World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Navigating the Intersection of U.S. Regulatory Frameworks and Artificial Intelligence: Strategies for Ethical Compliance

Tessy Oghenerobovwe Agbadamasi [1], Lois Kumiwaa Opoku [2], Tobias Kwame Adukpo [3,*] and Nicholas Mensah [4]

[1] *Department of Business Intelligence and Data Analytics, Westcliff University Los Angeles, CA.*
[2] *Department of Crop and Soil Sciences, Kwame Nkrumah University of Science and Technology, Ghana.*
[3] *Department of Accounting, University for Development Studies, Ghana.*
[4] *Department of Accounting, University of Ghana.*

World Journal of Advanced Research and Reviews, 2025, 25(03), 969-979

Publication history: Received on 04 February 2025; revised on 12 March 20215 accepted on 14 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0814

Abstract

Artificial Intelligence (AI) has rapidly evolved, transforming sectors such as healthcare, finance, and transportation while raising complex ethical, legal, and societal concerns. This research examines the current state of AI ethics and regulation in the United States, evaluating whether existing frameworks are sufficient to govern emerging AI technologies and mitigate associated risks. The study aims to analyze the U.S. regulatory landscape, identify ethical challenges, and propose actionable measures for compliance and responsible AI deployment. Drawing from interdisciplinary literature, the research reviews major U.S. policies, including the Federal Trade Commission Act, Algorithmic Accountability Act, and Health Insurance Portability and Accountability Act (HIPAA), to assess their capacity to address key issues such as algorithmic bias, privacy protection, and system transparency. The analysis reveals that while these laws provide foundational oversight, they fall short in addressing the scale and complexity of contemporary AI systems. Significant findings show that AI-powered tools often perpetuate social biases in areas like hiring, lending, and law enforcement, whereas opaque algorithms undermine accountability and public trust. The empirical studies revealed that privacy is increasingly at risk, particularly through AI-driven surveillance and data collection practices that lack sufficient safeguards. The study concludes that a unified, comprehensive regulatory approach is essential to ensure fairness, accountability, and respect for individual rights. Recommendations include integrating ethical principles directly into legislation, fostering inter-agency collaboration, and promoting international cooperation to harmonize AI standards. Ultimately, this research advocates for proactive governance strategies to support the responsible growth of AI technologies while safeguarding societal values and human dignity.

Keywords: AI Privacy; Fairness; Transparency; Ethics; Ethical Compliance

1. Introduction

Artificial Intelligence has experienced remarkable growth and has permeated nearly every aspect of society and the economy [1][39][34]. From healthcare to finance, education to transportation, the potential of AI to drive efficiency, innovation, and new value propositions is unprecedented [2][29]. However, these advancements have also raised significant questions about the ethical implications and the need for proper governance to ensure fair and transparent results [3][39].

AI ethics is a field that draws from various disciplines, with the central focus being the ethical problems and consequences of AI development and application [3][39]. At its core, AI ethics delves into the complex web of ethical

* Corresponding author: Tobias Kwame Adukpo

considerations that arise from the use of artificial intelligence, examining the far-reaching impacts on individual privacy, human rights, social justice, and the overall well-being of society.

The boundaries of AI ethics encompass far more than just identifying risks; it involves a comprehensive strategy for ensuring that AI technologies are beneficial, promote respect for human rights, and contribute to the common good [4]. This entails not only the technical qualities and characteristics of creating AI systems that are fair, reliable, and safety-driven, but also the external impacts of AI system applications, such as employment concerns, social equity, and the digital divide [3][5][6]. Navigating the ethical landscape of AI is a multifaceted and complex endeavor that requires a holistic approach. This paper aims to provide a comprehensive overview of the current state of AI ethics, highlighting the key principles, challenges, and potential solutions for governing the responsible development and deployment of artificial intelligence.

AI ethics is a branch of study in which knowledge is comprised of various fields of science where the main subject of interest relates to the ethical problems and consequences of AI development and application [39].

AI ethics helps in improving the understanding of the current and future scenarios of IT, specifically in connection with the use of artificial intelligence in various facets of life. For example, employment concerns, social justice and equity, or the digital divide. AI ethics also studies what becomes of the process over some extended period of time, including questions about ownership, the question of decision-making by AI systems, and the future [5].

In this way, AI ethics aims at ensuring positive interaction between humans and AI systems and addresses concerns that are as follows, interaction with machines, guaranteeing that the relevant technologies are created with full regard to their ethical Unauthorized translation, Dependency of humans and future AI's, that is making sure that AI technologies are built with ethical consequences and are carried out in processes that favor improvement as opposed to the depreciation of human worth and its related legal rights.

Currently, there is no unified and centralized approach for AI regulation in the USA; at present, it is a job for several agencies and actors. The objectives of this paper are as follows; analyze the current status of the regulatory environments in the U.S. that are related to AI, determine the ethical issues, and recommend tangible measures towards working compliance.

1.1. Evolution of AI Technologies

The rapid proliferation of AI technologies has led to a global convergence around some ethical principles: privacy, liberty, equality and freedom, rationality, justice, and reasonableness [6]. AI algorithms such as deep learning, generative models, and reinforcement learning have expanded AI's capabilities, enabling applications in predictive diagnostics, autonomous vehicles, and conversational agents like ChatGPT [1][28]. The founding of AI involves escaping from the narrow speculation of entertainment and film gnomes' humor and successfully defining itself as a discipline of science can be dated back to a conference that was held in Dartmouth College in 1956 by luminaries John McCarthy, Marvin Minsky, Allen Newell, and Herbert A. Simon's which sought to find how machines could imitate aspects of human intellect [7]. Advances in AI are increasing, but not without several ups and downs which are known as AI winters, which are times of decreased development potential due to technological or funding issues. However, the progress in graphical models and mathematical optimization in particular, and machine learning, and neural networks at the turn of the twentieth and twenty-first centuries, computing power growth, and data availability initiated a new wave of interest in AI. The current generation has seen the development of superior artificial intelligence structures that are capable of mimicking human performance in unique chores [31][32].

As AI technologies continue to mature, their societal impact is becoming more pervasive, raising critical questions about ethical deployment.

1.1.1. Challenges and Opportunities in AI

The opportunities presented by AI are vast, including enhanced efficiency, innovation, and problem-solving capabilities. However, the challenges are equally pressing. Issues such as algorithmic bias in hiring systems, privacy breaches through facial recognition, and the opaque nature of AI-driven decisions highlight the need for regulatory oversight. In the U.S., addressing these challenges requires navigating a unique regulatory environment characterized by decentralized governance and sector-specific policies [8][40][35].

Artificial Intelligence technologies have experienced rapid advancements and have become ubiquitous across various industries, profoundly disrupting society [9][30][33]. From healthcare diagnostics to financial trading, AI-powered

systems are now capable of performing tasks that previously required human input, often with greater accuracy and efficiency [10][36][34]. In the healthcare sector, AI-driven diagnostic systems have demonstrated the ability to analyze medical images, such as X-rays and MRI scans, and provide recommendations for appropriate treatments, potentially streamlining the diagnostic process and aiding medical professionals in their decision-making [11]. Similarly, in the financial domain, AI algorithms have been employed for automatic trading and fraud detection, enhancing the speed and precision of these operations [2].

However, the widespread adoption of AI in societies presents significant social dilemmas [12]. The increased use of robots and automation in the workplace has led to concerns about job displacement and redundancy, as certain tasks and roles can be automated, potentially disrupting traditional employment patterns. Moreover, the data-driven nature of AI systems has raised concerns about privacy, data control, and the potential for biased decision-making that reinforces prejudicial views [11][13][37]. As these AI-powered technologies continue to evolve, it is imperative to carefully consider the ethical implications and ensure that the development of AI systems is guided by principles that mitigate the negative societal impacts while harnessing the significant benefits they offer [10][12][13].

2. Literature Review

2.1. Current U.S. Regulatory Frameworks Governing AI

The U.S. lacks a single, comprehensive AI law, relying instead on a patchwork of sector-specific guidelines. Key frameworks include:

- **The Federal Trade Commission Act (FTC Act)**: This Act focuses on preventing unfair or deceptive practices, with implications for AI transparency and accountability [14]. With the help of the Federal Trade Commission (FTC), many cases involving violations of laws in the sphere of AI have been considered over the years. FTIC investigates various companies in that sphere. For example, the Equitable Credit Reporting Act passed in 1970, and the Equal Credit Opportunity Act passed in 1974 deal with portions of automated decision-making. Credit risk assessment becomes possible through the application of these laws to credit underwriting models fueled by artificial intelligence [15]. Furthermore, the FTC has brought enforcement actions under Sections 5 and 6 (FCT Act) accusing entities of engaging in unfair and deceptive practices, and consumer harm arising from the application of artificial intelligence and digital systems.

In 2016, the FTC published a report titled ***Big Data***: That is Why it is named a Tool for Inclusion or Exclusion, to which those companies using big data analytics machine learning should contribute to avoid the risk of bias [16] . Later in November 2018, the FTC conducted a hearing considering AI, algorithms, and predictive analytics as the subjects of discussion [16] . In enforcing the Act, undertaking studies, and providing guidelines on the use of AI, FTC has maintained the democratic message that AI systems are expected to be transparent and intelligible: They must also be fair, evidence-based, and the subject of accountability. This reasoning is based on the vast practical experience of the Commission, as well as the existing legislation, which provides important guidance for companies that face and may need to address the challenges of consumer protection in relation to AI and algorithms.

- **The Algorithmic Accountability Act**: This Act aims to require impact assessments for high-risk automated systems to address bias and discrimination [17]. This act gives certain requirements to particular kinds of businesses that primarily employ automated decision systems for making important decisions and are used for checking the impact of such systems on consumers. High-stakes decision-making is described as the occasions when a consumer's life-altering choices involve relying on information that may be false or misleading including the cost of healthcare, housing, education, or financial services [18]. The FTC working with stakeholders has the responsibility of developing regulations that will support the bills. The enforcement responsibilities are given to the FTC and other designated officials of the state. Also, the bill authorizes the creation of a Bureau of Technology that is going to supply the FTC with specific knowledge about the technological side of this agency.
- **The Health Insurance Portability and Accountability Act (HIPAA)**: This Act governs the use of AI in healthcare, ensuring data privacy and security [19]. The Privacy Rule aims at setting guidelines for the utilization and disclosure of individuals' PHI and applies to entities known as ''covered entities.'' It also establishes privacy provisions protecting people's rights to learn how and in what manner their health information is being used [19]. The rule protects PHI while allowing legitimate access to foster quality healthcare delivery and public health. In keeping with the privacy and confidentiality of patients and clients along with the high stakes associated with health data and informatics uses, the Privacy Rule thus allows

appropriate uses of health data while equally preserving the confidentiality of individuals seeking healthcare services.

2.1.1. Addressing Ethical Challenges

These regulations tackle ethical issues to varying extents:

- **Bias**: The FTC has emphasized the need for fairness in AI algorithms, as evidenced in cases involving biased hiring tools [14]. The discussion of the biases and the fairness in machine learning and artificial intelligence (both AI) show how those technologies continue to amplify or even aggravate existing social prejudices that would be a question to ethical standards [16]. Any AI system, especially those based on machine learning algorithms, for instance, acquires information from large databases. There are two scenarios for such datasets: These datasets contain historical biases and/or no historical datasets. Since the AI system serves as a representative of diverse populations, those prejudices are embedded in the system and can worsen them. Facial recognition is one of the widely known AI applications. Research has noted that many of the facial recognition software have higher disparities in error rates between women and people of color compared to white men [21] . This results in a separation between training datasets that mainly contain white population images, which means that its ability to identify features of the faces of people of color is lower in underrepresented groups. The consequences are rather vast and range from wrongful arrests due to wrong identification in police work, all the way to social media identification in everyday practices such as tagging, thus affirming the exclusion of people with albinism and discrimination of specific individuals. A second domain that has extensively been considered AI bias is in decision-making applications, especially in areas like hiring, lending, and criminal justice. In hiring, AI tools would use algorithmic means and match such data with what had been learned from previous hiring may lead to a continuation of some categories of prejudices, for example, due to prejudices of gender or race if earlier employee hiring contained preferences for some categories of people [21] . In lending, algorithms credit risk identification could be prejudicial to persons from low-income or colored groups because historical financial data may have some bias [18]. Likewise, “risk assessment instruments used in the criminal justice system relating to that of the sentencing and bail decisions are discriminatory towards minority races possibly resulting in severe penalties.” recurring systemic forms of disadvantage. These cases are the urgent necessity of measures that guarantee fairness and eliminate the bias of AI systems. Several approaches to addressing fairness in AI include using a variety of training data to face the problem of excluding some particular group of individuals [7]. Integrating the principles of fairness into the creation of algorithms and conducting frequent checks of biases along the system’s life cycle of AI systems for preconfigured results. Furthermore, interaction with various members during the construction and implementation of AI technologies should be understood as consisting of four layered elements, and thus the investigation of bias and fairness must address each of them. Addressing these challenges is not only the task of specialists but also a social responsibility for AI development to be useful and positive melding across different sectors or society to promote individual equitability.
- **Transparency**: The National Institute of Standards and Technology, NIST’s AI Risk Management Framework promotes explainable AI systems to improve accountability [7]. As such, the questions of responsibility and responsibility in artificial intelligence (AI) remain the core of the ethical use of these technologies, raising substantial problems of how to control the understandable behavior of such systems. And that there are agent capabilities for such outcomes to be causally linked and made actionable and accountable for [7]. As AI systems are becoming intricate and self-sufficient, getting a clear perspective of how such systems arrive at decisions only gets tricky. This complexity can result in situations that are called “black boxes” because the way the AI algorithms work cannot be explained to a human. Thus, making it difficult to evaluate the efficiency, effectiveness, fairness, and safety of these decisions. Transparency has been put forward as the key component of accountability in the case of AI [7] . Whenever an AI system commits an error, or produces a biased result, it is challenging to apportion blame since the AI development and deployment involve many strata such as data providers, algorithm developers, and end-users [7]. Several research has noted that many of the facial recognition software have higher disparities in error rates between women and people of color compared to white men. This diffusion of responsibility makes it difficult for anybody to make clear reference to a single entity that is responsible for the wrongs done by AI systems. For example, it is entirely possible for an AI-based healthcare system to incorrectly diagnose a patient's harm, working out whether this is due to defects within the dataset, the algorithm, or the method of deployment is needed.
- **Privacy**: HIPAA enforces stringent data protection measures, relevant to AI applications in medical research [8]. Privacy as well as surveillance with artificial intelligence (AI) entails a complex of ethical decisions since AI is advanced in handling large amounts of data of people. AI-driven surveillance systems, such as facial recognition and predictive policing, highlight the dual-use nature of these technologies [7]. On the positive side,

they can bring various positive effects for society but at the same time, pose big threats to people's privacy and rights. Out of all the issues discussed, the one that raised the most concerns is facial recognition technology, already actively used by institutions throughout the territory and in public areas [8][39]. What it does is that it increases security and makes identity authentication easier while at the same time compromising privacy as people can be observed time and again without their consent. Real-time recognition and the lack of overall legal regulation in many regions contribute to the AI system's lack of clear governance of its implementation. The presence of the surveillance culture at such a high level might discourage personal liberties because people change their behavior in light of perceived surveillance. The prophylactic use of artificial intelligence in identifying crime 'hotspots and risk assessment contributes to further enhancement of invasive surveillance [10]. These systems depend on mining intertwined large data that is frequently gathered without prior permission from the subject of interest to forecast the actions or conduct of an individual in the future [10][38]. Apart from privacy issues, such applications are speculative in their goals and suffer from fairness and accuracy issues because algorithms learn from the data it has been fed, which may produce racist results. Similarly, the role of Al in the commercial sphere while it primarily functions as accountable data miners to gather information about the consumer is transformative to its privacy [12][39]. With the help of AI, companies and organizations can more effectively use personal data for advertisement and behavior prediction but more and more people do not know how their data is gathered, analyzed, used, and sold. As a result of this lack of clarity, there have been increasing demands to limit or outright ban consumer data mining and utilization for business gain [13]. These ethical challenges show the important need for developing proper legal and ethical models for AI use in privacy and surveillance. Asserting private dignity demands governing AI use through the tenants of accountability, visibility, and permission. Hence the need for governments and regulators to conduct the right inspections to guarantee that the positive possibilities of AI technologies would not be felt with the infringement of citizens' privacy and rights within the digital realm [13][41].

2.2. Case Studies

2.2.1. COMPAS Recidivism Algorithm

One of the most used AI tools in the U.S. Criminal Justice System is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), developed by Northpointe, to predict a defendant's risk to recidivate the system has come under a lot of criticism for perpetuating racial prejudice even though the system has been praised for efficiency in the approval of parole and punishment determination [29]. The American technology news website ProPublica in 2016 found that the algorithm's predictions revealed massive racism differences [29]. From our perspective, this report also shows that COMPAS over-represented Black defendants as risky while under-representing white defendants, particularly in instances where they have not offended again. Specifically, the system committed the opposite error for white defendants and was nearly twice as likely to categorize Black defendants as high risk [9]. As a result, COMPAS's private structure, which does not admit external examination and verification of these findings, led to debates regarding the visibility of the scoring mechanism. Critics argue that such a decision-making process is not very transparent, which affects accountability, particularly in sensitive areas such as criminal justice [18]. The case has contributed towards demands for opening of algorithms, explanation, and fairness of automatons in decision-making, as well as broader debate on the ethical use of AI in life risky scenarios. Currently, advocates and researchers have come out to ask for Parliament to make it mandatory for there to be independent audits and bias mitigation practices for all algorithms used in the decisions on sentencing and parole [22] .

2.2.2. Clearview AI

The facial recognition business Clearview AI has been the subject of controversy, as per its critics who argued that the firm violates people's right to privacy [7]. Without the consent of the users, the business captured billions of photos from open sources that are available for public viewing like web pages, and social networking sites. High-quality facial recognition software was then created from such photos and was primarily marketed to corporations and police forces [23]. Clearview AI's solution is based on facial photos and a database where identification can take place immediately. Technological voices have been raising questions about the abuse of technology despite the company insurance that enhances the efficiency of law enforcement organizations and assists them in their criminal investigations. Due to multiple complaints about the effects of Clearview AI falsely representing itself and its practice and for violating consumer privacy laws, the Federal Trade Commission, commonly referred to as FTC launched an investigation into Clearview AI [10]. The business methods used to collect data may be in clear violation of laws like the Illinois Biometric Information Privacy Act (BIPA), which requires businesses to obtain prior consent to collect biometric identifiers. As concerns the problem of Clearview AI the demands toward setting more strict legal restraints for face recognition technology have become more vociferous including prohibitive of towards complete moratorium for using face eBooks

recognition technology in open spaces. The cases of unlawful taking of biometric data and facial recognition abuse have been highlighted by advocacy groups asserting the need for clear laws to protect people [11].

3. Ethical Challenges in AI Development and Deployment in the USA

3.1. Algorithmic Bias

A concrete risk of AI is when an algorithm acts in a discriminative or unfair way, based on the prejudice contained in the dataset used for its training phase [7]. Discriminatory biases present in such systems can only help perpetuate inequalities in our society especially when high-risk usage of the systems or tools are applied in areas like employment, health, or security. An example of algorithmic bias that is hard to miss is the facial recognition techs that are widely used. Research has indicated that facial recognition software shows a higher level of accuracy in identifying white males than Black, Asian, and Female individuals. For example, a study conducted in 2018 at MIT Media Lab discovered that the worst-performing commercial systems had 34.7% error rates on dark-skinned females and below 1% on light-skinned males [12]. This gives a clear indication that such technologies are not fair and give a lot of credit to researchers particularly when such technologies are used by law enforcement or government institutions. In real–life scenarios, these biases may result in wrong arrests or refusal of service based on wrong identification. There have been many demands made in trying to address algorithmic bias including diversifying training data, bias audits, and using fair constraints with AI models. The necessity to regulate such technologies is best illustrated by examples such as Amazon's Recognition, which was accused of errors and its ability to be misused by police departments [13].

3.2. Privacy Concerns

AI systems that collect and analyze vast amounts of personal data pose significant privacy risks. The Cambridge Analytica scandal exemplified how AI-driven data analytics could be misused for political manipulation. AI involves the use of big data as a primary asset as well as the collection and processing of large quantities and quality of personal data. As with any big tech company, there are large and inherent risks when it comes to data privacy, especially when data is captured, stored, or used with little or no protection or permission. AI data analytics app from the platform as manifested by the Cambridge Analytica fake news disaster serves as the best example [14]. The data processing scandal showed the problem of using AI in marketing in data processing and came into question the informed consent of data users and their right to be informed. For instance, AI-controlled smart home gadgets like voice assistants are bound to capture and process owners' data and frequently do so without explaining how the information will be utilized or shared [7]. Ideally, such practices can result in unauthorized disclosure or leakage of such data and additionally reduce consumer confidence.

3.3. Lack of Transparency

The term ''black box" of many AI systems means that it is hard to comprehend how the decisions made are arrived at. This is a major ethical issue befitting AI since it hinders users, and even the regulators, not to mention, developers from comprehending or having trust in those AI decision-making methodologies [7]. The applications of black-box algorithms are especially concerning industries whose decisions are likely to cause important implications, as are the fields of healthcare, finance, and criminal justice. For example, in the case of the COMPAS recidivism algorithm used to assess the likelihood of reoffending the black box nature of the system did not allow external auditors to understand exactly how the score was arrived at. As discussed before, research showed the overrepresentation of Black defendants as high risk by COMPAS and consequent unfairness and lack of responsivity [15]. Moreover, most AI systems are black-boxed; thus, when deployed, it becomes challenging for the regulators on how organizations are ethical or not or if they are violating certain laws likes as data protection or discriminating against clients or employees [16]. This clearly may lead to reduced trust because a person may feel helpless when facing results produced by a model for which he or she cannot explain or appeal.

4. Case Studies of Controversial Applications

4.1. Amazon's Recognition

This case was criticized for its inaccuracies and potential misuse in law enforcement. Said to be aimed at industries as diverse as law enforcement, public safety, and business security, Amazon Recognition is a cloud-based facial recognition service. Despite such features as real-time facial recognition, face matching in real-time, and video analysis, Recognition has been accused of numerous errors, including its ability to wrongly identify people of color [21]. A 2018 ACLU experiment used Amazon Recognition to find out that all its 535 members of the U.S. Congress photos were a match for

25,000 out of a database of publicly available mugshots. The software was able to incorrectly categorize 28 members of Congress as criminals with people of color being flagged at a higher proportion than white people even when the software was marketed as a tool that accurately sorts out criminals [17]. According to the experiences of such mistakes, the applicability of the program in policing leads to wrong arrests and racial profiling. Some of the critics of Recognition say it helps create a surveillance society, which compromises civil liberties and the right to privacy. The ACLU and several other groups also urged police departments to stop deploying facial recognition technology until there is regulation in place to address problems such as accuracy and bias. To mitigate the social pressure created by the ACLU, Amazon declared in 2020 that it would temporarily cease to offer Recognition to police departments for one year, although the technology needed more extensive regulatory supervision [18].

4.2. AI in Hiring

Tools like Hire Vue have faced allegations of perpetuating bias through unvalidated screening metrics. Some of the most prominent AI-driven hiring includes Hire Vue whereby companies are selecting smart Tal Rochester Institute of Technology Technical Report AI in Hiring Applying natural language processing for selection, seeking to build efficient mechanisms of talent attraction. These tools mainly employ artificial intelligence and machine learning techniques to identify and assess successful candidates from resumes, and video interviews to their behaviors [28]. Although presented as instruments designed to make the recruitment process more effective and freer from human prejudice, such systems have been accused of reproducing prejudice and discrimination. As recalled, one of the major areas of controversy in Hire Vue is the use of non-validated screening measures. The signup utilizes signals such as facial expressions, voice intonation, and lexical items to evaluate a candidate for a position. However, the experts pointed out that these indicators are poorly researched and may deviate from the social justice perspective, disadvantage candidates, mainly from a diverse background or disabled persons [19]. For instance, a certain candidate does not show certain behavioral attributes including leadership skills during an interview because he or she comes from a different culture and hence could be locked out. In 2019, Advocacy agencies such as the Electronic Privacy Information Center sued Hire Vue demanding the Federal Trade Commission investigate. EPIC also questioned the company's algorithms and the probability of discriminating against results since the training dataset contains bias [20]. In 2021, Hire Vue defended itself saying that it would cease to use facial analysis in its tests despite the criticism there is still too much use of AI in various hiring procedures. This case makes perfect sense when describing the major issues related to the usage of AI in hiring, more specifically, the problems of fairness, accountability, and transparency. With the growing use of AI in significant employment decisions, the implementation of tighter rules and algorithmic checks has grown louder.

5. Strategies for Ethical Compliance in AI

5.1. Transparency

Adopting explainable AI (XAI) principles can enhance transparency. Techniques such as model interpretability and post-hoc explanations are essential for regulatory compliance. Perhaps one of the most fundamental needs for all things AI is trust and that cannot be initiated until there's openness. Creating and using models that are easily understandable and capable of explaining themselves to regulators and end users [25]

5.1.1. Fairness

Implementing bias detection and mitigation strategies during model development can reduce discriminatory outcomes. Tools like IBM's AI Fairness 360 provide practical solutions [23]. Filtering bad algorithms in the same way to eliminate such results is called fair intelligence. Bias arises in most cases when algorithms enhance initial existing disparities or when training data do the same.

Methods and Tools for Detecting Bias: IBM also dreamed up AI Fairness 360 – an open-source kit designed to let you check datasets for prejudice and machine learning algorithms for racial bias, sexism, and the like [24]. Data scientists and developers can also use the tool to find out the impact of protected attributes, including age, gender, and race, on the models.

5.1.2. Accountability

Establishing clear lines of accountability through governance frameworks ensures that organizations can address ethical lapses effectively [18]. It is possible to successfully handle ethical transgressions in AI systems by establishing distinct lines of accountability. Determining the roles and duties of developers, organizations, and users in the creation, implementation, and oversight of AI systems is a crucial part of accountability. Companies can put in place governance frameworks that assess the moral consequences of AI projects. Independent evaluations can be put in place to confirm

adherence to legal and ethical requirements. Systems for recording the datasets, algorithms, and decision-making standards used in AI development processes are examples of internal accountability mechanisms. In AI Risk Management Framework, the U.S. National Institute of Standards and Technology (NIST) highlights accountability as a fundamental tenet, urging enterprises to keep thorough records of the development and decision-making processes of AI systems. [26]

5.1.3. Stakeholder Engagement

Inclusive policymaking that involves diverse stakeholders including technologists, ethicists, and affected communities can lead to more equitable AI governance [27]. Diverse stakeholders must contribute to the development of ethical AI to guarantee that systems are developed and implemented fairly. Collaboration between engineers, ethicists, legislators, and communities impacted by AI applications is encouraged by inclusive policymaking.

6. The Role of National Importance in AI Regulation

Ethical AI practices align with national priorities by:

- **Driving Economic Growth**: Responsible AI fosters innovation and market competitiveness. The present work highlights that ethical and responsible AI contributes to the development of the economy and the protection of market competitiveness. By incorporating AI into the healthcare, manufacturing, financial, and logistics sectors, countries are able to increase productivity, cut expenses, and generate new employment. Nevertheless, it is imperative for ethical compliance as the lack of it destroys public trust and results in lasting commercial disadvantages due to misapplication or backlash.
- **Enhancing National Security**: Ethical AI reduces risks associated with adversarial AI attacks and enhances trust in defense applications. AI is utilized in enhancing the national security front including information protection and defense use. Ethical AI practices mean that AI technologies used in security contexts are reliable and favorable for democracy.
- **Global Leadership**: The U.S. could set global standards for ethical AI, leveraging its technological and regulatory expertise. Ethical AI best practices are a foundation for nations to bring a leadership claim to the international level by setting benchmarks for creation and regulation. Those countries that invest in building proper AI regulations can set up the tone for international legislation and lead the discussion on the most important aspects of artificial intelligence.

6.1. Future Directions for U.S. AI Regulation

Emerging challenges posed by generative AI and its integration into critical infrastructure require adaptive and globally coordinated policies to ensure safety, security, and ethical use. The rapid rise of models like GPT-4 and Google Bard has highlighted difficulties in regulating AI-generated content, which can easily produce misinformation, deepfakes, and other harmful outputs. At the same time, as AI systems become embedded in vital sectors like health, transportation, and energy, ensuring their resilience against failure and cyber threats is crucial. Frameworks like the U.S. National AI Initiative Act and the EU Artificial Intelligence Act are important starting points but must evolve to address new risks. Additionally, international cooperation through efforts like the OECD AI Principles and the Global Partnership on AI (GPAI) is essential to harmonize standards, address data sovereignty concerns, and reconcile differing cultural and ethical approaches to AI governance, all while supporting innovation and responsible AI development worldwide.

7. Conclusion

Ethical compliance in AI is not merely a regulatory requirement but a societal imperative. By navigating the complex intersection of U.S. regulatory frameworks and AI technologies, this paper underscores the importance of fairness, transparency, and accountability. Stakeholders must act collaboratively to address ethical challenges and position the U.S. as a global leader in responsible AI innovation. The path forward demands proactive engagement, robust governance, and unwavering commitment to ethical principles.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Cowls, J., & Floridi, L. (2018). Prolegomena to a White Paper on an Ethical Framework for a Good AI Society. In SSRN Electronic Journal. RELX Group (Netherlands). https://doi.org/10.2139/ssrn.3198732

[2] Hussein, E. J., Abed, T. F., & Kandemir, M. T.. Artificial Intelligence and Machine Learning in Healthcare. Springer.

[3] Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. In Philosophical Transactions of the Royal Society A Mathematical Physical and Engineering Sciences (Vol. 376, Issue 2133, p. 20180080). Royal Society. https://doi.org/10.1098/rsta.2018.0080

[4] Khan, F. A., Abid, A., Farooq, M. S., & Uddin, M.. Artificial intelligence and COVID-19: Applications, challenges and future prospects. International Journal of Environmental Science and Technology, 19, 7631-7646.

[5] Pizzi, D., Romanoff, K., & Versace, P.. The digital divide in the age of artificial intelligence. AI & SOCIETY, 35, 663-671.

[6] Coeckelbergh, M. (2020). AI Ethics. In The MIT Press eBooks. The MIT Press. https://doi.org/10.7551/mitpress/12549.001.0001

[7] Muhammad, F., & Bayan, H. (2024). The Ethics of AI: Navigating the Moral Dilemmas of“

[8] Federal Trade Commission (FTC). (2021). Statement Regarding Clearview AI Investigation. Retrieved from: https://www.ftc.gov

[9] Korinek, A., & Stiglitz, J. E.. Artificial intelligence and its implications for income distribution and unemployment. In NBER Chapters (pp. 487-540). National Bureau of Economic Research, Inc.

[10] Yiğitcanlar, T., & Cugurullo, F.. The rise of smart cities: implications for planning practice. European Planning Studies, 28, 212-228.

[11] Ruschemeier, D.. Artificial intelligence in healthcare: a comprehensive overview. Journal of Healthcare Engineering, 2023.

[12] Gao, J., & Wang, D. (2023). Quantifying the Benefit of Artificial Intelligence for Scientific Research. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2304.10578

[13] Borenstein, J., & Howard, A. (2020). Emerging challenges in AI and the need for AI ethics education. In AI and Ethics (Vol. 1, Issue 1, p. 61). Springer Nature. https://doi.org/10.1007/s43681-020-00002-7

[14] Conger, K. (2020). Amazon Pauses Police Use of Its Facial Recognition Software. The New York Times. Retrieved from: https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition.html

[15] Bello, O. A. (2023). Machine learning algorithms for credit risk assessment: an economic and financial analysis. International Journal of Management, 10(1), 109-133.

[16] Goland, J. A. (2022). Algorithmic Disgorgement: Destruction Of Artificial Intelligence Models As The Ftc’s Newest Enforcement Tool For Bad Data. In Richmond Journal of Law & Technology: Vol. XXIX (Issue 2).

[17] Snow, J. (2018). Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots. ACLU. Retrieved from: https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28-members-of-congress-with-mugshots

[18] Odinet, C. K. (2022). FINTECH CREDIT AND THE FINANCIAL RISK OF AI. https://www.cbsnews.com/news/the-united-states-of-indebted-america

[19] Federal Trade Commission (FTC). (2021). Aiming for Truth, Fairness, and Equity in Your Company’s Use of AI. Retrieved from: https://www.ftc.gov

[20] Bellamy, R. K. E., et al. (2018). AI Fairness 360: An Extensible Toolkit for Detecting and Mitigating Bias in Machine Learning Models. Retrieved from: https://arxiv.org/abs/1810.01943

[21] Krishnapriya, K. S., Albiero, V., Vangara, K., King, M. C., & Bowyer, K. W. (2020). Issues Related to Face Recognition Accuracy Varying Based on Race and Skin Tone. IEEE Transactions on Technology and Society, 1(1), 8–20. https://doi.org/10.1109/tts.2020.2974996

[22] Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. Minds and Machines, 30(1), 99–120. https://doi.org/10.1007/s11023-020-09517-8

[23] Chander,A.(2016).TheRacistAlgorithm?http://ssrn.com/abstract=2795203Electroniccopyavailableat:https://ssrn.com/abstract=2795203

[24] European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from: https://gdpr-info.eu

[25] Bibas, S. (2006). ESSAY TRANSPARENCY AND PARTICIPATION IN CRIMINAL PROCEDURE. http://www.albany.edu/sourcebook/pdf/t546.pdf

[26] National Institute of Standards and Technology (NIST). (2023). AI Risk Management Framework. Retrieved from: https://www.nist.gov/itl/ai-risk-management-framework

[27] Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency. Retrieved from: https://dl.acm.org/doi/10.1145/3287560.3287598

[28] Electronic Privacy Information Center (EPIC). (2019). EPIC Files Complaint with FTC to Stop Use of HireVue's AI Hiring System. Retrieved from: https://epic.org/epic-files-complaint-with-ftc-to-stop-use-of-hirevues-ai-hiring-system/

[29] Adebayo, O., Mensah, N., Adukpo, T. K. (2025). Beyond Cash Flow Management: How Machine Learning and Scenario Planning Drive Financial Resilience. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 81-89. https://doi.org/10.36713/epra20503

[30] Umoren, J., Adukpo, T. K., Mensah, N. (2025). Exploring factors, outcomes, and benefits in supply chain finance: Insights and future directions for the U.S. healthcare system. World Journal of Advanced Research and Reviews, 25(2), 60-71. https://doi.org/10.30574/wjarr.2025.25.2.0345

[31] Adebayo, O., Mensah, N., Adukpo, T. K. (2025). Navigating Liquidity Management Challenges in the Era of Digital Banking in the United States. World Journal of Advanced Research and Reviews, 25(2), 2711-2719. https://doi.org/10.30574/wjarr.2025.25.2.0576

[32] Umoren, J., Adukpo, T. K., & Mensah, N. (2025). Leveraging Artificial Intelligence in Healthcare Supply Chains: Strengthening Resilience and Minimizing Waste. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(2), 190-196. https://doi.org/10.36713/epra20385

[33] Adukpo, T. K., & Mensah, N. (2025). Financial technology and its effects on small and medium-scale enterprises in Ghana: An Explanatory Research. Asian Journal of Economics, Business and Accounting, 25(3), 268-284. https://doi.org/10.9734/ajeba/2025/v25i31709

[34] Olise, P., Opoku, L. K., Mensah, N. (2025). The impact of advanced safety leadership training programs on reducing workplace accidents and enhancing asset reliability in U.S. industrial sectors. International Journal of Science and Research Archive, 14(1), 25-33. https://doi.org/10.30574/ijsra.2025.14.1.2594

[35] Amoako, E.K.W., Boateng, V., Ajay, O., Adukpo, T.K., Mensah, N. (2025). Exploring the Role of Machine Learning and Deep Learning in Anti-Money Laundering (AML) Strategies within U.S. Financial Industry: A Systematic Review of Implementation, Effectiveness, and Challenges. Finance & Accounting Research Journal, 7(1). https://doi.org/10.51594/farj.v7i1.1808

[36] Atisu, J. C., Mensah, N., Alipoe, S. A., & Rahman, S. A. (2024). The Effect Of Non-Performing Loans On The Financial Performance Of Commercial Banks In Ghana. IOSR Journal of Economics and Finance, 15(5), 42-48. https://doi.org/10.9790/5933-1505054248

[37] Olise, P., Opoku, L. K., Mensah, N. (2025). Innovative Strategies for Cost Reduction and Risk Mitigation in Event and Public Safety Management (Noting a Case Study of Large-Scale Event). EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(1). https://doi.org/10.36713/epra19964

[38] Atisu, J. C., Mensah, N., Junior, K. N., Akuamoah, O. A. (2024). Board Gender Diversity and Financial Performance of Listed and Unlisted Firms in Ghana. International Journal of Research Publication and Reviews, 5(9), 2788-2796. https://doi.org/10.55248/gengpi.5.0924.2658

[39] Mensah, N., Adukpo, T. K. (2025). Impact of Government Expenditure on Economic Growth of Ghana. Asian Journal of Economics, Business and Accounting, 25(3), 232-247. https://doi.org/10.9734/ajeba/2025/v25i31706

[40] Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). The Role of Business Intelligence in AI Ethics: Empowering U.S. Companies to Achieve Transparent and Responsible AI. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 8-14. https://doi.org/10.36713/epra20314

[41] Mensah, N., Atisu, J. C., Alipoe, S. A., Ofori, D. E. K. (2024). Impact of Corporate Governance Structure on Profitability of Quoted and Unquoted Firms in Ghana. International Journal of Research Publication and Reviews, 5(10), 1026-1033. https://doi.org/10.55248/gengpi.5.1024.2731