DIGITAL LAW, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

Article

DOI: 10.17803/2713-0533.2024.3.29.415-451

Generative Artificial Intelligence and Legal Frameworks: Identifying Challenges and Proposing Regulatory Reforms

Animesh Kumar Sharma, Rahul Sharma

Lovely Professional University, Phagwara, Punjab, India

***Abstract*:** This research paper seeks to understand the deficit arising from the generative AI and its potential in redefying various sectors and suggesting modification on the current laws. Generative AI systems can generate distinctive content which could be used in text, images, or music, among others, by training from the available data. It highlights how generative AI influences the legal profession in terms of work like contract writing, as well as how newer language models like GPT-4 and chatbots like ChatGPT and Gemini are evolving. Thus, while generative AI has numerous opportunities, it also raises concerns about ethical issues, authorship and ownership, privacy, and abuses, such as the propagation of deepfakes and fake news. This study focuses attention on the importance of strengthening the legal frameworks to answer the ethical issues and challenges linked to generative AI, such as deepfakes, piracy of contents, discriminative impact, or naked breaches of privacy. It calls for proper and sensitive use of generative AI through regulation, openness, and commonly agreed global guidelines. This paper emphasizes that innovations need to be balanced by a set of effective regulations to unleash the potential of generative AI and minimize potential threats.

***Keywords*:** Generative Artificial Intelligence (Generative AI, GAI); legal frameworks; regulatory reforms; Intellectual Property (IP)

Cite as: Sharma, A.K. and Sharma, R., (2024). Generative Artificial Intelligence and Legal Frameworks: Identifying Challenges and Proposing Regulatory Reforms. *Kutafin Law Review*, 11(3), pp. 415–451, doi: 10.17803/2713-0533.2024.3.29.415-451

Contents

I. Introduction

Generative Artificial Intelligence (GAI), often known as Generative AI, is a significant achievement in the field of artificial intelligence (Dwivedi et al., 2021, p. 23). Unlike standard AI systems, which are geared for specialised tasks such as categorization or prediction, Generative AI focuses on creating new material. Text, photos, music, and even sophisticated data simulations can all be learned from current datasets using patterns and structures (Mondal et al., 2023, p. 12). Generative AI models such as GPT-4 and DALL-E excel in producing human-like text and visuals (Aydın and Karaarslan, 2023, p. 126). The rise of Generative AI has enormous promise across multiple disciplines. In the creative sectors, it can help artists generate ideas and content. In healthcare, it can aid in the development of novel medication molecules (Pérez et al., 2023). In education, it can give personalised learning materials (De Angelis et al., 2023, p. 4). The technology promises to revolutionise how we create and interact with digital information, providing unparalleled efficiency and creativity (Campbell et al., 2022, p. 25; Dwivedi et al., 2023, p. 37). However, the development and application of Generative AI poses considerable hurdles. Ethical problems are crucial, as the technology has the potential to generate deepfakes and spread misinformation, with major societal consequences (Porsdam Mann et al., 2023). There is also the issue of intellectual property, as these models frequently train from massive datasets containing copyrighted material, generating concerns about the ownership of generated content (Anderljung and Hazell, 2023). Furthermore, training large-scale AI models has a significant environmental impact due to the massive computational resources required. Ensuring that Generative AI is used ethically and sustainably is a difficult task that requires technological, legal, and ethical concerns (He, 2019, p. 227).

While generative AI brings forth numerous benefits, it also poses significant challenges and potential misuse. Generative AI can be misused to generate deepfake content, misinformation, or for other malicious purposes. The rapid advancement of generative AI techniques requires proactive measures to mitigate potential risks, including the spread of manipulated or fabricated information (Chan, 2023, p. 57). One of the primary concerns is the generation of deepfake content, where AI systems can create incredibly realistic videos, images, or audio recordings that are difficult to distinguish from genuine ones (Maras and Alexandrou, 2019, p. 258). This has raised concerns about the potential for misinformation, identity theft, and the erosion of trust in media. Another area of concern is the potential for AI-generated content to infringe upon intellectual property rights. If generative AI is used to create content that closely resembles existing copyrighted works, it could lead to legal disputes and challenges in determining originality and ownership (Kietzmann et al., 2020, p. 141). There are ethical implications surrounding the use of generative AI, such as the creation of biased or discriminatory content (Illia et al., 2023, p. 206). If the AI models are trained on biased datasets, they may inadvertently generate content that perpetuates existing social inequalities or reinforces harmful stereotypes. Given the potential risks associated with generative AI, it is crucial to amend existing laws and regulations to ensure its responsible and ethical use (Mittelstadt, 2019, p. 503). These amendments should address issues such as the identification and labeling of AI-generated content, establishing guidelines for fair use and intellectual property rights, and implementing mechanisms to prevent the dissemination of malicious or harmful content (Lucaj et al., 2023, p. 1270). Moreover, there is a need to establish frameworks for auditing and certifying generative AI systems to ensure transparency, accountability, and fairness. This would involve defining standards for dataset collection, model training, and evaluation to mitigate biases and ensure that the technology is used in a manner that aligns with societal values and norms. Furthermore, international cooperation and collaboration are essential to developing a cohesive global approach to regulating generative AI. As technology transcends geographical boundaries, harmonized efforts are required to address legal and ethical challenges consistently. Nevertheless, its potential for misuse, particularly in the creation of deepfakes and dissemination of false information, raises significant ethical concerns (Meskys et al., 2020, p. 25). To address these challenges, legal amendments are necessary to regulate the use of generative AI, protect privacy, and combat malicious activities. By striking the right balance between innovation and regulation, we can harness the transformative power of generative AI while safeguarding against its potential misuse. Generative AI, a rapidly advancing field of artificial intelligence, holds immense potential for revolutionizing various industries and empowering creative endeavors (Haluza and Jungwirth, 2023, p. 13). By employing advanced algorithms and neural networks, generative AI systems can generate realistic and original content such as images, videos, music, and even text. However, as with any powerful technology, there is a need to carefully consider its uses and potential misuse. While generative AI offers exciting possibilities, it also raises concerns regarding intellectual property rights, privacy, and ethical considerations. As society continues to navigate this technological frontier, it is imperative to strike a balance between fostering innovation and ensuring appropriate safeguards are in place. Therefore, there is a growing need to amend laws and regulations to address the unique challenges posed by generative AI, while also fostering its beneficial applications.

While Generative AI has transformative potential, understanding its hurdles is critical to reaping its benefits while minimizing its hazards. The future of Generative AI depends on the joint efforts of researchers, policymakers, and industry leaders to overcome these complex concerns. The emergence of Generative AI brings significant legal concerns that current laws are unprepared to address. By changing existing legal frameworks to handle issues of intellectual property, liability, data privacy, and bias, society may better reap the benefits of GAI while limiting the hazards. These legal changes are critical for creating a responsible and equitable AI environment that respects the rights and interests of all stakeholders.

II. Legal Challenges due to GAI and Possible Solutions

Generative Artificial Intelligence has gained significant attention in recent years due to its ability to produce original and creative content. This study examines the advantages and disadvantages of generative AI and highlights the need for legal amendments to address the ethical, social, and legal challenges associated with its use. GAI raises a slew of legal issues that demand broad changes to existing legislation (Moulaei et al., 2024). As these advanced AI systems develop new content, they blur the distinction between human creativity and machine-generated output, posing difficult legal problems about intellectual property, liability, and data privacy. Misuses of generative artificial intelligence are discussed below.

II.1. Intellectual Property Concerns

Generative artificial intelligence raises questions regarding intellectual property rights, as it can replicate existing creative works, potentially leading to copyright infringement and devaluation of original creations (Uzun, 2023, p. 49). GAI raises complex questions about intellectual property rights and ownership. The generated content often builds upon existing works, making it difficult to determine the boundaries of originality and the rights of creators. Legal frameworks need to adapt to address these challenges and provide adequate protection for creators and their works.

One of the most serious IP concerns is determining ownership rights for AI-generated material. Traditional IP rules are intended to safeguard creations that are the result of human intelligence, creativity, and labour. However, GAI systems, such as those used to create art, music, literature, and software code, develop content on their own using algorithms and training data. This raises a number of questions. Who owns the AI-generated content? Is it the AI model developer, the user who submitted the input prompt, or the company that controls the data used to train the AI? Can AI have intellectual property rights? While existing laws do not recognise AI as an entity with rights, this may change in the future as AI systems progress. For example, if an AI system creates a new piece of music, establishing whether the copyright belongs to the AI developer, the user who instructed the AI, or another party becomes difficult. The lack of clear legal precedents and rules in respect of this problem leads to uncertainty and probable conflict among stakeholders.

Potential Infringement of Copyrights: Another key IP issue arises from the manner in which GAI systems are trained. These algorithms often need a large quantity of data to understand patterns and generate new content (Thongmeensuk, 2024, p. 7). This training data frequently includes copyrighted content, such as books, photographs, music, and videos. When AI systems use these materials without legal authority, various problems arise.

Unauthorized Use of Copyrighted Works**:** If an AI system is trained on copyrighted content without the required permissions or licences, it may violate the rights of the original creators and owners. This unauthorised usage may result in legal issues and claims for damages.

Derivative Works and Plagiarism: AI-generated material may closely resemble the original works utilised in training. This similarity might blur the borders between original creativity and plagiarism, making it difficult to identify AI-generated works from actual copyrighted items. For example, if an AI-generated artwork closely mimics the style of a well-known artist whose works were included in the training dataset, there may be concerns that the resulting artwork is an unauthorised derivative work. Similarly, if an AI system generates language that is identical to the structure and content of a copyrighted book, this may be called plagiarism.

II.2. Regulatory Reforms Needed to Address IP Challenges

Addressing these intellectual property challenges necessitates broad legal and regulatory changes. Possible solutions are the following.

Creating New IP Categories: Adding new categories or extending existing IP rules to address AI-generated content. This could involve clarifying ownership rights for AI-generated works and creating policies for using copyrighted content in AI training.

Licencing and Fair Use Policies: Implementing licencing frameworks and fair use standards to allow AI developers to use copyrighted resources while compensating the original inventors and rights holders. This could entail developing common licences for AI training datasets.

Transparency and Documentation: Requiring AI developers to be transparent and document the training data utilised by their algorithms. This can assist ensure that copyrighted items are utilised lawfully and ethically, as well as providing a basis for dispute resolution.

The IP challenges raised by Generative AI are extensive and varied. Determining ownership of AI-generated work and mitigating potential copyright infringements are major difficulties that necessitate thoughtful legal and regulatory changes. By setting explicit norms and frameworks, it is possible to balance the interests of AI developers, users, and original content creators, promoting an atmosphere conducive to innovation while protecting IP rights.

II.3. Misinformation and Deepfake Content

The rapid progress of generative AI increases the risk of producing convincing fake content, including deepfake videos and counterfeit documents, which can have severe social, political, and economic consequences (Bontridder and Poullet, 2021, p. 15). Generative AI has the potential to facilitate the creation of sophisticated deep fakes, which are manipulated videos or images that appear genuine but are actually fabricated. This poses a significant threat to privacy, reputation, and the spread of misinformation. Regulations are necessary to combat the misuse of generative AI in generating malicious content.

Generative Artificial Intelligence (GAI) has the ability to generate highly realistic content, which can be both advantageous and detrimental. While it creates new opportunities for creative and technological innovation, it also introduces substantial threats such as misinformation and deepfakes. False and manipulated media can have a significant impact on public perception, security, and faith in information.

GAI systems may generate hyper-realistic images, movies, and audio materials that are indistinguishable from actual ones. This functionality can be used to create misinformation and deepfakes, resulting in a number of following issues.

Erosion of Trust: The spread of deepfakes and incorrect content threatens public faith in digital media. When people can no longer tell the difference between real and fake material, they lose trust in respectable news sources and truthful reporting.

Political Manipulation: Deepfakes can be used to influence political events and individuals. For example, manufactured movies depicting politicians making provocative words or indulging in unethical behaviour can be used to influence public opinion and disrupt elections. These manoeuvres can destabilise political structures and jeopardise democratic processes.

Personal Harm and Defamation: Individuals can be targeted with deepfakes that portray them in compromising situations, resulting in reputational damage, emotional suffering, and even legal ramifications. Such targeted attacks might be used for extortion, harassment, or retaliation.

Financial Fraud: Deepfakes can also be used in financial schemes, such as producing fake videos of chief executive officers (CEOs) or executives telling employees to transfer payments. These realistic deceptions can cause considerable financial losses for corporations.

II.4. Challenges in Detecting and Mitigating the Impact of Deepfakes

The realistic character of deepfakes and other AI-generated misinformation poses significant hurdles for detection and prevention (Romero Moreno, 2024, p. 15).

Technical Detection Difficulties: Advanced technology and expertise are required to detect deepfakes. As GAI systems become more advanced, the fake material they generate becomes increasingly difficult to detect using standard forensic approaches. Researchers and technology businesses must constantly create and upgrade detection algorithms to stay up with GAI improvements.

Resource Intensive: Creating and deploying good deepfake detection technologies can be resource-intensive. It necessitates significant investment in research, technology, and infrastructure, which may not be possible for all organisations, particularly smaller corporations and individuals.

Rapid Spread of Misinformation: In today's digital age, misinformation can spread quickly via social media and other venues. Even if a deepfake is found, the bogus information may have already affected a huge audience.

II.5. Regulatory Measures Needed to Address the Problems of Misinformation and Deepfake Content

Current legal and regulatory structures are frequently unprepared to address the complications posed by deepfakes. There could be gaps in regulations governing the development, distribution, and use of modified media, making it difficult to hold culprits accountable. To mitigate the impact of deepfakes, the public must be made aware of their presence and potential dangers. Educating people to critically analyse the information they consume is crucial, but difficult given the disparities in media literacy between communities. Addressing the difficulties of misinformation and deepfakes requires a holistic approach that combines legal, technical, and pedagogical initiatives (Montasari, 2024, p. 247).

Misinformation and deepfakes generated by GAI present substantial and diverse issues. To limit these dangers and maintain the integrity of information in the digital age, a mix of legislative measures, advanced detection technology, collaborative efforts, platform regulations, and public education can be used.

Regulatory Measures: Governments and regulatory organisations must update existing laws and enact new legislation that expressly address the creation and dissemination of deepfakes and AI-generated misinformation. This includes providing clear legal definitions and punishments for offenders.

Advanced Detection Technologies: Continued investment in the development of better detecting technology is essential. This includes employing machine learning and AI to detect tiny artefacts and inconsistencies in modified media that are not evident to the human eye.

Collaboration and Standardization: Collaboration among governments, technological businesses, and academic institutes can aid in knowledge exchange and the development of standardised methods for detecting and combating deepfakes. Creating industry standards for content verification and authentication might also be beneficial.

Platform Policies: Social media networks and online services must put in place strong policies and tools for detecting and removing deepfakes. This includes implementing AI-based moderation systems and giving users tools to report suspected deepfakes.

***Public Education Campaigns**:* Running public education efforts to raise awareness about the presence and risks of deepfakes is critical. These initiatives should focus on enhancing media literacy by teaching people how to establish the veracity of the content they come across.

III. Ethical Challenges due to GAI and Possible Solutions

Generative artificial intelligence poses ethical concerns, as it can be used for malicious purposes, such as generating explicit or harmful content, invading privacy, or manipulating public opinion through the creation of misleading narratives (Fiske et al., 2019). There exist ethical concerns related to content ownership, copyright infringement, and authenticity. The automated generation of content blurs the lines between original and artificial creations, leading to challenges in determining the rightful ownership and proper attribution of generated works. GAI raises ethical concerns like misinformation through deepfake, immortalize of bias and possible discrimination due to biased training data. Various ethical concerns arising due to GAI and its potentials solutions are discussed below.

III.1. Perpetuation and Amplification of Existing Biases

AI systems are trained on large datasets that can contain inherent biases, which may be perpetuated in the generated content (Jobin et al., 2019, p. 394). This bias poses a risk of discrimination and exacerbates societal inequalities, emphasizing the need for responsible training and bias mitigation strategies. Generative AI systems are trained on large datasets, which may contain biases present in the data. If not properly addressed, these biases can be amplified in the generated content, perpetuating societal inequalities and discrimination. Developing robust ethical guidelines and regulations is crucial to mitigate these concerns.

GAI systems have the potential to transform several fields by producing fresh information and insights. However, one of the major issues they face is the possibility of replicating and increasing existing biases in their training data. This can result in discriminatory decisions that harm individuals or groups, exacerbating societal disparities and prejudices. GAI systems are trained on big datasets, which frequently contain biases reflecting society prejudices and inequality (Khowaja et al., 2024). These biases can be unintentionally learned and repeated by the AI, resulting in following issues.

Bias in Data Collection: The data used to train AI models may be skewed due to historical injustices, a lack of diversity, or biased sampling techniques. For example, datasets with more data on particular demographics than others may result in an AI system that favours those demographics.

Bias in Data Annotation: When human annotators label training data, they may introduce their own biases. If the annotations represent stereotypical or prejudiced viewpoints, the AI system can learn and reproduce these biases.

Reinforcement of Stereotypes: GAI systems have the potential to generate information that reinforces existing stereotypes. For example, if an AI model is trained on literature containing gender biases, it may generate content that reinforces such biases, such as associating certain professions with a specific gender.

III.2. Discrimination in Respect of Certain Individuals or Groups

GAI system approaches can lead to biased decisions with major consequences for certain individuals or groups. GAI system can enhance biased decisions influencing marginalized communities, females, persons with disabilities, and low income-group. Various religious groups, lesbian, gay, bisexual, transgender, queer or questioning, or another diverse gender identity (LGBTQ+) individuals, ethnic and racial minorities may be facing discrimination in law enforcement, recruitment, and healthcare. Females may encounter gender disparity in jobs, medical care and other fields. People with special needs may be refrained from services, while low-income individuals could be viciously penalized in financial support and employment opportunities. Older individuals and immigrants may also be in pain from AI biases in community services and legal works. These concerns focus attention on the need for trustworthy and inclusive AI design.

Unfair Treatment: AI-generated content may result in discriminatory treatment of people based on their ethnicity, gender, age, or other protected characteristics. If a generative AI employed in recruitment has learned biased patterns from prior hiring data, it may favour certain groups over others.

Misinformation and Harmful Content: Biases in AI-generated content can lead to the spread of disinformation and negative stereotypes. This has the potential to aggravate social differences and contribute to the marginalisation of already vulnerable populations.

***Inequitable Access to Resources and Opportunities**:* Discriminatory AI systems can lead to unequal access to resources and opportunities. For example, an AI model used in lending may deny loans to particular groups more frequently due to biased training data, reinforcing financial inequities.

Compliance with Anti-Discrimination Laws: AI systems must follow anti-discrimination laws and regulations that prevent unfair treatment based on protected traits. To ensure compliance, AI models must be rigorously tested and validated to discover and mitigate biases.

III.3. Ethical Responsibility

Generative AI presents substantial issues in terms of prejudice and discrimination (Ferrara, 2023, p. 7). Developers and users of GAI may assist create more fair and equitable AI systems by identifying sources of bias in training data, understanding the potential for discriminatory outcomes, and adopting robust solutions to address these issues. This necessitates a concerted effort to ensure that AI technologies are developed and deployed in ways that foster inclusivity, fairness, and ethical responsibility.

Developers and users of GAI systems must ensure that their AI technologies do not damage people or increase societal injustices. This includes applying justice and inclusion ideals to AI development and deployment. Several strategies can be used to reduce prejudice and discrimination in GAI systems.

Diverse and Representative Data: Keeping training datasets broad and representative of the population might help decrease biases. This entails actively searching out and incorporating data from underrepresented populations which include individuals with disabilities, minorities, low-income groups, less educated or uneducated individuals, older people and people with rural background etc.

Bias Detection and Mitigation Techniques*:* Implementing bias detection and mitigation strategies, such as reweighting data, employing fairness constraints, and using debiasing algorithms, can aid in the identification and reduction of biases in AI models.

Regular Audits and Transparency: Regular audits of AI systems to determine their fairness and transparency are required. Providing detailed documentation and explanations of AI decision-making processes can help to foster confidence and accountability.

Inclusive Design Practices: Adopting inclusive design methods that include diverse teams in the development process will assist ensure that different points of view are considered, lowering the likelihood of biased results.

Ongoing Monitoring and Evaluation: Continuously monitoring and reviewing AI systems after deployment to identify and resolve any developing biases or discriminatory effects is critical for long-term fairness.

IV. Data Privacy Concerns due to GAI

GAI systems are often trained on large datasets containing personal and sensitive information. The use of such data creates serious legal concerns, notably around permission and data protection. Existing data privacy legislation, like as the General Data Protection Regulation (GDPR) in Europe, may need to be revised to account for the complexities of AI training procedures. To ensure that individuals' privacy rights are safeguarded under GAI, strong data governance procedures and unambiguous data usage and retention regulations are required.

The deployment of GAI systems creates serious privacy problems (Kar et al., 2023, p. 675). These issues originate from the considerable usage of personal and sensitive information in AI model training, as well as the problems of guaranteeing compliance with existing data protection rules, such as the GDPR. Addressing these challenges is crucial for protecting individuals' privacy rights and preserving public trust in AI technologies.

IV.1. Challenges in Protecting Personal and Sensitive Information

Generative AI systems frequently require large volumes of data to learn and generate new information effectively. This data may contain personal and sensitive information, such as text from social media posts, medical records, financial data, and other private information. The usage of such data presents the following challenges.

Data Collection and Consent: Obtaining and using personal data for training AI models requires proper consent. However, it can be difficult to confirm that all data utilised in training was obtained legally and with the informed agreement of all parties involved. Datasets are frequently aggregated from multiple sources, making it difficult to track the consent status of each piece of data.

Anonymization and De-Identification: To maintain privacy, data used to train AI models should be anonymised or de-identified. However, complete anonymization is difficult to achieve, and there is always the possibility that anonymized data will be re-identified, particularly when paired with other data sources. This poses a serious threat to people's privacy.

Data Minimization and Purpose Limitation: Data protection principles promote data reduction (using only the data required for the purpose) and purpose limitation. Ensuring that generative AI models adhere to these principles is difficult, especially given the large and diverse datasets they require.

IV.2. Ensuring Compliance with Data Protection Laws like GDPR

The GDPR and other data protection legislation impose strict restrictions on the processing and protection of personal data. Ensuring compliance with these regulations when building and deploying generative AI systems presents the following three important challenges.

Right to be Forgotten: Individuals have the right under GDPR to request that their personal data be deleted. This presents a problem to AI systems that have already been trained on data including the personal information of persons who later exercise this right. Retraining models to exclude such data, as well as developing technical solutions to meet these needs, can be time-consuming and costly.

Data Subject Rights: Individuals have a variety of data-related rights under GDPR, including the ability to access, correct, and restrict data processing. Implementing measures to protect these rights in the context of generative AI is difficult, especially when dealing with huge, dynamic datasets.

Data Breach Notification: Data breaches are a risk for generative AI systems, as they are for any other digital system. Respective law of the land needs to be either updated or put in place, systems to detect, respond to, and alert affected individuals.

IV.3. Legal and Technological Solutions to the Problem of Protecting Personal and Sensitive Information

Protecting data privacy in the context of Generative AI entails tackling the issues of using personal and sensitive information to train AI models while also guaranteeing compliance with data protection legislation such as GDPR. These dangers can be mitigated and individuals' privacy rights protected by adopting strong data governance frameworks, utilising privacy-enhancing technologies, conducting regular audits, and maintaining transparent policies. To address these data privacy challenges, a mix of the following legal and technological solutions are required.

Data Governance Frameworks: Putting in place complete data governance frameworks that include policies and processes for data collecting, consent management, anonymization, and data minimization. These frameworks should ensure that the data used to train AI models is handled ethically and lawfully.

Privacy-Enhancing Technologies (PETs): Using privacy-enhancing technologies such as differential privacy, federated learning, and homomorphic encryption can help safeguard personal data while also allowing AI models to be trained effectively. These technologies can lower the danger of data breaches and re-identification.

Regular Audits and Assessments: Regular privacy impact studies and audits are conducted to examine and mitigate the privacy hazards associated with generative AI systems. These audits can help to verify continuing compliance with data protection rules and suggest areas for improvement.

Transparent Practices: Maintaining transparency in the collection, usage, and protection of data in generative AI systems. Individuals' trust and compliance with data protection standards can be increased by providing them with clear and accessible information about their rights and how their data is handled.

V. Liability and Accountability for GAI-Generated Content

Determining accountability for GAI-generated content is still another big difficulty. If an AI system generates defamatory content, disinformation, or damaging outputs, it is critical to determine who is to blame (Dogru et al., 2023, p. 1089). Current legal frameworks fail to explicitly specify the accountability of AI developers, deployers, and consumers. Legal changes are required to define obligations and ensure that the relevant parties can be held accountable for the conduct of generative AI systems.

GAI systems, while strong and inventive, present substantial liability and accountability concerns. These difficulties must be addressed in order to ensure that AI technology is used and deployed responsibly and ethically. The key difficulties in this field are determining who is liable for AI-generated content and addressing the legal ramifications when such content causes harm or violates laws.

V.1. Establishing Who Is Responsible for the Content Generated by AI

One of GAI's primary issues is identifying culpability for the content it generates. Unlike traditional software, which relies on explicit instructions from human programmers, GAI systems generate content on their own using patterns acquired from training data (Yang et al., 2024, p. 7). This poses various questions.

Developer Responsibility: Should the AI system's designers be held responsible for the results produced by their technology? Developers manage the AI's design and training, but not its specific outputs once deployed.

User Responsibility: Should users that interact with the AI and provide input prompts be held liable for the created content? Users can alter the material by providing inputs, but they may not fully comprehend the AI's underlying operations.

Joint Responsibility: Could there be a joint duty between developers and users? This approach acknowledges both parties' roles in the creation and usage of AI-generated material. For example, if an AI-generated artwork is discovered to infringe on existing copyrights, it is unclear whether the guilt should be placed on the AI developer, who developed and taught the system, or the user, who gave the precise input that resulted in the infringing output. This ambiguity hampers the process of determining liability and needs explicit legal definitions and frameworks.

V.2. Addressing Legal Consequences when AI-Generated Content Causes Harm or Violates Laws

When AI-generated content causes harm or violates laws, finding the proper legal repercussions is another difficult task. Harm can take many forms, including defamation, disinformation, or the creation of harmful or unlawful content (Ling, 2023, p. 105). The legal system must change to adequately deal with these new forms of injury.

Defamation and Misinformation**:** If an AI system creates content that defames someone or spreads incorrect information, it is critical to determine who is legally responsible. This is especially problematic when material is developed by an autonomous machine rather than a human.

Illegal and Harmful Content: AI systems have the potential to generate illegal or harmful content, such as explicit material, hate speech, or encouragement to violence, either accidentally or on purpose. Addressing the legal implications of such content necessitates new legislation that can hold responsible parties accountable.

Consider the scenario in which an AI chatbot produces damaging or offensive speech. Should the platform hosting the chatbot be held accountable, or should the burden fall on the developers who designed the chatbot's algorithms? Furthermore, if an AI-generated deepfake is used to deceive or hurt people, identifying culpability is critical for ensuring justice and preventing such instances.

V.3. Legal and Regulatory Implications

To effectively handle the difficulties of liability and accountability in GAI, numerous legal and regulatory approaches can be considered.

Clear Liability Frameworks: Creating explicit liability frameworks outlining the roles of developers, users, and other stakeholders engaged in the deployment and usage of GAI systems. These frameworks should specify the situations under which each party may be held accountable.

Compliance and Oversight Mechanisms**:** Putting in place measures to monitor and regulate the use of GAI systems. This might include frequent audits, certification processes, and the creation of regulatory agencies to monitor AI systems.

Robust Legal Recourse**:** Offering strong legal remedies to individuals and entities affected by AI-generated content. This involves ensuring that there are clear legal channels for seeking restitution and justice in cases of harm or infringement.

Ethical Guidelines and Best Practices: Government and associated relevant regulatory bodies should encourage the application of ethical guidelines and best practices in the creation and implementation of GAI systems. This can help to reduce harm and guarantee that AI technologies are used responsibly and ethically.

Addressing the responsibility and accountability issues raised by Generative AI necessitates a multidimensional approach that includes clear legal frameworks, strong oversight, and ethical principles. We can make the AI ecosystem safer and more accountable by determining who is liable for AI-generated material and dealing with the legal ramifications of damaging outputs. This will assist to increase trust in AI technologies and ensure that their benefits are realised without jeopardising legal and ethical standards.

VI. Cases of Deepfakes

After the evolution of GAI, deepfake cases have increased (Shoaib et al., 2023, p. 4). Few political deepfake, deepfake cases of celebrities, video fraud calls, cases of social media information, corporate espionage and financial scam cases are discussed below.

VI.1. Political Deepfakes

In 2018, director Jordan Peele worked with Buzzfeed to create a deepfake video depicting former US President Barack Obama. The video, titled "Obama Deepfake," utilises Peele's voice and facial manipulation technologies to resemble Obama giving a public service statement. This video received a lot of attention and highlighted how deepfakes can trick viewers by successfully imitating popular people (Cuthbertson, 2018). In 2018, researchers made a deepfake video of former US President Barack Obama to demonstrate how readily disinformation may spread. The video depicted Obama saying statements he never said, emphasising the potential for deepfakes to sway public perception and electoral outcomes.

In 2019, the Belgian political party Socialistische Partij Anders launched a series of deepfake videos starring several Belgian politicians, including the Prime Minister. These movies were produced as part of a campaign to raise awareness about the risks of deepfake technology and its possible impact on political discourse and public confidence.[1]

Deepfake technology was reportedly used to make fake remarks by Gabonese politicians in 2020. These edited videos were shared on social media platforms, raising concerns about their ability to influence public opinion and cause unrest in the country.[2]

During the 2019 Indian general election campaign, deepfake videos of political leaders were shared on social media platforms. These videos were modified to show politicians making provocative statements or acting unethically, raising worries about the use of deepfakes for political propaganda and misinformation (Chaturvedi and Kumar, 2019).

These incidents show the increasing prevalence of political deepfakes, as well as the need for more awareness, legislation, and countermeasures to address the hazards connected with synthetic media manipulation in political contexts.

VI.2. Celebrity Deepfakes

Deepfake videos of actress Scarlett Johansson appeared online in 2019, showing her in uncomfortable settings. These fully produced videos demonstrated the potential for deepfakes to ruin individuals' reputations and invade their privacy.

In 2021, a deepfake video of Tom Cruise went viral on TikTok. Chris Ume, a visual effects specialist, made the film, which convincingly depicted Cruise performing magic tricks and chatting golf, sparking widespread doubt about its validity.[3]

[1] Mast, J., (2019). Prime Minister appears in deepfake video about Facebook. *The Brussels Times*. Available at: https://www.brusselstimes.com/all-news/belgium-all-news/education/70836/prime-minister-appears-in-deepfake-video-about-facebook/ [Accessed 12.05.2024].

[2] BBC News. (2020). Gabon government "using deepfakes to create fake speech." *BBC News*. Available at: https://www.bbc.com/news/technology-51219120 [Accessed 10.05.2024].

[3] ABC News. (2021). Viral deepfake video of Tom Cruise on TikTok heightens concerns about manipulated media. *ABC News*. Available at: https://abcnews.go.com/US/viral-deepfake-video-tom-cruise-tiktok-heightens-concerns/story?id=76249861 [Accessed 11.05.2024].

In 2020, a deepfake video surfaced online in which creator Steve Buscemi's face was digitally transplanted onto Jennifer Lawrence's body. The film, which went viral on social media, demonstrated how deepfake technology can generate misleading and fraudulent information.[4]

These incidents emphasise the ethical and privacy concerns surrounding celebrity deepfakes, emphasising the importance of improved awareness, regulation, and technological remedies to address the hazards posed by synthetic media manipulation.

VI.3. Fraudulent Video Calls

In 2020, a UK-based energy company was duped out of $ 243,000 with a deepfake audio call. The crooks employed artificial intelligence to impersonate the CEO's voice and direct an employee to transfer funds to a fake account. This example highlighted the risks connected with AI-generated voice impersonation in corporate security. In 2019, a UK-based energy company fell victim to a deepfake audio fraud that resembled the CEO's voice. The fraudsters impersonated the CEO using AI-generated voice technology and convinced an employee to transfer € 220,000 to a Hungarian supplier. This event exposed the ability of deepfake technology to support sophisticated financial fraud schemes.[5]

In 2020, a European energy company was targeted with a deepfake video conferencing hoax. During a video conference call with a senior executive, the fraudsters impersonated the CEO of the company using AI-generated footage. The deepfake video convinced the CEO to authorise a fraudulent money transfer, resulting in significant financial losses for the company.[6]

[4] Ridder, K., (2020). Steve Buscemi Replaces Jennifer Lawrence in Deepfake Video and It's So Confusing. *Newsweek*. Available at: https://www.newsweek.com/steve-buscemi-jennifer-lawrence-deepfake-video-1482503 [Accessed 12.06.2024].

[5] BBC News. (2019). UK energy firm probes "deepfake" video of boss. *BBC News*. Available at: https://www.bbc.com/news/technology-49574808 [Accessed 11.05.2024].

[6] Bloomberg. (2020). A European Energy Firm Pays Up After Cyberattack, Deepfake. *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2020-10-30/a-european-energy-firm-pays-up-after-cyberattack-deepfake [Accessed 09.05.2024].

In 2021, criminals targeted a German corporation by impersonating its CEO with AI-generated voice technology. The fraudsters employed a deepfake voice to ask an employee to send € 220,000 to a Hungarian supplier. Despite the company's verification measures, the deepfake voice's convincing nature allowed the fraudulent transaction to be carried out successfully.[7]

In 2020, fraudsters attempted to scam a UK-based energy corporation by impersonating a British CEO using deepfake technology. The deepfake video chat was convincing enough to trick the company's finance controller into sending € 220,000 to the criminals' account. The event demonstrated the vulnerability of organisations to deepfake-based impersonation frauds.[8]

These examples highlight the real-world consequences of fraudulent video calls enabled by deepfake technology. They emphasise the importance of organisations using strong authentication and verification mechanisms to detect and avoid deepfake-related scams. They also emphasise the significance of raising awareness about the risks connected with synthetic media manipulation in financial transactions and corporate communications.

VI.4. Social Media Misinformation

Deepfake technology was used during the 2020 US elections to generate videos of politicians making incendiary statements. These videos propagated on social media channels, confusing voters and propagating misleading information.

In 2019, a doctored video of US House Speaker Nancy Pelosi became popular on social media platforms. The video was slowed to make Pelosi appear intoxicated or incapacitated, causing considerable outrage and

[7] DW News. (2021). German energy firm becomes victim of deepfake cyberattack. *DW News*. Available at: https://www.dw.com/en/german-energy-firm-becomes-victim-of-deepfake-cyberattack/a-57192482 [Accessed 11.05.2024].

[8] IT Governance. (2020). Deepfake scams: UK CEO loses € 220,000 in latest attack. *IT Governance*. Available at: https://www.itgovernance.co.uk/blog/deepfake-scams-uk-ceo-loses-220000-in-latest-attack [Accessed 10.05.2024].

underlining the potential for deepfakes to propagate misinformation and political propaganda.[9]

Throughout the Covid-19 outbreak, multiple deepfake videos circulated on social media platforms, spreading falsehoods about the virus and its origin. These videos contained false remarks from health authorities, conspiracy theories, and incorrect information about viable therapies, all of which contributed to confusion and public mistrust.[10]

During elections and political campaigns, deepfake videos have been used to propagate misinformation and political propaganda on social media sites. For example, in the run-up to the 2020 presidential election in the United States, deepfake videos including falsified claims from political candidates circulated online, with the goal of manipulating public perception and influencing voter behaviour. Deepfake videos of celebrities have been used to promote disinformation and false tales on social media platforms. For example, falsified videos of celebrities making controversial words or engaging in illegal actions have spread online, confusing viewers and feeding rumours.[11]

These examples demonstrate the various ways deepfake technology has been used to propagate misinformation and disinformation on social media sites. They emphasise the significance of critical media literacy and strong fact-checking processes in combating the spread of false content online.

VI.5. Corporate Espionage

A bad creator might utilise deepfake technology to construct a convincing video or audio clip of a company's CEO or another high-ranking executive. Deepfakes could be used to broadcast misleading

[9] BBC News. (2019). Pelosi "drunk" video: Faked footage shows House speaker slurring. *BBC News*. Available at: https://www.bbc.com/news/world-us-canada-48348059 [Accessed 11.05.2024].

[10] The Guardian. (2020). "We're in a Petri Dish": How a Covid-19 Office Outbreak Unfolded — and Was Covered Up. *The Guardian*. Available at: https://www.theguardian.com/world/2020/aug/15/covid-19-petri-dish-how-a-coronavirus-outbreak-unfolded [Accessed 11.05.2024].

[11] NBC News. (2020, January 13). Deepfake videos are getting better, but they're still easy to spot. *NBC News*. Available at: https://www.nbcnews.com/tech/security/deepfake-videos-are-getting-better-they-re-still-easy-spot-n1116181 [Accessed 29.05.2024].

information, issue fraudulent directions, or deceive personnel or stakeholders, causing reputational damage or financial losses to the targeted organization (George and George, 2023). Deepfake technology might be used to create realistic video footage of boardroom meetings or private discussions inside a firm. Competitors or adversaries could use the faked content to obtain access to strategic plans, sensitive information, or trade secrets, undermining the targeted organization's competitive advantage. Deepfake videos or audio recordings could be used to construct false financial reports or earnings calls that misrepresent a company's financial status or prognosis. Attackers who disseminate false financial information may manipulate stock prices, disrupt financial markets, or erode investor trust in the targeted organisation. Deepfake technology may enable sophisticated phishing assaults or social engineering techniques aimed at a company's employees or business partners. Malicious creators could create convincing deepfake videos or audio messages that impersonate trusted individuals within the organisation, such as colleagues, supervisors, or IT administrators, in order to trick targets into disclosing sensitive information, granting unauthorised access, or conducting fraudulent transactions.

The deepfake cases cited above highlight areas of concern for the corporate world. Need of the hour for corporates is to be aware about bad usage of the GAI in the industry. Corporates must put a system in place to detect deepfakes and resolve any issues arising of it in minimum possible times.

VI.6. Financial Scams

In 2022, deepfake movies and audio samples were utilised in a series of scams aimed at individuals and businesses. Fraudsters exploited AI-generated material to imitate bank officials and get personal information, causing considerable financial losses for the victims (De Rancourt-Raymond and Smaili, 2023). A bad creator could utilise deepfake technology to imitate a company's CEO or another senior executive in video or audio recordings. The deepfake might be used to tell staff to transfer funds to fake accounts under the pretence of essential business activities, causing financial loss for the targeted organisation. Deepfake technology might be used to generate fake video testimonials or endorsements from well-known figures or financial experts, thereby promoting fraudulent investment schemes or possibilities. The persuasive nature of the deepfakes may fool potential investors into making financial contributions or investments that result in losses. Malicious creators might utilise deepfake technology to make fake movies or audio recordings with misleading information about publicly traded firms, economic indicators, or geopolitical events. By releasing false information, attackers can manipulate stock prices, commodity markets, or cryptocurrency values for personal benefit or to cause financial harm to others. Deepfake videos or audio messages could be used in phishing or social engineering attacks on individuals or financial institutions. For example, attackers could construct convincing deepfake recordings imitating bank personnel, government authorities, or trusted associates in order to fool victims into providing critical financial information, such as account credentials or payment authorization codes.

While these instances demonstrate potential concerns related with deepfake technology in the context of financial frauds, it is crucial to remember that documented cases may be limited or unknown due to the secretive nature of fraudulent activity. Furthermore, breakthroughs in deepfake detection and verification systems are being developed to reduce the hazards associated with synthetic media manipulation in financial transactions and communications.

VII. Discussion

Generative AI holds immense promise for driving innovation, creativity, and advancements across various industries. However, its potential uses and misuses necessitate a careful examination of existing laws and regulations. As generative AI systems become more autonomous and capable of independent decision-making, determining accountability and liability becomes challenging. Legal amendments should establish clear frameworks to attribute responsibility in cases of AI-generated content causing harm or infringing legal rights. By amending legal frameworks, and addressing concerns surrounding intellectual property rights, privacy, and ethics, society can foster the responsible and beneficial deployment of generative AI. Legislation must be revised to establish legal frameworks that address the creation, distribution, and detection of fake content, ensuring accountability and protecting individuals and organizations from the harmful effects of misinformation. Generative AI relies on vast amounts of data, raising concerns about data privacy and security. Legal amendments should address these concerns by ensuring transparent data usage, informed consent, and robust security measures to protect sensitive information. Striking the right balance between enabling innovation and protecting individual rights is crucial to ensure that this transformative technology benefits humanity. To address the unique challenges posed by generative AI, it is imperative to amend existing laws and regulations.

Existing intellectual property frameworks may not adequately address the challenges posed by generative AI. Amendments are necessary to clarify ownership, attribution, and licensing rights concerning content generated by AI systems, protecting the rights of both creators and consumers. Intellectual property laws should be revised to account for the generation of original content by AI systems. This may involve establishing clear guidelines for ownership, attribution, and licensing of generative AI-generated content, ensuring that creators are appropriately recognized and protected. The privacy laws need to be strengthened to tackle the potential harms arising from the misuse of generative AI. Generative AI raises concerns about privacy and data protection. Amendments in legislation should focus on regulating the collection, storage, and use of personal data in generative AI systems to safeguard individual privacy rights. Stricter regulations can be implemented to deter the creation and distribution of maliciously generated content, safeguarding individuals' privacy and preventing the spread of misinformation. Existing copyright laws need to be amended to account for the challenges posed by generative AI. New regulations should address issues of ownership, attribution, and fair use of content generated by AI systems.

Ethical considerations should be at the forefront of legal amendments concerning generative AI. Transparency requirements could be imposed to ensure that generated content is distinguishable from human-created content, reducing the potential for deception.

Additionally, guidelines for the responsible development and deployment of generative AI systems should be established, promoting accountability and mitigating potential risks. Laws and regulations should encourage the development and adoption of ethical guidelines for generative AI research and applications. Furthermore, mechanisms for accountability, transparency, and auditing of AI systems must be established.

Given the potential uses and misuse of generative AI, it is crucial to update existing laws and regulations to address the associated ethical and societal challenges. Legal amendments should focus on three key aspects: accountability, consent, and transparency. Accountability measures should be established to ensure that the creators and users of generative AI technologies bear responsibility for the content generated. This can involve holding individuals or organizations accountable for the misuse of generative AI, especially in cases of malicious deepfakes or other harmful manipulations. Consent frameworks need to be strengthened to protect individuals' rights and privacy. Clear guidelines should be established regarding the generation and dissemination of synthetic content involving real individuals, ensuring that consent is obtained and that there are strict limitations on the use of personal data. Transparency regulations should be enacted to enhance the explainability and traceability of generative AI systems. This includes requiring clear identification of generated content and implementing mechanisms that allow users to verify the authenticity of media. By promoting transparency, users can make informed decisions and distinguish between genuine and manipulated content.

VIII. Implications

The implications of this research can shape future discussions on copyright laws, licensing agreements, and attribution practices in the context of AI-generated content. The implications of this study are divided into two sections i.e., theoretical and practical implications. Theoretical implications reflect the current study's contribution into the literature while practical implications show how this study contributes to the field of legal policies and procedures.

VIII.1. Theoretical Implications

The study on generative AI has significant theoretical implications for ethical and legal frameworks, particularly in terms of liability, accountability, and bias mitigation. It contributes to the ongoing debate on legal frameworks attributing liability to developers, users, or AI systems themselves. Moreover, it addresses bias in AI systems and aids in the development of fair and unbiased algorithms that prioritize fairness, transparency, and diversity for equitable outcomes. This research proposes measures that specifically target the risks created by AI applications. It advocates for the identification of high-risk applications and the establishment of clear requirements for generated AI systems used in such applications. Furthermore, it emphasizes the need for defining specific obligations for both AI users and providers of high-risk applications. To ensure safety and compliance, the research recommends the implementation of a conformity assessment before the AI system is deployed or made available in the market. This study proposes the enforcement of regulations and policies once an AI system is placed in the market.

Fair and Transformative Use: Fair use is a US legal doctrine (as recently upheld by the US Supreme Court) that allows limited use of copyrighted material without permission under certain circumstances (King, 2023, p. 124). To determine whether an AI-generated work qualifies for fair use, factors such as the purpose, nature, extent, and effect of its use are needed to be considered. Transformative use is often considered an important factor in fair use analysis, which involves adding new meaning or expression to the copyrighted work.

Obligations and Responsibilities: Determining liability for copyright infringement in AI-generated works can be complex, involving questions regarding the role of AI developers, users, and artificial intelligence itself. The responsibility for ensuring compliance with copyright law lies with both the creator and the user of AI-generated works. Determining the rightful copyright owner becomes challenging if the AI system operates without human intervention.

The Indian Copyright Act, 1957[12] and the Patents Act, 1970[13] make specific provisions for fair treatment and enumerated exceptions for copyright infringement. The use of copyrighted material for training AI models is kept on the legal gray list. As such copyright laws do not protect any creation generated solely by AI, even if it stems from a human-generated text indicator. Observations and decisions of international courts and other jurisdictions, such as the recent US Supreme Court decision on copyright and AI, may influence the interpretation of fairness in Indian copyright law.[14]

Indian copyright law and fair use provisions will need to be adapted to address the challenges posed by AI-generated content. The purpose of the use is crucial, whether the AI-generated content is intended for commercial gain or non-profit educational purposes. The nature of the copyrighted work should be evaluated, along with the amount and substantiality of the portion used in relation to the entire copyrighted work. Another crucial consideration is the effect of AI-generated content on the potential market or the value and importance of the original copyrighted work. It is essential to update intellectual property laws to keep pace with advancements in AI technology, ensuring they encompass the intricacies of AI-generated content. The implementation of data use and governance policies, along with oversight and compliance mechanisms, is necessary to regulate AI projects effectively. To protect copyright, it would be prudent to mandate AI firms to appoint compliance officers who are responsible for copyright protection, conducting audits, and performing assessments. These measures collectively aim to strike a balance between innovation and the preservation of intellectual property rights in the realm of AI-generated content in India. The intersection between copyright infringement and AI may impact the development of AI technology and

[12] The Indian Copyright Act No. 14 of 1957, enacted by the Parliament of India on 4 June 1957.

[13] The Patents Act No. 39 of 1970, enacted by the Parliament of India on 19 September 1970.

[14] AI and Copyright Law: Understanding the Challenges, 2023. Available at: https://www.wileyconnect.com/AI-and-Copyright-Law-Understanding-the-Challenges [Accessed 15.05.2024].

its potential applications. Establishing a balance between protecting the rights of copyright owners and promoting innovation in the field of AI is essential for the development and progress of this field.

VIII.2. Practical implications

This research study has the potential to contribute to the development of legislation concerning copyright, attribution, and licensing issues regarding AI-generated content. It can aid in the establishment of laws that set up clear guidelines for assigning liability and holding accountable the individuals or organizations involved in the creation and implementation of AI systems.

The study's findings on generative AI can also contribute to the formulation of ethical guidelines for its development and deployment. These guidelines can serve as a fundamental framework for formulating legislation aimed at governing the application of AI within sensitive domains, including healthcare, finance, criminal justice, and autonomous vehicles.

By establishing clear boundaries and prescribing acceptable principles and procedures, these norms would facilitate the conscientious and morally upright utilization of AI technology, promoting responsible conduct and ethical practices. The research emphasizes the significance of promoting public awareness and education about AI technologies, including their capabilities and potential impact on society. It suggests the collaboration of policymakers and stakeholders in the promotion of AI literacy, ensuring that individuals possess a comprehensive understanding of the implications and risks associated with generative AI.

IX. Conclusion

This research study highlights the pressing need and significance of establishing comprehensive legal frameworks tailored specifically for the field of generative artificial intelligence. Through addressing key areas such as intellectual property, ethics, privacy, and collaboration, policymakers can cultivate responsible and innovative AI development, all while protecting the rights and welfare of individuals and society at large. The study highlights the crucial importance of comprehensive laws and regulations that encompass various facets such as intellectual property rights, privacy concerns, accountability, and liability about AI-generated content. Moreover, it emphasizes the significance of interdisciplinary collaboration among technologists, policymakers, legal experts, and other stakeholders.

A unified and concerted effort involving all relevant parties is imperative to navigate the intricate legal implications of generative AI and to develop robust and adaptable regulatory frameworks. Furthermore, this study offers invaluable insights into the legal implications and challenges associated with the emergence of generative AI. By addressing these challenges through the implementation of updated legal frameworks, ethical guidelines, and interdisciplinary collaboration, we can fully harness the immense potential offered by generative AI while concurrently safeguarding the rights, privacy, and overall well-being of individuals and society at large.

This study focuses attention on the urgent need to reform the current laws and regulations to effectively address the generative AI's legal complications. The research study recommends modifications in legal framework to distinctly ensure the responsibility of the AI generated content. Furthermore, this study stresses to chart out clear ethical guidelines for the development and responsible deployment of generative artificial intelligence. The need of the hour is to inculcate ethics related content in the curriculum of primary and secondary education in schools. A clear-cut set of punishments need to be specified by the respective governments in the IT Acts / Cyber laws of their countries to tackle misuse of generative artificial intelligence.

However, this research study on generative AI and laws faces a significant limitation, namely the potential presence of data bias. The study is done in the context of Indian laws, future studies could be carried out on other countries' laws. This issue necessitates future research endeavors aimed at advancing the development of legal and policy frameworks that effectively tackle the legal challenges posed by generative AI. Several critical aspects require attention, including liability, intellectual property, data handling, privacy, and accountability. To make substantial progress, future investigations on generative AI and laws should strive to overcome various limitations, encompassing but not limited to data bias, ethical considerations, legal interpretation, adversarial attacks, human-AI collaboration, regulatory frameworks, and user experience. By systematically addressing these areas, researchers can significantly contribute to the establishment of robust, equitable, and reliable generative AI systems within the legal domain.

References

Anderljung, M. and Hazell, J., (2023). Protecting Society from AI Misuse: When are Restrictions on Capabilities Warranted? *arXiv preprint arXiv:2303.09377,* doi: 10.48550/arXiv.2303.09377.

Aydın, Ö. and Karaarslan, E., (2023). Is ChatGPT leading generative AI? What is beyond expectations? *Academic Platform Journal of Engineering and Smart Systems*, 11(3), pp. 118–134, doi: 10.21541/apjess.1293702.

Bontridder, N. and Poullet, Y., (2021). The role of artificial intelligence in disinformation. *Data & Policy*, 3, p. e32, doi: 10.1017/dap.2021.20.

Campbell, C., Plangger, K., Sands, S. and Kietzmann, J., (2022). Preparing for an era of deepfakes and AI-generated ads: A framework for understanding responses to manipulated advertising. *Journal of Advertising*, 51(1), pp. 22–38, doi: 10.1080/00913367.2021.1909515.

Chan, A., (2023). GPT-3 and InstructGPT: Technological dystopianism, utopianism, and “Contextual” perspectives in AI ethics and industry. *AI and Ethics*, 3(1), pp. 53–64, doi: 10.1007/s43681-022-00148-6.

Chaturvedi, S. and Kumar, H., (2019). Deepfakes and beyond: The new landscape of political propaganda. *The Hindu*. Available at: https://www.thehindu.com/elections/lok-sabha/from-it-bots-to-ai-deepfakes-the-evolution-of-election-related-misinformation-in-india/article68015342.ece [Accessed 15.05.2024].

Cuthbertson, A., (2018). Obama deepfake warns of “terrifying” future for fake news. *The Independent*. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/obama-deepfake-jordan-peele-video-fake-news-a8313901.html [Accessed 11.05.2024].

De Angelis, L., Baglivo, F., Arzilli, G., Privitera, G.P., Ferragina, P., Tozzi, A.E. and Rizzo, C., (2023). ChatGPT and the rise of large language models: the new AI-driven infodemic threat in public health. *Frontiers in Public Health*, 11, pp. 1–8, doi: 10.3389/fpubh.2023.1166120.

De Rancourt-Raymond, A. and Smaili, N., (2023). The unethical use of deepfakes. *Journal of Financial Crime*, 30(4), pp. 1066–1077, doi: 10.1108/JFC-04-2022-0090.

Dogru, T., Line, N., Hanks, L., Acikgoz, F., Abbott, J.A., Bakir, S., Berbekova, A., Bilgihan, A., Iskender, A., Kizildag, M. and Lee, M., (2023). The implications of generative artificial intelligence in academic research and higher education in tourism and hospitality. *Tourism Economics*, pp. 1083–1094, doi: 10.1177/13548166231204065.

Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A. and Galanos, V., (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, pp. 1–47, doi: 10.1016/j.ijinfomgt.2019.08.002.

Dwivedi, Y.K., Kshetri, N., Hughes, L., Slade, E.L., Jeyaraj, A., Kar, A.K., Baabdullah, A.M., Koohang, A., Raghavan, V., Ahuja, M. and Albanna, H., (2023). “So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, pp. 1–63, doi: 10.1016/j. ijinfomgt.2023.102642.

Ferrara, E., (2023). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. *Sci*, 6(1), pp. 1–15, doi: 10.3390/sci6010003.

Fiske, A., Henningsen, P. and Buyx, A., (2019). Your robot therapist will see you now: ethical implications of embodied artificial intelligence in psychiatry, psychology, and psychotherapy. *Journal of medical Internet research*, 21(5), p. e13216, doi: 10.2196/13216.

George, A.S. and George, A.H., (2023). Deepfakes: The Evolution of Hyper Realistic Media Manipulation. *Partners Universal Innovative Research Publication*, 1(2), pp. 58–74, doi: 10.5281/zenodo.10148558.

Haluza, D. and Jungwirth, D., (2023). Artificial Intelligence and Ten Societal Megatrends: An Exploratory Study Using GPT-3. *Systems*, 11(3), pp. 1–18, doi: 10.3390/systems11030120.

He, T., (2019). The sentimental fools and the fictitious authors: rethinking the copyright issues of AI-generated contents in China. *Asia Pacific Law Review*, 27(2), pp. 218–238, doi: 10.1080/10192557.2019.1703520.

Illia, L., Colleoni, E. and Zyglidopoulos, S., (2023). Ethical implications of text generation in the age of artificial intelligence. *Business Ethics, the Environment & Responsibility*, 32(1), pp. 201–210, doi: 10.1111/beer.12479.

Jobin, A., Ienca, M. and Vayena, E., (2019). The global landscape of AI ethics guidelines. *Nature machine intelligence*, 1(9), pp. 389–399, doi: 10.1038/s42256-019-0088-2.

Kar, A.K., Varsha, P.S. and Rajan, S., (2023). Unravelling the impact of generative artificial intelligence (GAI) in industrial applications: A review of scientific and grey literature. *Global Journal of Flexible Systems Management*, 24(4), pp. 659–689, doi: 10.1007/s40171-023-00356-x.

Khowaja, S.A., Khuwaja, P., Dev, K., Wang, W. and Nkenyereye, L., (2024). Chatgpt needs spade (sustainability, privacy, digital divide, and ethics) evaluation: A review. *Cognitive Computation*, pp. 1–23, doi: 10.1007/s12559-024-10285-1.

Kietzmann, J., Lee, L.W., McCarthy, I.P. and Kietzmann, T.C., (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), pp. 135–146, doi: 10.1016/j.bushor.2019.11.006.

King, Y.M., (2023). Written Statement: Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith. *Chicago-Kent Journal of Intellectual Property*, 23 (1), pp. 124–126.

Ling, D., (2023). Analysis on Tort Liability of Generative Artificial Intelligence. *Science of Law Journal*, 2(12), pp. 102–107, doi: 10.23977/law.2023.021215.

Lucaj, L., van der Smagt, P. and Benbouzid, D., (2023). AI Regulation Is (not) All You Need. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency,* pp. 1267–1279, doi: 10.1145/3593013.3594079.

Maras, M.H. and Alexandrou, A., (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof*, 23(3), pp. 255–262, doi: 10.1177/1365712718807226.

Meskys, E., Kalpokiene, J., Jurcys, P. and Liaudanskas, A., (2020). Regulating deep fakes: legal and ethical considerations. *Journal of Intellectual Property Law & Practice*, 15(1), pp. 24–31.

Mittelstadt, B., (2019). Principles alone cannot guarantee ethical AI. *Nature machine intelligence*, 1(11), pp. 501–507, doi: 10.1038/s42256-019-0114-4.

Mondal, S., Das, S. and Vrana, V.G., (2023). How to bell the cat? A theoretical review of generative artificial intelligence towards digital disruption in all walks of life. *Technologies*, 11(2), pp. 1–17, doi: 10.3390/technologies11020044.

Montasari, R., (2024). Responding to Deepfake Challenges in the United Kingdom: Legal and Technical Insights with Recommendations. In: *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses*. Cham: Springer International Publishing, pp. 241–258, doi: 10.1007/978-3-031-50454-9_12.

Moulaei, K., Yadegari, A., Baharestani, M., Farzanbakhsh, S., Sabet, B. and Afrash, M.R., (2024). Generative artificial intelligence in healthcare: A scoping review on benefits, challenges and applications. *International Journal of Medical Informatics*, p. 105474, doi: 10.1016/j.ijmedinf.2024.105474.

Pérez, J., Castro, M. and López, G., (2023). Serious Games and AI: Challenges and Opportunities for Computational Social Science. *IEEE Access,* doi: 10.1109/ACCESS.2023.3286695.

Porsdam Mann, S., Earp, B.D., Nyholm, S., Danaher, J., Møller, N., Bowman-Smart, H., Hatherley, J., Koplin, J., Plozza, M., Rodger, D. and Treit, P.V., (2023). Generative AI entails a credit — blame asymmetry. *Nature Machine Intelligence*, pp. 1–4, doi: 10.1038/s42256-023-00653-1.

Romero Moreno, F., (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. International Review of Law. *Computers & Technology*, pp. 1–30, doi: 10.1080/13600869.2024.2324540.

Shoaib, M.R., Wang, Z., Ahvanooey, M.T. and Zhao, J., (2023). Deepfakes, misinformation, and disinformation in the era of frontier ai, generative ai, and large ai models. *2023 International Conference on Computer and Applications (ICCA)*, pp. 1–7, doi: 10.1109/ICCA59364.2023.10401723.

Thongmeensuk, S., (2024). Rethinking copyright exceptions in the era of generative AI: Balancing innovation and intellectual property protection. *The Journal of World Intellectual Property*, pp. 1–15, doi: 10.1111/jwip.12301.

Uzun, L., (2023). ChatGPT and academic integrity concerns: Detecting artificial intelligence generated content. *Language Education and Technology*, *3*(1), pp. 45–54. Available at: http://www.langedutech.com/letjournal/index.php/let/article/view/49/36 [Accessed 11.05.2024].

Yang, Z., Wu, J.G. and Xie, H., (2024). Taming Frankenstein's monster: Ethical considerations relating to generative artificial intelligence in education. *Asia Pacific Journal of Education*, pp. 1–14, doi: 10.1080/02188791.2023.2300137.

Information about the Authors

Animesh Kumar Sharma, PhD in Marketing, Research Scholar, Mittal School of Business, Lovely Professional University, Phagwara, Punjab, India
mr.animesh@gmail.com
ORCID: 0000-0002-6673-319X

Dr. Rahul Sharma, PhD in Marketing, Professor, Mittal School of Business, Lovely Professional University, Phagwara, Punjab, India
rahul.12234@lpu.co.in
ORCID: 0000-0001-8880-7527