Vol.15No.3(2024):442-460
DOI:https://doi.org/10.61841/turcomat.v15i3.14959

Ethical Considerations in Deploying AI Systems in Public Domains: Addressing the ethical challenges of using AI in areas like surveillance and healthcare

Vedant Singh

Abstract
The general use of AI technology, especially in public sectors like security and even in the medical field, has been subject to a number of questions to do with ethics. This paper aims to understand the ethical dilemmas concerning the instantiation of Artificial Intelligence in these fields, specifically privacy, bias, responsibility, and openness concerns. In security, advanced technologies like facial recognition and predictive policing attract concerns pertaining to violation of privacy, importation of race bias, and lack of social control, among others. In health care, the AI systems employed in the diagnosis and treatment of patients call into question issues to do with patient choices, data privacy, and discrimination in medical treatment. Within the scope of the paper, the author considers contemporary ethical standards and legislation regulating AI creation and finds some deficiencies. In response to these issues, some of the potential work for the future highlighted in the paper includes enhancing the legal policies in the area of AI, insisting on the importance of ethical multi-disciplinary research, and creating awareness of the effects of AI in society. It underlines the requirement for responsible and explainable AI, the availability of efficient tools helping in monitoring and controlling AI, and increased people's involvement in creating AI policies to state that the launched AI technologies will be compliant with the people's benefit. With these suggestions, the paper sought to add knowledge to the ongoing discussion on AI ethics and ensure that decent utilization of AI systems is enhanced with reverence to human rights and ethical norms.

Keywords; Ethics, Artificial Intelligence (AI), Privacy, Bias, Accountability, Transparency, Healthcare, Surveillance, Regulations, Fairness.

1. Introduction

In recent years, AI has emerged as a disruptive technology, with its application penetrating deep into different spheres of operation across all public domains. Sectors such as healthcare, education, public safety, and city planning pay prominent benefits from the essence of AI's capability to analyze huge volumes of data, where AI can perform repetitive tasks while making real-time decisions. In this sector, it is changing diagnostics, drug discovery, and coming up with unique treatment regimens. In public safety, artificial intelligence facilitates matters such as policing based on predicting criminal activities, monitoring public facilities, and preventing such incidences. AI is also instrumental in smart city projects, the need for better traffic management, resource use, and public service provision. However, AI applications bring numerous ethical challenges, as the solutions are generally implemented in critical, open areas that directly affect people's rights and freedom.

Since the advent of AI Technologies is accelerating and their usage is growing in almost all sectors, they must be implemented ethically. Due to this social aspect of AI, ethical concerns are more vital when implementing AI systems in areas of public importance. For instance, assignments of prejudice are reduced in the concepts developed for AI algorithms, negations fairness, and equality. Endemic surveillance raises concerns about rights violations regarding privacy, while smart healthcare solutions can be discriminatory. These potential threats of AI are real, not imaginary, and therefore call for initiative-taking regulation, transparency, and accountability to protect individual liberties and social benefit. AI might even deepen divides, reinforce prejudice, and erode trust without an ethical direction that governs its application.

This article will examine the ethical issues that arise when AI systems are deployed in the public space, emphasizing surveillance and health care. Taking the complex relationship between AI technologies and ethics as the basis of the article, the author will outline critical ethical issues, including privacy, prejudiced decisions, responsibility, and disclosure. In addition, it will explore how these are being managed by using the current regulations, ethical principles, and standard implementation of AI applications. Through this exploration, this article will help

governments, developing technology companies, and the public understand how the ethicality of AI can emerge and how its positive aspects can be enjoyed without causing negativity.

Several ethical issues surround AI's application in the public sector. Some of the most significant challenges include privacy, with issues such as surveillance being worrisome as the AI systems may also monitor people's movements and activities. An obvious weakness of AI systems in healthcare is that as systems work with personal medical data, they can inadvertently disclose personal information and violate the patient's privacy. Another problem is that the AI algorithms are biased because if the system is not properly programmed, discrimination will only be reinforced if it is not managed and controlled. However, there are major concerns, such as accountability, since the machine learning-based AI systems are partially or fully opaque, and it becomes complicated to pinpoint who is responsible for the mishap that ensued. Explainability is vital for these new AI systems to be stable and conform to society's standards. Further, there is a pressing need to determine ways and approaches through which AI, as it continues to transform public sectors worldwide, may inflict ethical harm and, therefore, work out mechanisms to avert its negative impact. These raise several questions that this article will explore in hopes of noting the ethical principles required for applying AI in public domains.

2. Understanding AI Systems in Public Domains

AI systems have found their way to almost every public domain because they are efficient in improving existing decision-making systems. Therefore, a massive effort is needed to develop a clear understanding of what AI means, what types there are, and what the use cases are so that adequate ethical measures can be taken.

Table 1: ***AI Systems in Public Domains – Applications in Surveillance and Healthcare***

Application Domain	AI Technology	Description	Use Cases	Benefits	Challenges
Surveillance	**Machine Learning (ML)**	Allows systems to learn from data and make predictions or decisions with minimal human intervention.	Traffic monitoring systems, congestion prediction, dynamic traffic light control.	Efficient traffic management, reduced congestion, optimized routes.	Data accuracy, real-time processing demands, system integration.
	Neural Networks	Mimics the human brain's structure to process complex data, uncovering intricate connections.	Facial recognition, activity detection, crime prevention.	Enhanced security, efficient identification of suspects, anomaly detection.	Privacy concerns, false positives, ethical considerations.
	Natural Language Processing (NLP)	Helps AI systems understand and generate human language.	Chatbots, virtual assistants, automated surveillance report generation.	Better interaction with citizens, improved public service, communication.	Language complexities, accuracy in contextual understanding.
Healthcare	**Machine Learning (ML)**	Analyzes large datasets to make accurate predictions about health outcomes and patient conditions.	Diagnostics (X-ray, MRI), predictive analytics for patient care.	Faster diagnosis, better patient outcomes, cost-effective treatments.	Data privacy, model transparency, ensuring accuracy in diverse populations.
	Neural Networks	Used to recognize patterns in medical imaging for accurate diagnostics.	Detecting diseases in X-rays, MRIs, and other medical imaging.	Enhanced diagnostic accuracy, early disease detection.	High training costs, need for large labeled datasets.
	Natural Language Processing (NLP)	Helps AI interpret and analyze large quantities of medical text data (e.g., electronic health records).	Structured data analysis, clinical decision support systems.	Streamlined data interpretation, improved decision-making.	Data inconsistency, ensuring real-time processing.

2.1. Definition and Types of AI Systems

Artificial Intelligence involves using various technologies to develop smart systems that can handle tasks that a human being can otherwise carry out (Rashid et al., 2023). Such tasks include learning, logical reasoning,

problem-solving, and natural language comprehension. The ML models characteristic of AI systems used in public domains are Machine Learning, Neural Networks, and NLP. Machine Learning (ML) is a subfield of AI that allows the system to be trained on the data to make predictions or decisions with minimal human intervention. In-depth statistical analysis of big data is performed by drawing high-level conclusions about the existing data and using those conclusions when making forecasts or decisions on new inputs (Goodfellow et al., 2016). Such learning is especially important for application areas like policing and traffic control, where a constant learning process of data helps to refine results and performance.

Neural networks are an umbrella term for a group of computational models designed to keep with the structure of the human brain, whereby the set of interconnected nodes or neurons is often referred to as nodes. These networks deserve special attention for their ability to uncover intricate and many-parametric connections between the inputs, which is crucial for such applications as image and speech identification (LeCun, Bengio & Hinton, 2015). In public surveillance, neural networks help identify individuals and activities to improve security. Natural Language Processing (NLP) deals with the computer system's use of natural language. NLP helps AI systems comprehend, analyze, and produce natural language for the likes of chatbots, virtual assistants, and automated translation (Jurafsky & Martin, 2020). In healthcare, NLP helps structure, analyze, and make sense of a huge quantity of text data, which in turn enhances diagnostics and, thus, the quality of care given to the patients.

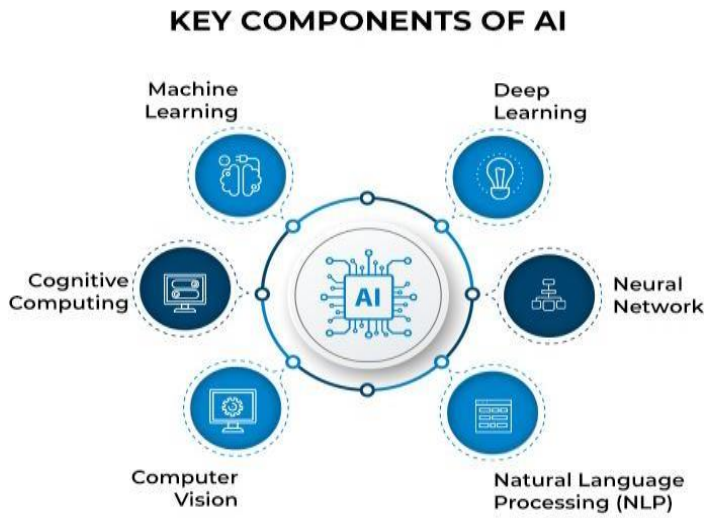

Figure 1: ***Key Components of AI***

2.2. Applications in Surveillance

Advanced Intelligent security systems have significantly improved safety and traffic control by using principles such as real-time data processing. Public safety and security are the areas that have benefited the most from AI-based surveillance technologies. Using facial recognition driven by neural networks helps the police arrest criminals effectively and more efficiently (Smith, 2019). Furthermore, this technology can scan video surveillance feeds for surveillance anomalies or threats, thus making crime preventative (Zhang et al., 2020). Traffic monitoring systems use artificial intelligence to control traffic within cities. Moreover, using Machine learning, the daily traffic congestion patterns can be predicted so that the traffic signals can vary according to the traffic conditions, and the best possible routes can be suggested (Gill, 2018). They also help eliminate traffic congestion, decrease pollution, and generally improve the business of cities.

2.3. Applications in Healthcare

The healthcare industry is at the forefront of using AI systems in diagnostics and personalized medication to enhance patient care services and treatment success (Alowais et al., 2023). AI-based diagnostic tools are more efficient and precise in diagnosing a disease than traditional methods. Computers, especially those with Artificial Intelligence capabilities, diagnose images like X-rays and MRIs more accurately than humans or conventional approaches (Esteva et al., 2017). Healthcare professionals use these tools to make the right decision, leading to the correct treatment at the right time.

Personalized Medicine uses Artificial Intelligence to deliver medical treatments keyed into a patient's genomics, behavior pattern, and other attributes. AI can process big data, search for the optimal treatment for the patient's characteristics, increase the success rate, and decrease negative side effects (Topol, 2019). This approach not only cures the client with improved results but also conserves heath resources. The application of AI systems in public

places, especially in surveillance and healthcare, shows how transformative AI systems are. Nevertheless, AI implementation in these sectors requires thoroughly examining ethical concerns to achieve the intended results while avoiding negative effects on peoples' rights and other social values.

Figure 2: ***Role of Artificial Intelligence in the Healthcare Industry***

3. Ethical Frameworks for AI Deployment

Owing to numerous complications affecting the use of AI systems in the public space, a proper framework that addresses various challenges that come along is crucial, especially in facets such as surveillance and healthcare. These frameworks are crucial to guarantee the proper integration of AI technologies with social norms and regarding each human subject's fundamental rights and constitutional equality. AI ethics, the rules for regulating it, and the application of various ethical theories offer a broad approach to solving these issues.

Table 2: ***Ethical Frameworks for AI Deployment***

Ethical Aspect	Description	Key Example	Benefits	Challenges
Principles of Ethical AI	Basic guiding principles to ensure AI is developed and used ethically.	Transparency, Accountability, Fairness	Builds trust, ensures rights are respected, and reduces bias.	Ensuring practical implementation across diverse sectors.
Regulatory Standards	Regulations and guidelines that govern AI use and deployment to align with ethical norms.	GDPR, IEEE Standards for AI Ethics	Ensures data protection, ethical use of AI, and compliance with human rights.	Varying regulations globally, implementation complexity.
Ethical Theories Applied to AI	Philosophical frameworks to address ethical concerns related to AI.	Utilitarianism, Deontological Ethics	Provides a basis for resolving moral dilemmas and ensuring fairness.	Balancing conflicting values, e.g., security vs. privacy.

3.1. Principles of Ethical AI

The proper use of AI systems falls back on the basic principles that guide their functioning to be ethical. Three of the most important principles, transparency, accountability, and fairness, are essential to the successful application of AI in areas of public concern. The trust in AI systems can only be based on the transparent system. It prepares the concept of artificial intelligence using decision-making that is ethical and clear to everyone. Transparency makes it possible for users and any other affected person to understand how and why something is done. This is especially true in industries that directly affect the individual's privacy and health, like surveillance and healthcare (Hagendorff, 2020). Transparency also includes the availability of information, what sources were used, where models were created, and what types of bias are inherent in the system.

Responsibility in the case of AI specifies the duties that developers or organizations, as well as the government, have in maintaining the right use of AI. The effectiveness of the measures used in AI applications today requires accountability mechanisms for the parties concerned since they are liable for the outcomes that affect individuals' lives. For instance, in healthcare, if an AI system makes a wrong medical diagnosis, leading to harm,

accountability guarantees that the guilty parties shall be made to answer. This principle is related to accountability in AI systems, where the decision-making process is logged and can be audited (O'Neil, 2016).

Nonbiasing and equal treatment of all people are cardinal to the concept of fairness in designing AI systems. The concept of fairness protects against AI systems reinforcing bias in decision-making, especially concerning race, gender, or economic status. For instance, in the healthcare sector, prejudiced information can cause wrong diagnoses and obviously will impact ethnic and racial minorities first (Binns, 2020). There is a need to prove and actively eliminate bias and preconceptions in AI systems across different groups of people to promote an equal approach across the board.

Figure 3: Popular-AI-Ethics-Principles

3.2. Regulatory Standards and Guidelines

The increasing institutionalization of AI systems in societies has thus made policy standards and guidelines important instruments of AI governance. These standards help create guidelines on how AI technologies will work, from legal parameters to ethical-sounding ones. The two predominant regulatory structures that affect the adoption of AI are the GDPR and the IEEE Standards for AI Ethics.

The GDPR, a privacy regulation enacted by the European Union in 2018, is one of the broad regulations on AI deployment. It focuses on the principles of processing personal data, which is essential in areas such as surveillance and health, where most AI systems are known to draw data from. Consumers have rights to data protection based on GDPR to be informed on how their data is being used and control over the data and its processing. This regulation sets detailed conditions under which an AI developer must operate to protect personal data and provide accessible explanations of an AI decision (Voigt & Von dem Bussche, 2017).

The set of recommendations created in the IEEE Standards for AI Ethics formed by the Institute of Electrical and Electronics Engineers helps navigate the ethical usage of artificial intelligence. These standards target elements such as openness, impartiality, and responsibility, and they call for the development of pro-human AI systems that do not demean people. The guidelines also include monitoring and recognizing that AI systems should not operate beyond the acceptable ethical standards as soon as they are implemented (Jobin, Ienca, & Vayena, 2019). These regulatory frameworks are useful in placing institutional frameworks for the enhancement of the development of systems in AI that comply with human rights while promoting technological growth.

3.3. Ethical Theories Applied to AI

There are many ethical theories that offer a philosophical framework for resolving ethical issues related to the use of AI. Two of the remaining theories that address AI ethics are utilitarianism and deontological ethics. Another important ethical theory is utilitarianism, developed by Jeremy Bentham and John Stuart Mill. It is a type of consequentialism that measures the morality of actions by their impact on increasing the general net happiness. When used in the context of AI, it means that AI systems should be developed to benefit the most significant number of people. In practice, this might mean identifying health as a vital aspect of using artificial intelligence, for instance, in security and medicine. An issue not easily resolved is how to quantify and moderate one or multiple objectives whereby the benefit of one often harms the other, which is the agency's primary obstacle. For instance, the benefits that accrue from personal or public security come at the expense of an individual's privacy (Taddeo & Floridi, 2018).

Whereas deontological ethics focuses on the moral worth of the action done without regard to the outcome of the action. This ethical theory was developed by Immanuel Kant, who believed that some duties and rights should

be followed regardless of the consequences. In deontological aspects of AI, the major focus is on rights where the external benefits of AI, such as improved yields, are good, but the rights of the public, such as privacy, should still not be infringed. For example, in the case of AI surveillance, deontologists would be right in saying that people have the right to privacy, and such a right should not be violated by the opportunity to get more efficient security. This approach concurs with the transparency and accountability principles that allow AI systems to respect rights that all humans are entitled to (Gogoll & Puehse, 2020).

Consequentialism and deontology are ethically appropriate theories that can be applied to AI's deployment to avoid possible negative consequences and maximize the positive impact on society while respecting people's rights and being fair to them. In practice, a combined approach based on utilitarianism and a deontological ethical system might provide the most effective tool for solving moral problems concerning AI technologies.

4. Ethical Challenges in AI-based Surveillance

Artificial Intelligence (AI), in particular, has enhanced public safety and security surveillance systems through superior monitoring and analysis options (Alahi et al., 2023). However, this advancement raises numerous ethical questions that need to be solved carefully regarding AI-based solutions.

Table 3: ***Ethical Challenges in AI-based Surveillance***

Ethical Challenge	Description	Example	Impact	Possible Solutions
Privacy Concerns	Continuous data collection and surveillance without informed consent. Privacy rights are often violated.	Facial recognition, biometric data, and license plate tracking	Erosion of personal privacy and potential misuse of data.	Strengthen data protection laws, enhance consent protocols.
Bias and Discrimination	AI systems may reflect and amplify societal biases, leading to unfair treatment of certain groups.	Racial bias in facial recognition technology.	Discriminatory practices, social injustice, and racial profiling.	Diversify training data, incorporate bias detection mechanisms.
Accountability and Transparency	AI systems are often "black boxes," making it difficult to assign accountability when errors occur.	Unclear responsibility for wrong or biased AI decisions.	Decreased trust in AI systems and potential injustices.	Improve AI explainability and establish clear liability frameworks.
Data Security	The large volumes of sensitive data generated by AI systems are vulnerable to cyberattacks and breaches.	Hackers gaining access to surveillance data.	Identity theft, financial loss, and public distrust.	Implement robust encryption, security checks, and access control.

4.1. Privacy Concerns

Privacy uncertainty is one of the most significant ethical challenges in surveillance with the help of an AI technique, mainly because of the constant data gathering and processing. AI surveillance systems capture many personal details such as facial recognition, license plate numbers, cardiovascular health information, credit scores, biometric data, and much more, the flow of which is usually unknown to a given individual. This constant data collection will violate people's rights to privacy as the data collected can be used and accessed inappropriately. These privacy concerns are further compounded by the fact that most organizations do not obtain consent and rarely provide sufficient information about how data is being collected from individuals, putting them at the mercy of perpetual tracking and data mining.

Surveillance here-off takes its toll and further augments privacy complications. One danger of using artificial intelligence is that systems can accurately sort public and private areas, which can result in intrusive surveillance. This can provide a surveillance state-like environment by making people continually feel they are being watched, which is detrimental to personal liberties and agency (Kumar, 2019). There is the problem of the constant presence of AI surveillance and widespread surveillance, which can lead to distrust between the government and the citizens. However, there is a significant overlap between sociopolitical liberty and private life, which imposes high demands on legislation to protect people from surveillance technology abuse.

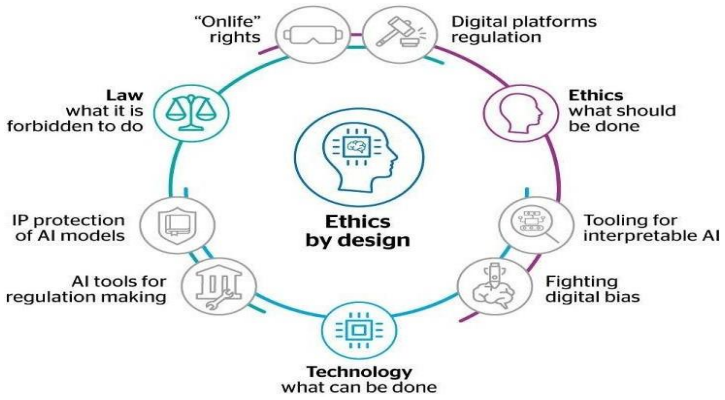

Figure 4: AI ethics by design

4.2. Bias and Discrimination

The objectivity that characterizes most AI applications means that AI-based surveillance systems, too, can discriminate against some population groups. Most of these biases stem from the data used when training the artificial intelligence systems. When the specifics of training data are not sufficiently diverse or contain pre-existing biases, AI systems can enforce and amplify existing societal prejudices (Buolamwini & Gebru, 2018). For instance, biometric technologies, such as facial recognition ones, have been confirmed to produce discrepancies in ethnicity-based results that enact wrongful identification and subsequently result in disparate treatment of persons of color.

With such an emphasis, minorities are the most affected by this sort of policy. Because AI surveillance tools can disproportionately affect these groups, they will be offered uneven treatment and continue the perpetuation of social prejudice (Barocas & Selbst, 2016). Discrimination of this type results in social isolation, increasing the conflict between the police and members of some races and increasing skepticism about artificial intelligence. Overcoming bias in AI surveillance calls for a more robust approach that incorporates diversified data feeds, bias detection analytics, and constant monitoring to ensure that the use of AI in decision-making processes proactively mirrors fairness and equality.

4.3. Accountability and Transparency

Another major ethical issue in AI-used surveillance is accountability and transparency. The AI methods are generally considered "black box" systems due to their complexity, and, often, the non-transparent nature makes it more difficult to determine how decisions are made (Burrell, 2016). Such issues arise because AI systems operate in a closed loop from which you cannot deduce specific individuals or organizations responsible for their actions and decisions. When either a wrong or a biased decision has been made by the AI surveillance systems, deciding on the liability becomes a challenge, thereby increasing the chances of injustices and lowering confidence in the technologies.

Transparency in AI systems is key to preventing surveillance practices from overstepping ethical and legal benchmarks. A lack of understanding of how self-learning algorithms work makes it almost impossible to standardize and monitor them adequately. Improving the explainability of artificial intelligence implies the possibility of rendering intelligible the processes leading to a decision to interested parties, including the general population and control and supervisory authorities (Mittelstadt et al., 2016). Additionally, what could be depicted as the sunset of AI accountability is essential to guarantee checks and balances in case of any ethical violations or AI fatal errors.

Figure 5: ***Ethical Considerations in AI-Based Cybersecurity***

4.4. Data Security

Another important ethical question connected with AI-based surveillance is data security. Such systems generate extensive data, which is stored, and this data is a perfect target for cyber-attacks and data breaches. Sensitive information must be safeguarded to bar intruders from gaining access, those who have access from changing the contents, and those who access it from misusing it (Zuboff, 2019). The failure to provide adequate protection to the data can result in irreversible negative effects such as identity theft, loss of money, and, most importantly, loss of nerve by the public in institutions involved in surveillance.

Additionally, the consequences of stolen data are personal and social, affecting the whole population. By putting the data into the wrong hands, the surveillance systems risk falling into the wrong hands and being used for malicious purposes or reducing the effectiveness of public safety measures (Kesan, 2020). To minimize these risks, the actual protection of data security, like encryption, data storage, and security checks, should be optimized. Similarly, proper access controls or enforcements and surveillance mechanisms will go a long way in protecting critical information and upholding the ethicality of artificial intelligence surveillance systems.

The ethics of using artificial intelligence in surveillance systems can be categorized in terms of privacy, fairness, robotics accountability and transparency, and data protection (Hermansyah et al., 2023). These issues cannot be solved without having sound legal enactments needed for the effective regulation of AI, codes of ethics, and long-term systematic checks and balances to ensure that many advances from artificial intelligence are implemented responsibly and fairly. With the progress of AI in total, it is crucial to address problems of an ethical nature to achieve a proper set of tools that guarantee the usage of security potential and protect the rights of every person and the value of society.

5. Ethical Challenges in AI-based Healthcare

The implementation of AI in the healthcare system has changed the medical world by adding diagnostic tools, individualized treatment, and advanced patient satisfaction. Nevertheless, it presents some new shocking ethical issues that require advanced solutions that can help achieve proper utilization of this technology.

Table 4: ***Ethical Challenges in AI-based Healthcare***

Ethical Challenge	**Description**	**Example**	**Impact**	**Possible Solutions**
Patient Privacy and Data Protection	The need to protect sensitive patient data and prevent unauthorized access.	Use of personal health data for AI training without consent.	Violation of privacy, potential data leaks, and patient distrust.	Strengthen data protection laws (e.g., HIPAA), implement clear consent processes.
Informed Consent	Patients must be fully informed about how AI	Lack of transparency in AI	Reduced patient autonomy, confusion,	Ensure transparency in AI usage, involve

Ethical Challenge	Description	Example	Impact	Possible Solutions
	systems contribute to their care decisions.	diagnostics and treatment plans.	and the inability to make informed choices.	patients in discussions, and allow opt-outs.
Bias in AI Healthcare Tools	AI systems may reflect biases present in training data, affecting the accuracy of healthcare outcomes.	Ethnic biases in diagnostic tools leading to incorrect diagnoses.	Disparities in healthcare outcomes, especially for minorities and marginalized groups.	Diversify training data, implement bias detection and correction mechanisms.
Responsibility and Liability	Determining who is accountable when AI systems make errors in healthcare.	Misdiagnosis by AI leading to incorrect treatment.	Legal complications, confusion over responsibility, and lack of patient recourse.	Establish clear legal frameworks defining responsibility for AI-based decisions.

5.1. Patient Privacy and Data Protection

The first emerging ethical issue key to discussing artificial intelligence in healthcare settings is the issue of patient privacy and the security of medical records. AI systems must use large amounts of data from which to learn, including personal data, particularly when it comes to patients' health. The acquisition, storage, and use of this data are controversies due to violation and possible leakage (Sharon & Elger, 2020). It is crucial to implement strong measures for data protection to meet patients' expectations and the requirements of the legislation, as well as the guidelines of global legislation such as HIPAA in the United States of America (Rieke et al., 2020). However, it is very important to have respondents give their informed consent over data collection and usage. A patient's data must be protected from unauthorized access, and the patient should be very well advised on how exactly the data is going to be used, the people who are going to use the data, and any probable dangers that can be associated with such use. Clear information sharing relating to the data practices assists in fostering trust and control by the patients over their information. Controlling AI in healthcare without appropriate consent mechanisms is a foundation for ethical transgressions and the erosion of the credibility of medical organizations.

Figure 6: Challenges towards building privacy-preserving AI in healthcare.

5.2. Informed Consent

Patient information is an important standard of professional ethicality because it establishes what patients ought to know about the treatments given to them. In the context of AI it translates to meaning that in order to allow patient's self-determination, one needs to be informed about AI's decision as well as his recommendations. AI systems give diagnostic and treatment recommendations that cannot be readily understood by patients or even some clinicians

(Char et al., 2018). This lack of transparency may limit patient's unique ability to make an informed decision about their care.

One of the major vulnerabilities when it comes to patient autonomy is the need to ensure that they understand the elements suggested by an AI system. The model also applies pressure on healthcare providers who need to engage patients in discussions on how Artificial Intelligence supports medical decisions and in what ways information technology can be helpful or unhelpful. Furthermore, the patients must be allowed to either consent to or opt out of receiving AI-supported care delivery strategies. Maintaining legal and proper patient consent in developing an AI-based healthcare system requires the intervention of technology developers, medical practitioners, and patients to enhance respect for patient decisions regarding the use of technology in healthcare (Saria, 2019).

5.3. Bias in AI Healthcare Tools

Using AI in tools that relate to healthcare is not without implications. It brings with it bias that is a cause of concern in dispensing health care and is likely to widen the disparities in the results of the health care delivery process. This means that AI systems learn from data, and datasets may include some biases such as race, gender, and class, among others. A lack of color-blind and sensitive solutions to these biases may result in AI algorithms that create minority- and marginalized-people-biased outcomes (Obermeyer et al., 2019).

Lack of equity in medical outcomes is thereby obtained when the AI solutions ignore variations in the characteristics of different patient populations. For example, an AI diagnosis tool that was trained largely on a sample of one ethnic population may not be accurate when applied to members of other ethnicities because, for a start, it will diagnose them inaccurately and then recommend a treatment that might not be the best (Buolamwini & Gebru, 2018). Equal treatment can only be achieved provided the AI systems are tested in various populations and appropriate measures are made and put into practice whenever the AI systems are being developed and deployed to the market. This involves employing balanced data, integration of fairness measures, and the constant assessment of the performance of the AI to ensure that discriminating features are detected and corrected (Chouldechova & Roth, 2018).

5.4. Responsibility and Liability

Holding someone responsible in cases where an error occurred due to the AI algorithm is nonetheless one more ethical issue in AI-based healthcare systems. It is, therefore, important to know when an AI system gives out wrong recommendations or diagnoses and who bears the blame for the effects caused by an incorrect diagnosis. Due to the shared responsibility question, the differentiation between who is to blame—AI developers, health care professionals, or the institutions using the technology—is challenging in addressing such cases (Gerke et al., 2020).

Consequential issues for HL entail legal repercussions for AI application in health care practice, where providers are required to recognize legal liabilities of AI technology usage while providing care. Given these challenges, healthcare institutions need to draw comprehensive policies that define the function and responsibility for the use of AI in the organization. This includes guaranteeing that AI applications augment tools for practice rather than being stand-ins for clinical experience. Moreover, the limitations of AI accountability include the lack of legal precedents to support frameworks for responsibility, which can protect patients who an AI system's mistakes have injured (Mittelstadt, 2019).

It demonstrates that ethical issues of healthcare with AI are complex and include matters to do with patient privacy, patients' consent, biases, and liability. Realizing these challenges needs a multi-sectorial approach that focuses on the ethical consideration of AI. Therefore, based on the analysis of the risks associated with AI in the healthcare sector, potential measures can be identified to optimize its implementation and minimize the abuse of patient rights. Proper data protection, patients' awareness, informed consent, elimination of prejudice, and definition of responsibility and liability.

6. Balancing Innovation and Ethics

6.1. Benefits of AI in Public Domains

It is important to note that the adoption of AI has intensified across most public sectors and domains, amongst them surveillance and healthcare (Campion et al., 2022). This experience shows that with the help of Big Data, AI systems are able to process the amounts of data and increase efficiency as well as accuracy in these fields. For instance, in surveillance, integrated systems that use artificial intelligence can analyze real-time data from the video to detect any looming security threats, meaning public safety agencies can move faster to address incidents. In the same regard, Calo (2015) also notes that AI eliminates tedious tasks that are time-consuming and would require many workers to carry out their responsibilities effectively. Besides, it also increases throughput and accuracy because it minimizes the chances of an error made by an individual.

The application of AI in healthcare can lead to improved diagnostics, early disease identification, patient risk assessment, and individualized treatment recommendations. For example, machine learning, which is artificial intelligence, can analyze doctor records, as well as images, and come up with patterns that are difficult to recognize by human beings. Thus, one can expect the increase in interventions to happen earlier, and this would provide better outcomes for the patient and fewer expenses for treatment in the future (Rajkomar et al., 2019). In addition, by using AI related to telemedicine, existing or intended communication gaps in healthcare delivery are closed by offering patients in rural areas and other remote places consultation through computerized telecommunication systems. These improvements clearly illustrate how AI can help bring a higher level of quality to public services by making the effects of healthcare better and refining the use of public safety strategies.

6.2. Ethical Decision-Making in AI Deployment

It is argued that AI useful in public settings positively advances societal gain, yet implementing such elements entails ethical reflection (Ashok et al., 2022). One of the major areas of concern is to have AI developed and utilized in a manner that captures societal ideals as much as possible. Ethics have to be considered at the developmental stage of AI to ensure that it is not a threat to society in any way. This entails incorporating values into the design process as well as the implementation of the AI systems. According to Binns (2018), the application of the four principles of accountability, fairness, and transparency within the decision-making of AI must be met by the developers of AI. For instance, the algorithms applied in public safety surveillance have to be created in a way that will not favor one group, for example, Black people, or design ways that infringe on people's rights to privacy.

Another important measure is the creation of boards for ethical reviews to aim at the responsible use of AI technologies. These boards, comprised of ethicists, lawyers, and technologists, can review the possible danger that AI systems could pose before they are released to the general environment. They can also act as a continuous monitoring and auditing mechanism and revisit the AI systems as they mature to continue to make sure that whatever they do is within the stated ethical values that were set during the development process. Independent ethical review committees provide insight into the responsible development and deployment of AI technologies to provide public trust as the development of new interventions strictly follows the ethical guidelines of Jobin et al. (2019).

Furthermore, ethical decision-making is a collective responsibility of the developers, policymakers, and the public in its ability to achieve a common general good through the deployment of Artificial intelligence technologies. As for the citizenship aspect, this collaboration is particularly valuable when thinking about the social and ethical purpose of AI in easily recognizable spheres like healthcare and surveillance.

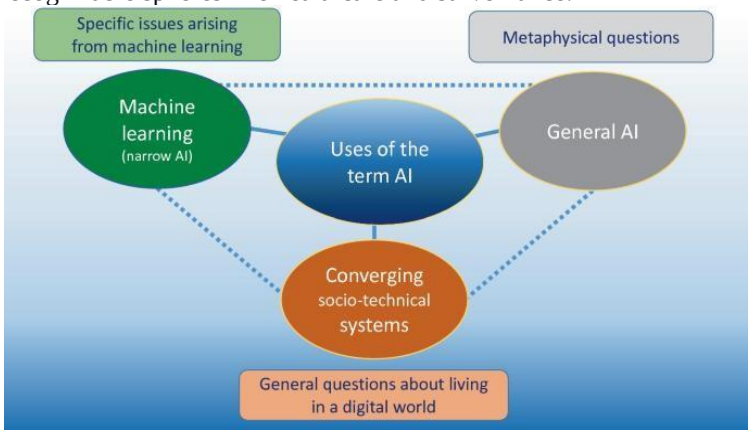

Figure 7: ***Ethical Issues of AI***

6.3. Stakeholder Engagement

Engaging the public in AI policy dialogue is for privacy in this segment and aims to make AI technologies more responsive to societal values. Public participation enables the people to air their opinion hence enabling the formulation of policies. There is no doubt that AI technologies can revolutionize people's lives, and thus, engaging the public in the process of development, deployment, and usage of these technologies is believed to bring certainty and ultima ratio of scientists and researchers when it comes to considerations of possible negative consequences of the AI technologies in the society (Whittlestone et al., 2019). There is nothing wrong with involving the public in the

ethical decision-making process because it applies to areas that society is not comfortable with, such as surveillance or the usage of AI in health.

It is also feasible to rely on common work between technological parties and states since the application of such innovations as AI presupposes obligatory adherence to certain ethical standards and regulations. People's governments give laws on how best to develop these systems and the processes that should be in place to ensure that the systems are made accountable. In contrast, primarily technology companies participate in the development of AI technologies, and those companies have to be held accountable for the consequences that their technologies could have a negative impact on society or violate certain individuals' rights. Two of the most important sectors that should work closely are the government and business since the former is capable of creating suitable policies and frameworks. At the same time, the latter could provide information regarding the opportunities that AI offers, as well as the risks and threats that are present when using the technology in question (Binns, 2018).

In practice, such collaboration can be either organized at the industry level, or may be a result of direct cooperation between hi-tech firms and public authorities. For instance, the recent regulations of artificial intelligence incorporated in the European Union's General Data Protection Regulation (GDPR) permit the use of personal data by artificial intelligence systems under the Protection of the Privacy Act. In the same way and style, social partnerships between technology firms and institutions in charge of public health can foster the exploration of AI interventions to some of the most pertinent public health challenges without compromising on the principles relating to ethical best practices (Mittelstadt, 2019).

Cooperation between the private sector and governments can help establish the right regulatory framework that will promote technological advancement while guaranteeing the proper use of AI. Therefore, engagement and collaboration between the doing and thinking sectors ensured that the benefits, risks, and interdisciplinary concerns that must confront public AI were balanced (Lescrauwaet et al., 2022).

7. Case Studies

7.1. Surveillance: Examples and Ethical Implications

Facial Recognition Technology in Public Spaces

Consequently, FRT has become one of the key elements of public surveillance systems, as recognition of people in real-time by utilizing sophisticated algorithms. This technique has been widely used for many reasons, inclusive of public security, to enhance the flow of border checks. However, the deployment of such platforms brings several ethical questions into question. For example, the violation of privacy is a common issue since people's biometrics data can be gathered without their consent. Zuboff (2019) pointed out that widespread FRT creates hazards to people's basic rights because surveillance targets identified people, which in turn aggravates injustices for individuals of color.

A final ethical issue of particular FRT is its inefficiency in democratic countries and its utilization by authoritarian states. The authors Wachter et al. (2017) pointed out that FRT has been used as an equal to stifle opposition in different parts of the globe, thus limiting freedom of speech. Additionally, errors have been attributed to facial recognition algorithms where the algorithms are not accurate in identifying persons of a specific color or origin. A pioneering piece of research by Buolamwini and Gebru (2018) showed that the models tested act unjustly and produce a considerable number of errors when it comes to recognizing dark-skin-toned faces. Addressing these issues requires more intensive regulation and stronger protection from the outside, as well as open-source algorithm creation to avoid prejudice.

Predictive Policing Systems

Computerized and advanced policing refers specifically to an analytical tool that applies an algorithm to crime reports to predict future risks and, in the process, helps police organizations schedule their resources. Although these systems have shown some possibility of ensuring an environment for crime prevention, there are ethical issues that surround them, including bias and lack of clarity of operations. Nyati (2018) argues that while predictive technologies are useful in fields such as telematics and asset tracking, any utilization of these technologies in public safety must be met with caution because these technologies are essentially utilizing historically biased data sets.

Conservatives remarked that predictive policing systems are a way of reinforcing prejudice. For example, Richardson et al. (2019) noted that such systems end up focusing on low-income areas, thereby continuing the annexation of those areas by the police. Transparency is another important issue. The underlying algorithms of predictive policing are often obscure, which is why it is challenging to measure the fairness of a prediction. Measurements may include investment in the creation of more open source predictive models and third-party auditing of these systems to improve the levels of transparency of these systems.

Figure 8: ***Advantages of Predictive Policing***

7.2. Healthcare: Examples and Ethical Implications

AI Diagnostics in Hospitals

Through artificial intelligence, diagnoses of diseases and other health complications have been enhanced. Computerized platforms like those applied in the analysis of images in radiology have been known to identify ailments like cancer and cardiovascular diseases. Gulshan et al. (2016) showed the effectiveness of AI algorithms in diagnosing DR with similar levels of performance to ophthalmologists, which points as well to the possibility of such technologies.

Nevertheless, there are still ethical implications regarding the easy interpretations of diagnoses made by AI systems. Black-box algorithms, in which the means for coming to certain conclusions are not explained, go against the concept of transparency. According to Floridi et al. (2018), a lack of interpretability reduces the confidence that clinicians can have in AI recommendations to affect patient outcomes. Moreover, there is allaying of data privacy to which AI diagnostics are prone as they often involve the use of patient data. AI, therefore, demands strong data protection standards to protect clientele identities as highlighted, yet affirms their adoption's benefits.

Telemedicine and AI-Driven Patient Care

Telemedicine has become a popular theme with AI assistants and has offered important new opportunities to people to receive needed healthcare services in regions that have a low density of healthcare facilities. Such systems provide agnostic real-time consultations and tailored treatment suggestions, closing gaps in the delivery of healthcare services. Nyati (2018) describes how telematics and AI have demonstrated the possibilities of achieving efficiency improvements. Nevertheless, risks to ethical considerations concerning the enforcement of telemedicine employing the use of artificial intelligence have to be addressed.

Another considerable problem is that patients have restricted equipment in AI telemedicine since some of them don't have internet access or are completely illiterate in the information technologies field. This imbalance has the potential to deepen the already existing disparities in accessing health services. In addition, the problem of informed consent is given. According to Roski et al. (2014), patients may also not be aware of the involvement of AI in their care, and this is a major issue in terms of their ability to make decisions. These concerns call for specific approaches in the form of awareness creation on the use of digital technology and development of polices that would compel the medical institution to be clear on the use of artificial intelligent based patient care.

8. Strategies for Ethical AI Deployment

The use of AI in public sectors like surveillance and the health sector has ethical issues. To reduce these risks and make sure that AI works in a way that will respect human rights, equality, and openness of actions, the ways in which ethical actions for AI applications should be managed must be defined. This section explores three key strategies: This includes enforcing ethical standards, increasing accountability and responsibility, and constant observation and assessment.

Figure 9: ***Ethics of Artificial Intelligence***

8.1. Implementing Ethical Guidelines

The following is one of the most basic approaches for implementing AI righteously: the creation of sound AI policies that lay down the ethical principles governing the use of AI. These comprise the principles through which AI development is guided at early stages and through its progression and use. Potential harms can be mitigated since ethical considerations bear concerns about privacy, bias, and discrimination (Crawford, 2021). Such policies force developers to undertake risk assessment activities that take into account both the short-run and extended impacts within the society.

Introduction to the ethical use of AI is another strong component in the process of preventing AI from being utilized irresponsibly (Méndez-Suárez et al., 2023). While AI technologies are rapidly advancing and are embedded across various sectors of society, it is useful to key stakeholders – developers, policymakers, and end-users have a coherent understanding of some of the ethical considerations that accompany them. Organizational ethical training can offer the needed learning on issues to do with fairness, accountability, and protection of individuals' privacy. Therefore, the first approach is to promote ethical awareness within the organization so that the employees can learn to make the right decision when it comes to designing, deploying, and managing AI systems (Jobin et al., 2019). Moreover, ethical training should always be reinforced due to emerging new technologies in the forms of artificial intelligence and new ethical issues related to them.

8.2. Enhancing Transparency and Accountability

This goes hand in hand with the need for AI to be transparent in order that people can place their confidence in it. In order to enhance the AI system, it is also required that all of the processes that run behind the screen should be transparent enough to the stakeholders that engage the AI system. AI systems that governing bodies can open to outside auditors or inspectors provide more transparency in how the AI algorithms conduct their calculations and reach decisions (Binns, 2018). They are important in areas such as health and policing, where algorithms are frequently used to determine people's fates. Openness can also extend some of those benefits to developers, researchers, and the general public and thus result in more ethical development of AI.

There must also be clearly defined accountability mechanisms to address the situation when wrongdoers, reckless individuals, or organizations are using the AI systems that is build. The responsibility for decisions that are made by AI systems and processes has to be assumed by someone, especially in such fields as medicine, where AI can play an important role in making important decisions. Company structures to respond to why a certain piece of AI makes unfair, discriminating, or damaging decisions are also clear. This can include forcing developers, operators, or third parties to answer problems resulting from the deployment of AI tools (Zeng et al., 2020). Furthermore, when accountability mechanisms are not very clear, there are no mechanisms through which affected people can complain, as this may reduce the public's confidence in the use of AI.

8.3. Continuous Monitoring and Evaluation

Ongoing checking is an important aspect of the implementation of AI systems that should not in any way be done away with. This ongoing evaluation guarantees that AI technologies are always consistent with the set ethical values and that the tools will keep functioning as planned even after implementation. Among them, the frequency of AI audits is a critical element of the process, which makes it possible for organizations to check such problems and

correct them as necessary: algorithmic bias, security of data, and degradation of the system (Lepri et al., 2018). The purpose of auditing AI systems is to establish an independent assessment of organizational activities with regard to ethical guidelines and legal requirements. In addition, regular analyses make it possible for organizations to incorporate various changes in the system to counter new ethical issues or newfound problems.

Another important element of constant monitoring is the feedback that allows for improvement. These mechanisms should be embedded in AI systems to enable the interaction of AI with the users and other stakeholders in real time. It can assist in solving problems not envisaged at the time of its creation, for example, bias in decision-making processes or secondary effects, respectively. Furthermore, feedback control guarantees that the AI systems are responding to dynamics of social, legal, and ethical perspectives and are malleable to changes in these dynamics (Satariano, 2020). For instance, using feedback from patient experiences using AI-assisted diagnostics in healthcare facilities, algorithms guiding diagnostics can be adjusted to enhance efficacy concerning diagnosis and fairness in diagnostics. The integration of constant monitoring with strong feedback facilitates the ability of AI to retain ethical responsiveness throughout the usage cycle. It also enables stakeholders with a channel through which the developers and organizations involved in creating AI can be forced to meet certain ethical standards (Morley et al., 2020).

9. Future Directions and Recommendations

The ethical use of AI in the public sphere is still an evolutionary issue since AI inventions are rapidly increasing while ethical awareness and legal frameworks are struggling to keep up.

9.1. Emerging Ethical Issues in AI

AI and Autonomous Decision-Making

AI and software, such that they perform operations independently, present numerous questions of morality when it concerns sensitive fields such as health and security (Ahmad et al., 2022). These systems are frequently expected to make binary choices that directly impact people, for example, on where the emergency response effort should be allocated or what disease a patient has. Some unanswered issues relate to who is held responsible for the failure, and this becomes a problem when the underlying processes of many sophisticated AI systems involve black boxes, thus concealing its rationale (Bryson, 2019). This opaqueness undermines the efforts made by developers and regulators in check in order to arrive at decisions reflective of societal, ethical standards.

Long-term Societal Impacts

Introducing AI into the public space affects structures within society in a significant way. Some of the works pointed out that an overreliance on AI models imprints a gradual degradation of knowledge and rationality in human beings (Zuboff, 2019). Moreover, surveillance AI possibilities challenge the idea of democratic liberties and may change the population's behavior at large. It concerns the long-term effects of technologically mediated interventions in communities that still suffer social injustice, systemic equality, and systemic oppression; solving these concerns demands preventative measures that foresee the future repercussions of those populations affected by AI policies (Eubanks, 2018).

Figure 10: ***Ethical Implications of AI in Decision Making***

9.2. Policy Recommendations

Strengthening Regulatory Frameworks

In order to effectively manage ethical risks, highly comprehensive mechanisms must exist in the form of regulations. Modern frameworks like GDPR provide good starting points but inadequately meet AI-related challenges, especially in non-profit spheres like public healthcare and security (Floridi et al., 2018). It means that instead of relying

on vague recommendations for 'responsibility,' policymakers need to create clear regulatory guidelines based on AI risk factors that should include concrete expectations about explainability, transparency, and fairness. Another aspect of regulatory oversight which should be established are processes for periodic review and assessment of the AI systems for conformity to the resulting set of ethical principles.

Promoting Ethical AI Research

Supporting such papers enhances the discovery of proper ethics of artificial intelligence design and uptake. It is therefore encouraging to find horizon scanning activities like the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems are pointing to how ethical thinking can be integrated into the creating of AI solutions (IEEE, 2019). Furthermore, ethicists, technologists, and policymakers need to work together to guarantee the feasibility of ethicists' ideas and also to introduce new approaches to the development of ethical technology in practice. Financing organizations and universities need to invest in Studies on using or implementing bias in AI and the negative externalities of AI usage (Binns, 2018).

9.3. Encouraging Public Awareness and Education

Informing Citizens about AI Impacts

In today's world it is crucial to improve public awareness about what AI is capable of and what it is not capable of, to bring about better trust as well as accountability. The lack of confidence in AI is because previous research reveals that people are either completely trusting or distrustful of AI, and these prejudices cause AI negative effects in public domains (Jobin et al., 2019). Education, awareness, and free publicity of artificial intelligence technologies, as well as making training material available, can assist in eradicating misconceptions and stimulate informal debate about the morality of AI.

Building Trust in AI Systems

The Core working principle to the building of public trust is the provision of proof that AI systems are being designed and implemented equally, fairly and with accountability. Transparency should also be considered key to the development of AI systems, and it should mean that all the parties, developers, and regulators explain as closely as possible how the AI systems are functioning and why they have made the particular decision (Cath, 2018). Moreover, involving the public, especially in the policymaking for the development of AI systematic policies that target the citizens as their clients, will go a long way in achieving the visioned objectives.

10. Conclusion

AI systems make it possible to apply their ethical use in public areas, including surveillance and healthcare, with opportunities as well as challenges. In each of these sectors discussed in this article, the use of AI technologies presents the benefit of improving public safety, the quality of healthcare, and the efficiency of business and administrative functions. However, if the ethical perspectives in the development of these systems are not well observed, then the very systems meant to enhance the welfare of society could be used negatively to harm society or even to perpetuate inequalities. Among the main ethical considerations discussed is that of privacy with special emphasis on applications in architectures of surveillance. These technologies, including facial recognition, mass surveillance, and predictive policing, threaten individual rights by propelling society into a surveillance society. Likewise, in healthcare, there are privacy and data protection issues concerning patients, which include problems with consent and concerns arising from the impacts of bias in AI-driven medical diagnoses that mostly affect people of color. These issues demand robust ethical standards that embrace the principles of openness, nonbias, and responsibility in the deliberation and implementation of artificial intelligence systems that will respect the rights of the users of these systems and advance the well-being of society as a whole.

Another challenge to the ethical implementation of AI is the fact that the black boxes of most AI solutions continue to create many problems to overcome. Part of the danger is the problematic transparency of some algorithms in the decision-making process, where such AI applications raise questions regarding liability in case of mistakes or injustice. This is especially the case in the two industries of health and security, where choices made by AI may have dramatic effects. To minimize these risks, AI transparency needs to be increased, and pathways for explaining and vindicating AI actions have to be developed for citizens and other interested parties.

A multi-faceted approach is needed to address the ethical issues of AI. This means that policymakers should set up regulations that would be effective in fighting against the risks that AI brings into society but also allow for development in that field. This entails the enhancement of current laws like the GDPR alongside the extension of new guidelines meant particularly for the use of intelligent algorithms. Despite the increased regulation, if the field does not get a boost in funding to promote ethical AI research, the AI systems will be developed, and their ethical considerations will be an afterthought at best. Ali and his colleagues stressed that all stakeholders, from researchers

and developers to technologists, need ethicists, legal scholars, and policymakers to integrate fairness, transparency, and accountability into AI development. Just as important is informing the public and conducting formative education campaigns to ensure persons are knowledgeable about the disease. With the increase in the use of AI technologies in society, it becomes important for anyone to embrace both the advantages and the disadvantages of the use of these systems. Community involvement can be achieved via consultations, workshops, and awareness creation to ensure that members understand what AI is and the impact it has on society so that they decide on the appropriate use of these technologies. It is suggested that the future confidence in the AI outcomes will be based on the open and inclusive approach to the development of these systems.

Despite the great potential for the enhancement of public services, the practice of AI involves major ethical issues that need to be settled in order to avoid misuse of technologies. People need to follow ethical information and research studies to address the need to uphold ethical practices in the dissemination of AI technology for common good purposes. It is up to society and multiple disciplines to fashion AI solutions for public locales to incorporate the values of the latter with the protection of human rights and dignity. It is through such steps that experts can get towards the dream of having society augmented by artificial intelligence and smart technologies without having to compromise on essential ethical and moral values.

References;

1. Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, 100452.
2. Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. *Sensors*, *23*(11), 5206.
3. Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., ... & Albekairy, A. M. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC medical education*, *23*(1), 689.
4. Ashok, M., Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for Artificial Intelligence and Digital technologies. *International Journal of Information Management*, *62*, 102433.
5. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, *104*(3), 671-732.
6. Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency*, 149–159.
7. Binns, R. (2018). *On the importance of ethical design and development of AI systems.* Ethics and Information Technology, 20(1), 15-29.
8. Binns, R. (2020). *Fairness in Machine Learning: Lessons from Political Philosophy*. ACM Computing Surveys, 53(4), 1-29.
9. Bryson, J. J. (2019). The past decade and future of AI's impact on society. *Handbook of Artificial Intelligence Ethics.*
10. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1-15.
11. Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 2053951715622512.
12. Calo, R. (2015). *The boundaries of privacy harm.* Indiana Law Journal, 91(3), 713-776.
13. Campion, A., Gasco-Hernandez, M., Jankin Mikhaylov, S., & Esteve, M. (2022). Overcoming the challenges of collaboratively adopting artificial intelligence in the public sector. *Social Science Computer Review*, *40*(2), 462-477.
14. Cath, C. (2018). Governing artificial intelligence: Ethical, legal, and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,* 376(2133), 20180080.
15. Char, D. S., Shah, N. H., & Magnus, D. (2018). *Implementing Machine Learning in Health Care—Addressing Ethical Challenges*. New England Journal of Medicine, 378(11), 981-983.
16. Chouldechova, A., & Roth, A. (2018). *The Frontiers of Fairness in Machine Learning*. arXiv preprint arXiv:1810.08810.

17. Crawford, K. (2021). *Atlas of AI: Mapping the Ways Artificial Intelligence is Changing Our World*. Yale University Press.
18. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, 542(7639), 115-118.
19. Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press.
20. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689-707.
21. Gerke, S., Minssen, T., & Cohen, G. (2020). *Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare*. Artificial Intelligence in Healthcare, 295-336.
22. Gill, A. (2018). Developing a real-time electronic funds transfer system for credit unions. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 9(1), 162-184. Retrieved from https://iaeme.com/Home/issue/IJARET?Volume=9&Issue=1
23. Gogoll, J., & Puehse, U. (2020). *Deontological Approaches to AI Ethics: Ethical Considerations for AI in Surveillance*. AI & Ethics, 1(1), 47-63.
24. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
25. Gulshan, V., Peng, L., Coram, M., Stumpe, M. C., Wu, D., Narayanaswamy, A., ... & Webster, D. R. (2016). Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. *JAMA, 316*(22), 2402-2410.
26. Hagendorff, T. (2020). *The Ethics of AI Ethics: An Evaluation of the Ethical Guidelines for Artificial Intelligence*. Springer.
27. Hermansyah, M., Najib, A., Farida, A., Sacipto, R., & Rintyarna, B. S. (2023). Artificial intelligence and ethics: Building an artificial intelligence system that ensures privacy and social justice. *International Journal of Science and Society*, *5*(1), 154-168.
28. IEEE. (2019). *Ethically aligned design: A vision for prioritizing human wellbeing with autonomous and intelligent systems.* IEEE.
29. Jobin, A., Ienca, M., & Vayena, E. (2019). *The Global Landscape of AI Ethics Guidelines*. Nature Machine Intelligence, 1(9), 389-399.
30. Jurafsky, D., & Martin, J. H. (2020). *Speech and Language Processing* (3rd ed.). Prentice Hall.
31. Kesan, J. P. (2020). AI surveillance and data protection: Privacy implications of intelligent systems. *Journal of Cyber Policy, 5*(3), 321-340.
32. Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. *International Journal of Computational Engineering and Management, 6*(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf
33. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
34. Lepri, B., Oliver, N., Letouzé, E., & Pentland, A. (2018). *Fair, transparent, and accountable algorithmic decision-making systems*. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14.
35. Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging tech-nologies: Navigating the intersection for responsible innovation. *Law and Economics*, *16*(3), 202-220.
36. Méndez-Suárez, M., de Obesso, M. D. L. M., Márquez, O. C., & Palacios, C. M. (2023). Why do companies employ prohibited unethical artificial intelligence practices?. *IEEE Transactions on Engineering Management*.
37. Mittelstadt, B. D. (2019). *Principles alone cannot guarantee ethical AI*. Nature Machine Intelligence, 1(11), 501-507.
38. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 2053951716679679.
39. Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). *The ethics of AI in health care: A mapping review*. *Social Science & Medicine, 258*, 113172.

40. Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. *International Journal of Science and Research (IJSR), 7*(2), 1659-1666. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203183637
41. Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. *International Journal of Science and Research, 7*(10), 1804-1810. https://www.ijsr.net/getabstract.php?paperid=SR24203184230
42. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). *Dissecting Racial Bias in an Algorithm used to Manage the Health of Populations*. Science, 366(6464), 447-453.
43. O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.
44. Rajkomar, A., Dean, J., & Kohane, I. (2019). *Machine learning in medicine.* New England Journal of Medicine, 380(14), 1347-1358.
45. Rashid, A. B., Kausik, A. K., Al Hassan Sunny, A., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. *International Journal of Intelligent Systems*, *2023*(1), 8676366.
46. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYU Law Review*, *94*(15), 192-221.
47. Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H., Albarqouni, S., ... & Chen, L. (2020). *The Future of Digital Health with AI*. npj Digital Medicine, 3(1), 1-4.
48. Roski, J., Bo-Linn, G. W., & Andrews, T. A. (2014). Creating value in health care through big data: Opportunities and policy implications. *Health Affairs*, *33*(7), 1115-1122. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics*, *2*(6), eaan6080.
49. Saria, S. (2019). *Explainable AI for Transparent and Responsible Healthcare*. Clinical Pharmacology & Therapeutics, 105(6), 1047-1049.
50. Satariano, A. (2020). *The importance of continuous AI monitoring and improvement*. *Tech Journal*, *27*(2), 45–47.
51. Sharon, T., & Elger, B. S. (2020). *Privacy and AI in Healthcare: A Delicate Balance*. Journal of Medical Ethics, 46(12), 817-823.
52. Smith, A. (2019). The ethics of AI in surveillance: Privacy, bias, and accountability. *Journal of Information Ethics*, 28(2), 45-60.
53. Taddeo, M., & Floridi, L. (2018). *The Ethics of Artificial Intelligence*. In K. S. Shrader (Ed.), The Cambridge Handbook of Information and Computer Ethics (pp. 215-233). Cambridge University Press.
54. Topol, E. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books.
55. Vayena, E., Blasimme, A., & Cohen, I. G. (2018). *Machine Learning in Medicine: Addressing Ethical Challenges*. PLOS Medicine, 15(11), e1002689.
56. Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.
57. Whittlestone, J., Nyrup, R., Alexandrova, A., Dihal, K., & Cave, S. (2019). *The role and limits of ethics in AI policy.* Philosophy & Technology, 32(4), 537-563.
58. Zeng, Z., Lu, X., & He, H. (2020). *Accountability in artificial intelligence systems: A comprehensive review*. *Journal of AI Research*, *69*, 345–363.
59. Zhang, Y., Milin, P., Li, X., & An, J. (2020). AI in public safety: Applications and challenges. *IEEE Transactions on Systems, Man, and Cybernetics*, 50(4), 1345-1356.
60. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.