI creators need licenses for employing copyrighted works in training data and if so, whether outputs created by AI qualify as derivative works.

Most common law jurisdictions follow the doctrine of sweat of brow, which suggests that the protection of copyright could extend to the hard work and efforts put in creating something, even it was not particularly original.[2] Therefore, the command prompt which is supplied could raise a claim to be the rightful creator since it takes labour and skill to draft a prompt command. However, it is not just the command prompt that leads to the generation of the result.

LLMs are modelled on massive data sets containing the public domain. These are mostly scraped from websites. Although AI businesses claim that their models do not retain literal copies of texts but instead produce probabilistic responses, research has proven that LLMs can memorise and recite verbatim passages from copyrighted materials.[3] This demonstration of the capacity of LLMs to create copyrighted material without permission poses numerous legal issues. More specifically, these issues also concern with the reproduction, adaptation, and derivation of works through web scraping.[4]

Copyright law across jurisdictions bestows authors exclusive control over their works, and any use by LLMs without authorisation may violate such rights, more so, if the web scrapping breached the exclusive license of a publishing house to reproduce, store or disseminate the work. It is interesting to note that the developers of AI often invoke the “fair use” doctrine as a defence, arguing that training AI on copyrighted materials constitutes a transformative use.[5] However, courts have yet to provide a definitive ruling in this regard, leaving this as an unresolved legal question. Increase in the number of high-profile lawsuits underlining these issues underscore the growing tensions between AI companies and content creators. In the ongoing case, *The New York Times v. OpenAI and Microsoft*,[6] the newspaper alleged that OpenAI unlawfully used its articles to train AI models, effectively competing with its business model without providing compensation. Similarly, in *Getty Images v. Stability_AI*, Getty Images accused Stability AI of using copyrighted images without authorisation, highlighting parallel concerns in text-based LLMs.[7] The High Court- rejected the representative action, citing an unclear class definition, the need for individual assessments, and the significant case managements. It ruled that the claim could not proceed collectively due to the lack of a definitive list of affected copyrights works. Additionally, lawsuits filed by authors such as Sarah Silverman argue that AI-generated content infringes on their intellectual property rights. The claim of the author was against Meta for using her books without her knowledge and consent and failure of providing any royalty.[8] However, most of her claims were dismissed marking the second ruling from the court in favour of AI firm. These legal battles emphasise the need for clarity in the legal regime to mandate securing content licenses by the AI developers who intend to train the LLMs to access, retain and reproduce such contents through web scraping. Additionally, there must be an establishment of fair compensation mechanisms for content creators whose contents have been scrapped without their permission. Without clear legal frameworks, disputes over AI training data will continue to create uncertainty in intellectual property law.

Jurisdictional issues make the legal situation even more complicated. In the U.S., copyright is typically human-approach. Although AI creators use the fair use argument, judges have not yet decided if broad-scale AI training without direct permission is fair use. The European Union, however, has more restrictive copyright protections, with the Digital Single Market Directive focusing on protecting content creators' rights. Germany's Section 44b of the Urheberrechtsgesetz (UrhG) permits training AI on legally accessible works but also includes an opt-out option for copyright owners. The UK and China, meanwhile, allow some copyright protection for AI-generated works if a human has considerable creative control. Such differences in copyright legislation reflect the necessity for harmonised global legal framework.

Besides, serious legal and ethical threats are faced by LLM hallucinations.[10] The AI generated hallucinations lead to models generating false, misleading or completely new ideas which results due to limiting the trained data, chance-based errors, or inherent biases. The legal and academic field suffers due to this problem where the accuracy of information is paramount. For instance, in New York attorneys were penalised for filing fake citations generated by ChatGPT.[11] Similarly, a Bengaluru tax tribunal ruling referencing now existent court orders was quickly taken back, and issues regarding AI-generated disinformation were raised.[12] The impact of much dependency upon AI for legal research could be clearly seen from the above-mentioned cases where it generated non- existent legal precedents leading to the misdirection of the court. In academia, problems of frictional research citations are very much possible due to the generation of AI hallucinations which could ultimately affect academic integrity. These situations signify the importance of double checking the content generated by AI to make it correct and legally sound. Solving these challenges becomes crucial, so AI developers must incorporate ethical training strategies and regulatory measures to strike a right balance between safeguarding intellectual property rights and promoting innovation. The developers could adopt a licencing model as remedy, similar to that of the music industry, where the content creators are remunerated for the efforts by platforms like Spotify. Under this approach, AI companies need to get licence for any copyrighted content used in training the data sets. This ensures that fair compensation is paid to the authors, publishers and artists for their work. For ensuring Transparency which is as important, the AI developers must disclose the origins of their training materials in order to enhance accountability and abiding copyright laws. Additionally, Algorithmic changes discouraging LLMs from copying the verbatim passages of copyrighted content could be adopted to minimize the chances of direct infringement. Incorporating DRM methods within the AI generated material, could be done in order to prevent unauthorized resubmission and provide correct citations to the original source.

Furthermore, the encryption- based protections could be adopted as prompt engineering gains commercial value to prevent the misuse and unauthorized sharing of high- value AI prompts.[13] All together if these measures as suggested are incorporated in AI models this would eventually enhance security and prevention of copyright infringement at the same time preserving the innovation and growth of the technology. In addition to copyright safeguards, reducing LLM hallucinations is important for preserving AI's authenticity in the professional and legal domain. Retrieval- Augmented Generation (RAG) models, could be adopted as a remedy to it.[14] The model cross-checks information against verified external sources which could minimize errors and ensure reliability. Thus, strict verification procedures must be

However, their effect on intellectual property law remains a debated topic. From unauthorized use of copyrighted works for training AI models to copying the protected content and presenting legal ambiguity of AI generated work presents a challenging situation to the court and policy makers. The emergency of LLM hallucinations is in addition to these challenges and the reliability of the information provided is now in question. As technology continues to evolve, the law regulating it must parallelly evolve ensuring the pace in order to avoid any violations of the rights. This will result in the balance of the intellectual property rights and innovations. The future of AI and intellectual property law will ultimately depend on the choices made today—whether AI remains a force for innovation or becomes mired in legal and ethical complexities.

[1] Zhiyuan Yu, et.al, ‘Don’t Listen To Me: Understanding and Exploring Jailbreak Prompts of Large Language Models’, *SEC '24: Proceedings of the 33rd USENIX Conference on Security Symposium* (2024) 4675 <Don't listen to me | Proceedings of the 33rd USENIX Conference on Security Symposium> accessed on 7 March 2025.

[2] Hailshree Saksena, ‘Doctrine of Sweat of the Brow’ (2009) SSRN Electronic Journal <Doctrine of Sweat of the Brow> accessed on 7 March 2025.

[3] Antonia Karamolegkou, et.al, ‘Copyright Violations and Large Language Models’ in Houda Bouamor, et.al ed., *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing* (*Association for Computational Linguistics* 2023) 7403 <Copyright Violations and Large Language Models - ACL Anthology> accessed on 7 March 2025.

[4] Elisabetta Stringhi, ‘Hallucinatory (or poorly trained) LLMs? The problem of data accuracy’ (2023) 16(2) *i-lex*. Bologna 54 <Hallucinatory (or poorly trained) LLMs? The problem of data accuracy | i-lex> accessed on 7 March 2025.

[5] Elizabeth Spica, ‘Public Interest, the True Soul: Copyright's Fair Use Doctrine and the Use of Copyrighted Works to Train Generative AI Tools’ (2024) 33 Tex. Intell. Prop. L.J. 67 <Public Interest, the True Soul: Copyright's Fair Use Doctrine and the Use of Copyrighted Works to Train Generative AI Tools 33 Texas Intellectual Property Law Journal 2024-2025> accessed on 7 March 2025.

[6] Civil Action 1:23-cv-11195-SHS (S.D.N.Y. May. 30, 2024).

[7] Getty Images (US), Inc. v. Stability AI, Inc., 1:23-cv-00135, (D. Del.).

[8] Emilia David, ‘Sarah Silverman’s lawsuit against OpenAI partially dismissed’ (14 Feb 2024, *The Verge)* <Sarah Silverman’s lawsuit against OpenAI partially dismissed | The Verge> accessed on 7 March 2025.

[9] Samuel Cohen, ‘The Copyright Office’s Latest Guidance on AI and Copyrightability’ (2025) 15 (66) NLR <AI-Created Works Not Copyrightable: US Copyright Office> accessed on 7 March 2025.

[10] Jerrin B. Mathew, et.al., ‘The Disadvantages and Limitations of Using Large Language Models in the Field of Law’ (n.d., National Law School of India University) accessed on 7 March 2025.

[11] Molly Bohannon, ‘Judge Fines Two Lawyers For Using Fake Cases From ChatGPT’ (22 June 2023, *Forbes*) <Judge Fines Two Lawyers For Using Fake Cases From ChatGPT> accessed on 7 March 2025.

[12] Shipra Singh, ‘Judge Fines Two Lawyers For Using Fake Cases From ChatGPT’ (26 Feb 2025, *mint*) <Did AI hallucination play mischief with a tax tribunal order? | Mint> accessed on 7 March 2025.

[13] M. A. van Wyk, et.al., ‘Protect Your Prompts: Protocols for IP Protection in LLM Applications’ (2023) eprint arXiv:2306.06297 <Protect Your Prompts: Protocols for IP Protection in LLM Applications - Astrophysics Data System> accessed on 7 March 2025.

[14] Mathew, et.al., supra 10