International Journal of Computer Engineering and Technology (IJCET)
Volume 16, Issue 3, May-June 2025, pp. 37-46, Article ID: IJCET_16_03_003
Available online at https://iaeme.com/Home/issue/IJCET?Volume=16&Issue=3
ISSN Print: 0976-6367; ISSN Online: 0976-6375; Journal ID: 5751-5249
Impact Factor (2025): 18.59 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJCET_16_03_003

ETHICAL AND LEGAL ISSUES IN ARTIFICIAL INTELLIGENCE

Jyoti Kunal shah

USA.

ABSTRACT

Artificial Intelligence (AI) has revolutionized multiple sectors, but it has also introduced significant ethical and legal challenges. This paper discusses four critical areas: bias and discrimination, privacy concerns, accountability, and intellectual property (IP). As AI adoption accelerates, addressing these issues is essential to ensure fairness, transparency, and human right.

Artificial Intelligence (AI) is transforming industries and daily life, but it also raises significant ethical and legal challenges. Key concerns include the potential for AI systems to perpetuate bias and discrimination, threats to privacy through mass data collection and surveillance, difficulties in accountability for AI-driven decisions, and unresolved questions around intellectual property (IP) for AI-generated creations. Policymakers and regulators worldwide are grappling with these issues, aiming to promote innovation while safeguarding rights and societal values. Below is an in-depth overview of these four critical areas, including case studies, laws, and policy developments for each.

Keywords: Ethical issues in Artificial Intelligence, Legal implications of AI,AI bias and discrimination, AI and privacy concerns, AI accountability, AI and intellectual property, Algorithmic fairness, AI transparency and explainability, AI surveillance and data protection, AI governance frameworks, AI liability and regulation, Human rights in AI,AI ethics in law and policy, Bias in machine learning ,Facial recognition ethics, AI in criminal justice, AI-driven decision making, AI policy and compliance, Artificial Intelligence Law, AI ethics and accountability, Fairness in AI systems, Discrimination in algorithmic systems, Regulatory frameworks for AI,GDPR and AI compliance, Biometric data protection, Copyright and AI-generated works, Patent law and AI inventorship, AI governance and legal frameworks.

Cite this Article: Jyoti Kunal shah. (2025). Ethical and Legal Issues in Artificial Intelligence. *International Journal of Computer Engineering and Technology (IJCET)*, 16(3), 37-46.

https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_3/IJCET_16_03_003.pdf

Bias and Discrimination

AI systems can unintentionally **encode and amplify human biases**, leading to discriminatory outcomes. Machine learning models learn from historical data – if that data reflects societal biases, the AI may reproduce or even worsen those biases. This has been observed across multiple high-stakes domains:

- **Hiring:** AI recruiting tools have been found to favor certain demographics. A notable example is Amazon's experimental hiring algorithm, which was trained on past resumes and thus learned a preference for male candidates. It **penalized resumes containing the word "women's," (e.g. "women's chess club")** and downgraded graduates of women's collegesreuters.com. Amazon ultimately scrapped the tool upon realizing it was discriminating against women. Such **algorithmic bias in hiring** could violate equal employment laws by disadvantaging protected groups.
- **Lending and Finance:** Similarly, AI-driven credit scoring and loan approval algorithms have shown racial bias. A 2021 analysis by The Markup found **mortgage lenders using algorithmic underwriting were far more likely to reject minority applicants** compared to white applicants with similar profiles – **40% more likely for Latino borrowers, 80% more likely for Black borrowers, etc.brookings.edu**.
- **Policing and Criminal Justice:** AI tools used in law enforcement have exhibited troubling biases. For example, risk assessment software in U.S. courts (like the COMPAS system) was found to falsely label Black defendants as high risk at **nearly twice the rate of white defendants** – meaning Black individuals were far more often

incorrectly predicted to re-offendpropublica.org. Conversely, white defendants were more frequently misclassified as "low risk" when they did pose a riskpropublica.org. These disparities, revealed by a ProPublica investigation, highlight how **"black box" algorithms can exacerbate racial inequities in sentencing and bail decisionspropublica.org**.

- **Healthcare:** Bias in AI can even affect life-and-death decisions. One study uncovered that a widely used hospital algorithm for allocating extra care was biased against Black patients. The program, used to identify patients who would benefit from high-risk care management, **routinely ranked healthier white patients above sicker Black patients** for the same level of neednews.uchicago.edu. The bias arose because the algorithm used healthcare spending as a proxy for health: due to systemic inequities, less money was spent on Black patients with equal illness, causing the AI to underestimate their risk. Once this bias was revealed, researchers noted that **adjusting the algorithm could more than double the number of Black patients flagged for needed high-risk carenews.uchicago.edu**. This case shows how seemingly neutral metrics can mask prejudice, and if uncorrected, AI in healthcare could deny critical services to marginalized groups.

These examples illustrate that **AI systems can perpetuate existing social biases – or even create new forms of discrimination – in areas like employment, finance, policing, and health care.** The ethical implications are profound: AI may unfairly limit individuals' opportunities or resources based on race, gender, or other protected traits, thus reinforcing inequality under the guise of algorithmic objectivity.

Legal implications: When AI systems make decisions that adversely affect people, longstanding anti-discrimination laws typically still apply. In the United States, for instance, **an employer cannot use an AI hiring tool that has a "disparate impact" against protected groups** (race, sex, etc.) without violating Title VII of the Civil Rights Act. The U.S. Equal Employment Opportunity Commission (EEOC) has made clear that **the same standards for disparate impact in hiring apply to AI algorithms as to any other selection procedure**akingump.comakingump.com. If an AI recruiting tool selects female or minority applicants at less than 80% the rate of others (the "four-fifths rule"), the employer could be liable unless the tool is validated as job-related and necessaryakingump.com.

Proposed regulatory responses: Recognizing the risks of algorithmic discrimination, regulators and lawmakers are developing specific measures to audit and constrain biased AI. A pioneering example is New York City's **Local Law 144 (2021)**, which **requires annual**

independent "bias audits" of automated employment decision tools used by employers hiring in NYCnyc.gov. Under this law, employers must evaluate their hiring AI for disparate impact across gender and racial categories and publicly report the results before using the toolnyc.gov. Although the law doesn't mandate specific fixes based on the audit, it forces transparency and puts firms on notice that biased tools could run afoul of anti-discrimination lawsnyc.gov. Elsewhere, the EU's proposed **AI Act** will classify many recruitment, credit, and law enforcement AI systems as "high-risk," subjecting them to strict requirements for risk assessment and bias mitigation. The White House has also issued a non-binding **"Blueprint for an AI Bill of Rights"** (2022) which includes Algorithmic Discrimination Protections as a core principle, calling for testing AI systems for bias and protecting individuals from unfair algorithmic decisions. In short, there is growing consensus that **algorithmic fairness must be proactively managed** through audits, transparency, and updates to discrimination laws, to prevent AI from **entrenching systemic biases** in society.

Privacy Concerns

AI's hunger for data and the capabilities of modern surveillance technologies poses serious **privacy threats**. From the collection of personal data to the deployment of AI-driven surveillance, there are widespread concerns about how AI may erode individual privacy and civil liberties:

- **Mass Data Collection & Consent:** AI systems – especially those using machine learning – often rely on huge datasets, which can include personal information collected from users (e.g. online behavior, location, social media posts) sometimes without explicit consent. This raises questions about whether individuals have meaningful control over their data. For instance, large language models have been trained on text and images scraped from the internet, potentially ingesting private content or personal identifiers without people's knowledge. **Using copyrighted or personal data to train AI without consent** not only implicates IP (as discussed later) but also privacy:
- **Surveillance and Facial Recognition:** Advances in computer vision and AI-driven analytics have supercharged surveillance capabilities, enabling **real-time facial recognition and automated monitoring** of public spaces. This raises profound civil liberties issues. Authoritarian regimes have used AI surveillance to track and control populations, but even democratic societies are wrestling with the balance between security and privacy. **Facial recognition technology in particular has prompted backlash** due to its invasiveness and potential for misuse. In the United States, several

cities responded by banning or restricting government use of facial recognition. *San Francisco, for example, became the first U.S. city (in 2019) to ban police and city agencies from using facial recognition technology*npr.org, citing concerns over privacy and the technology's demonstrated racial biasesnpr.org.

- **Biometric Data and Monitoring:** Beyond facial images, AI systems can collect or infer other biometric and personal data – from voices and fingerprints to patterns of movement or even emotion recognition. The use of AI to analyze surveillance camera footage, track individuals across devices, or monitor workers (e.g. AI evaluating employees' keystrokes or attention) all raise privacy red flags. Biometric data is highly sensitive; misuse can lead to identity theft or unlawful profiling. **General Data Protection Regulation** (GDPR) classifies biometrics as "special category" data with added protections. Some jurisdictions have passed specific biometric privacy laws: the U.S. state of Illinois's **Biometric Information Privacy Act (BIPA)** requires companies to obtain informed consent before collecting someone's biometric identifiers (like face scans or fingerprints). This law has been used to sue companies deploying facial recognition without consent. In 2022, for instance, **Clearview AI** – an American company known for scraping billions of online photos to build a facial recognition database – settled a BIPA class-action lawsuit and agreed to restrict sales of its database in the U.S.aclu.org.
- **Personal Data and Profiling:** AI algorithms are increasingly used to profile individuals – predicting traits or behaviors (creditworthiness, health risks, likelihood to commit a crime, etc.) from data. Such profiling can be invasive and error-prone. Notably, California in 2023 amended its privacy law to include provisions about automated decision-making and even **"neural profiles,"** signaling recognition that AI uses of personal data need oversightconnectontech.bakermckenzie.com.

In summary, **AI poses privacy concerns both from the supply side (mass data used to train and fuel AI) and the deployment side (AI-enabled surveillance and decision-making)**. Legal frameworks like GDPR and CCPA are being tested and refined to address these issues – by requiring transparency, consent, data minimization, and giving individuals rights over automated decisions. Regulators are actively penalizing egregious privacy violations by AI (as seen in the Clearview cases). Still, the **ethical challenge** remains: how to reap AI's benefits in areas like security or personalization **without creating a "Big Brother" society**. Ongoing policy efforts, like the EU AI Act's bans on unacceptable surveillance practicesalgorithmwatch.org, aim to draw bright lines. But finding the right balance between innovation and privacy will likely require continual adjustment of laws as AI technology evolves.

Accountability

As AI systems play a greater role in decisions that affect humans, a pressing issue is **accountability: who is responsible when AI makes a mistake or causes harm?** This question encompasses challenges around **transparency**, **explainability**, and **legal liability** for AI-driven outcomes.

Black-Box Algorithms and Transparency: Many AI models, especially deep learning neural networks, operate as "black boxes" – their internal decision logic is complex and not easily interpretable, even by their creators. This opaqueness makes it hard to understand *why* an AI produced a given result. For example, if an AI system denies someone a loan or recommends a prison sentence, the affected person (and regulators) will want to know the rationale. However, AI algorithms often lack clear reasoning that can be communicated. The result is an accountability gap: **AI's autonomy and complexity make its decision-making processes "opaque and difficult to trace," which in turn "makes it more challenging to pinpoint the exact cause of harm and hold any party accountable" when things go wrongnatlawreview.com**.

Legal Liability and "Who to Blame": Under existing law, AI is not recognized as a legal entity – an AI cannot be sued or held liable in its own right. **Liability must therefore be traced back to the humans or organizations behind the AI**dailyjournal.com. This typically means the developer, the company deploying the AI, or other involved parties could be held responsible. The **emerging consensus** is that **organizations should be held liable for damages caused by their AI systemsnatlawreview.com**, rather than allowing an "accountability vacuum." However, implementing this is complex.

Regulatory developments in accountability: Governments are beginning to update laws to clarify AI accountability. A prominent effort is in the European Union, which in 2022 proposed two new legal frameworks: a revision to its Product Liability Directive and a dedicated **AI Liability Directive**. The **revised Product Liability** rules would explicitly cover software and AI systems, meaning if an AI product causes physical harm or property damage, it could trigger strict product liability (the injured person wouldn't need to prove the company was negligent, only that the AI was defective and caused harm)natlawreview.com.

Explainability and oversight: A key aspect of accountability is making AI **transparent and explainable.** Ethically, many argue that AI decisions affecting people's lives should not be a mysterious "black box." There is a push for **"Explainable AI" (XAI)** – techniques to make AI's workings more interpretable. Regulators are also considering mandates for **human oversight**. For example, the EU AI Act will require that users are informed when they are interacting with an AI system and, for high-risk AI, that systems are designed to allow human intervention or reviewnatlawreview.com

Intellectual Property

The rise of AI has generated difficult questions in **intellectual property law**, particularly regarding **AI-generated content and inventions**. Traditional IP regimes – copyright and patent – assume a human author or inventor. When creative works or novel inventions are produced with the significant involvement of AI, it challenges fundamental concepts of authorship, inventorship, and ownership.

Copyright and AI-Generated Works: Copyright law protects "original works of authorship" – historically understood to require a human creator exercising creativity. This raises the question: if an AI **writes a poem, composes music, or generates an image**, who (if anyone) owns the copyright? Under current law in most jurisdictions, the answer is that purely AI-generated works **are not eligible for copyright protection** because they lack human authorship. U.S. policy has been unambiguous on this point. In a 2023 decision, a U.S. federal court upheld the Copyright Office's denial of registration for an image that was created autonomously by an AI system (with no human creative input). The court reaffirmed that **copyright is reserved for "works of human creation"** and noted that no court has ever recognized copyright in a work originating from a non-human entityitsartlaw.org. Thus, when an AI produces content entirely on its own, the output is effectively **public domain** or unprotected – anyone could potentially reuse it, absent some new law to the contrary.

Patents and AI-Generated Inventions: Patent law faces a parallel dilemma with inventions claimed to be conceived by AI. Patents require an inventor who conceived the invention's idea. In recent years, a researcher, Dr. Stephen Thaler, tested this boundary by listing an AI system named "DABUS" as the sole inventor on patent applications for a novel food container and a flashing light device. Patent offices around the world uniformly **refused to recognize the AI as an inventor**, maintaining that inventorship is limited to natural persons. In late 2023, the UK Supreme Court definitively ruled that **"a machine which embodies an AI system could not be an inventor"** under UK patent law, aligning with earlier decisions in the U.S., EU, and Australia that only human beings can be inventorswhitecase.com.

Ownership and IP of AI Outputs: Aside from authorship/inventorship, another IP complexity is determining who owns or can exploit AI-generated content. For copyright, if a work has no human author, effectively no one automatically owns it – which can be problematic for those investing in AI creativity. Companies often address this contractually, claiming ownership over AI outputs via terms of service, even if the output isn't formally copyrighted. In patents, if an AI is not an inventor, any patent must be in the name of a human – for now, typically the AI's user or developer – or no patent is granted.

Use of Protected Material in Training AI: Another major IP issue in AI is the **training data**. AI models often learn from large corpora of text, images, music, etc., which may be copyrighted by others. Is ingesting these works to train an AI an infringement, or is it allowed (perhaps as fair use or an exception)? This question is the subject of active litigation. In 2023, groups of artists and authors filed lawsuits against AI companies (like the makers of image generator Stable Diffusion and services like Midjourney and OpenAI) alleging that **the unauthorized use of millions of their copyrighted works in training AI models infringes their rights**reuters.com.

In summary, **IP law is being stress-tested by AI**. The current legal consensus is conservative: AI cannot be an author or inventor, and thus **human creativity remains the cornerstone of IP protection**itsartlaw.orgwhitecase.com. But this can leave AI-generated outputs in a grey area regarding ownership and protection. Going forward, lawmakers may need to decide whether to adapt IP laws to new realities (for instance, by introducing a new category of rights for AI-generated works, or by clarifying how human creators who use AI can claim ownership). Until then, anyone using AI to produce creative or inventive works should be aware that **the fruits of AI might not receive the same legal protection as traditional works**, and traditional IP strategies (copyright registrations, patent filings) may not be available unless a sufficient human role is present.

Conclusion

AI's transformative power comes bundled with complex ethical and legal dilemmas. **Bias and discrimination** in AI remind us that technological progress is not automatically equitable – without deliberate checks, AI can mirror and magnify societal prejudices, prompting regulators to enforce fairness and civil rights in algorithmic decisions. **Privacy concerns** underscore the need to protect personal data and autonomy in an era of ubiquitous AI surveillance and data-hungry algorithms; laws like GDPR and new AI-specific rules are at the forefront of this effort, drawing lines around acceptable uses of AI with respect to human privacy. **Accountability** for AI systems is crucial to ensure that as we delegate decision-making to machines, we do not lose the ability to govern their outcomes – this has led to calls for greater transparency, explainability, and updated liability frameworks so that responsibility always traces back to a human or company. In the realm of **intellectual property**, AI is challenging the very definitions of creator and inventor, forcing a reexamination of how we incentivize and protect creativity and innovation when they emerge from human-machine collaboration.

These four areas are deeply interconnected. For instance, lack of accountability and transparency can exacerbate bias, and privacy invasions can feed biased or unaccountable AI systems. The legal system is beginning to respond through a combination of **enforcing existing laws** (applying anti-discrimination laws, privacy regulations, product liability law, etc. to AI) and **crafting new policies** (such as the EU AI Act's comprehensive rules, or various legislative proposals in the US and elsewhere). Ethically, there is increasing recognition that AI development must be guided by principles of fairness, respect for persons, and **"do no harm."** Initiatives like ethical AI guidelines, industry best practices, and international agreements are attempting to set norms for AI that complement formal laws.

In conclusion, while AI holds immense promise, it also presents ethical pitfalls and legal uncertainties that society must navigate. Ensuring that AI systems are **fair, privacy-preserving, accountable, and respect intellectual property** will require ongoing vigilance and adaptation of our legal frameworks. The conversation between technologists, ethicists, lawmakers, and the public is more important than ever to steer AI in a direction that upholds human values and rights. By learning from early case studies and proactively addressing these issues, we can harness AI's benefits while mitigating its risks – striving for an AI-infused future that is both innovative **and** justalgorithmwatch.org.

References

[1] reuters.com: Insight - Amazon scraps secret AI recruiting tool that showed bias against women | Reuters

[2] brookings.edu: The legal doctrine that will be key to preventing AI discrimination

[3] propublica.org: Machine Bias — ProPublica

[4] news.uchicago.edu: Health care prediction algorithm biased against black patients; study finds | University of Chicago News

[5] akingump.com: EOC Releases New AI Guidance for Employers | Akin Gump Strauss Hauer & Feld LLP

[6] nyc.gov: Automated Employment Decision Tools: Frequently Asked Questions

[7] npr.org: San Francisco Bans Use Of Facial Recognition Technology By Municipal Government: NPR

[8] algorithmwatch.org: As of February 2025: Harmful AI applications prohibited in the EU - AlgorithmWatch

[9] aclu.org: In Big Win, Settlement Ensures Clearview AI

[10] reuters.com: Clearview AI fined by Dutch agency for facial recognition database | Reuters

[11] connectontech.bakermckenzie.com: Minding Your Data: New Law Expands CCPA's Sensitive Personal

[12] natlawreview.com: Governing AI Risks: Challenges in Liability Laws

[13] dailyjournal.com: Legal liability concerns in artificial intelligence: What you need to know

[14] itsartlaw.org: Case Review: Thaler v. Perlmutter (2023) - Center for Art Law

[15] whitecase.com: UK Supreme Court Rules Against AI Inventorship of Patents | White & Case LLP

[16] reuters.com: Judge pares down artists' AI copyright lawsuit against Midjourney, Stability AI | Reuters

Citation: Jyoti Kunal shah. (2025). Ethical and Legal Issues in Artificial Intelligence. International Journal of Computer Engineering and Technology (IJCET), 16(3), 37-46.

Abstract Link: https://iaeme.com/Home/article_id/IJCET_16_03_003

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_3/IJCET_16_03_003.pdf

✉ **editor@iaeme.com**