IJARIIT
INTERNATIONAL JOURNAL OF
ADVANCE RESEARCH, IDEAS AND
INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1209)
Available online at: https://www.ijariit.com

Legislation of Artificial Intelligence

Samaira Gheek
samairagheek@gmail.com
The British School, New Delhi, Delhi

ABSTRACT

Alan Turing, "the founder of computer science", introduced artificial intelligence in his paper - "Computing Machinery and Intelligence" - in 1950. Artificial intelligence (AI), is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. This piece explores the emerging technologies of artificial intelligence and the regulations and legislation to control its impact in a beneficial way. AI was an evolved solution to support processes and aid humans in their daily lives. While it has many benefits to society such as better medical technology, it also has many ethical downsides. UNESCO, the EU, the UK, and the FDA have come up with specific proposals for regulating the use of AI to maximize the benefits and minimize its drawbacks - the question remains, is it enough? What other solutions can be employed and is the legislation of AI technology truly necessary or will it restrict innovation? This paper discusses the effect of AI on society and if regulations made by national and international authorities will become significant for its rapidly growing future.

Keywords: *UNESCO, EU, UK, Ethics, Application, Unemployment, Automation, Capitalism, Digital Divide, Market Manipulation, Algorithmic Bias, Discrimination, Human Rights, Human Autonomy, Transparency, Privacy, Security, Dilemmas, Policies, Guidelines*

I. INTRODUCTION

"It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable." - John Mcarthy

In simpler terms, it is a mechanism which uses both computer and data science to empower problem solving. After about 7 decades of research, innovation and development, AI has stretched its arms in a variety of fields including e-commerce, education, navigation, security, robotics, healthcare, agriculture, gaming, automobiles, social media, marketing and finance. 'Every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions, and concepts, solve kinds of problems now reserved for humans, and improve themselves.' - John Mccarthy

It is created to aid and simplify human lives. Some of these applications include reduced commuting time (autonomous vehicles), cybersecurity (better email spam filters), decreased power consumption (less devices required, one does the job) and less sexual violence (female bots can be used instead of actual women). Advancements like chatGPT and AlphaGo create ethical and economic issues like unemployment, inequality, racist robots and security which necessitate legal regulations and restrictions. AI is in its final stage, wherein the intelligence of a computer is a close equivalent of a human. Every innovative idea has to operate within a disciplinary structural framework to prevent and safeguard against the dangers it poses.
Not only does the technology itself have its advantages, society is effectively using AI to try and mitigate global issues. An example of this would be the work done by AI for good which is an organization which uses AI systems specifically for societal benefit.

Ethical Benefits
Artificial Intelligence has many applications, some of which have shown to have significantly positive impact on society. To ensure that these benefits are maximised, controls need to be put in place for this fast growing technology.

In the economic environment of modern society, businesses find it difficult to reduce waste and increase efficiency. AI is the solution for that. Its capacity for working at an exponentially higher rate than the human workforce, reduces the time for completing iterative jobs done by labour. AI controlled bots and machinery provide efficiency and productivity. In addition, simple jobs can be delegated to AI systems which would allow employees to do more satisfying tasks. This would allow for self actualization(the top most level in Maslow's hierarchy of needs).As stated by EU's High-Level Expert group: 'AI is not the end in itself, but rather a promising means to increase human flourishing, thereby enhancing individual and societal well-being and the common good, as well as bringing progress and innovation' Additionally, it will be advantageous for dangerous jobs viz the replacement of soldiers with robots avoiding collateral deaths of many innocent soldiers. Thereby decreasing the death rate during international and domestic conflicts. Other industries such as mining, deep sea oil rig and similar high-risk ventures. In the medical sector AI innovations could aid home-diagnostic treatments, AI operated surgeries and much more. These would in turn substantially decrease the injuries, diseases in communities as AI would enable speedy processes through time efficiency. During, the pandemic doctor visits were limited, this can be addressed in the future by using AI operated systems and softwares at home. These can diagnose a disease and even recommend medical advice. Since AI operated systems are fed algorithms, their accuracy is likely to be higher than a human doctor although the trust of patients might be difficult to attract. While the benefits are many, some might raise ethical concerns.

Ethical Concerns

Unemployment due to automation:

Unemployment is the average decrease in the percentage of the working population. Due to AI's ability to perform simplistic jobs done by labour and employees, these jobs will eventually be made redundant, leaving a large percentage of labour jobless.Especially since AI can work much faster and accurately than the average human. This raises the ethical question of whether AI is helpful or harmful in this humanitarian aspect. Its technical accuracy can reduce the workload of accountants and lawyers reducing them to mere legal orators. This is a double edge sword.

This unemployment situation differs from the recession induced one.
Norbert Wiener, an American mathematician, explain that:
"it is perfectly clear thatches will produce an unemployment situation, in comparison with which the present recession and even the depression of the thirties will seem a pleasant joke"

What separates unemployment due to AI systems from general IT technology is that the jobs replaced are high-paying jobs. Some researchers suggest that to protect people from unemployment one must consider reskilling.
But people may argue that unemployment due to AI is a major ethical concern besides the economic impact, such as capitalism: "is efficiency not the whole idea of capitalism, and the digital revolution its ultimate bust? The function of the new technologies is, in the logic of capitalism, to save labour costs."

Asymmetric distribution of wealth and the digital divide:

Unemployment is not the only economic effect of AI systems. There will be a major shift in the monopoly of organizations and individuals. Individuals who can afford AI automated systems will have more power and wealth while the AI systems can only be affordable to the wealthy, this may lead to larger gaps between the low and high income paid persons. Organizations with access to AI will excel while others will fail. These organizations are likely to attract more investors since they trust the value of AI. An example of this is Apple, which has recently been valued at 2 trillion dollars. Another divide will be transhumanism: Transhumanists believe that humans may be able to upload their consciousness into a computer or AI robot in order to achieve immortality by discarding their biological bodies. This technology is arguably going to be extremely expensive and only be afforded by wealthy persons. This could create higher levels of digital divide in our societies. Digital divide can be a consequence of nationality, age, gender however a large factor would be socio-economic and income levels. This could lead to more societal segregation and discrimination.

Others

Other economic impacts of the incorporation of AI involve:

Market manipulation - is defined as actions and/or trades by market participants that attempt to influence market pricing artificially, where a necessary criterion is an intention to deceive . Yet, such deceptions have been shown to emerge from a seemingly compliant implementation of an AA that is designed to trade on behalf of a user (that is, an artificial trading agent).'.

AI based cyber crimes - In addition, AI systems can be programmed to perform crimes such as order-book spoofing - an AA can learn the technique of order-book spoofing. This involves placing orders with no intention of ever executing them and merely to manipulate honest participants in the marketplace .

Pump and Dump Scheme - A scheme has recently gained popularity - the pump and dump scheme. It is the acquiring a position in a financial instrument, like a stock, then artificially inflating the stock through fraudulent promotion before selling its position to unsuspecting parties at the inflated price, which often crashes after the sale. - more than 36,000% when its penny stocks surged from less than $0.10 to above $20 a share in a matter of few weeks.

Bias and Discrimination across societal spectrums:

Discrimination is already a severe concern in modern society. To start with, less women are to be employed in the development of the AI due to the stereotypical beliefs of their weaknesses in the fields of STEM. Stanford University's Institute for Human-Centred Artificial Intelligence (HAI) shows that women accounted for less than 19 percent, on average, of all AI and computer science PhD graduates in North America over the past ten years and that, in 2019, 45 percent of new US resident AI PhD graduates were white, compared with 2.4 percent African American and 3.2 percent Hispanic. Not only do women face these discriminatory experiences, people of colour and different nationalities suffer too. Algorithms are fed data by programmers who have their own biases and prejudices. Ai presents social, historical, and political conditions in which that data was created. This is called algorithmic bias - where the programming takes on the prejudices of its creators, albeit unintentionally. In 2015, this was exemplified by Google Photos using advanced recognition software's which inaccurately identified two Black people as Gorillas. This is extremely offensive. Machines can result in the reproduction of existing biases which may lead to discrimination and is a violation of fundamental human rights.

This can impact the hiring process, if AI systems are programmed with in fed bias.
These prejudices in the algorithms will have grave impact on the merits and rationality of appointment.

There are graver concerns of these biases in predictive policing: the application of analytical techniques—particularly quantitative techniques—to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions. This can lead to unjust decisions made by the judicial authorities due to social/ racial contextual bias. Another example is in p2p(peer to peer) lending, done directly between two entities. The method may employ AI to understand if the entity is secure to make transactions. During surveillance, data is not the problem, it is the algorithm and programmer that might lead to discrimination. It may give results based on inaccurate correlations, leading to poor financial decisions of individuals and organizations. Another concern in the judicial system prevails: who should be held liable for AI operated crimes? The programmer, user, the bot itself? This argument could undermine existing liability models, thereby threatening the dissuasive and redressing power of the law.

Lastly, the implications of female sexbots. While many argue that it could help paedophiles and rapists relive their frustrations and wishes on bots, it raises concern of the dehumanisation of women after being portrayed by a robot. Another concern is the dehumanisation and the violence against the robot itself, should it be considered inanimate or do sexual crimes against them have consequences for the offender?

Democracy

What impact does it have in the political field? Arguments made by algorithm-based risk assessments may be considered arbitrary. An important factor to consider for this debate is the personal data of citizens collected by the government and analysed using AI systems. Another research explains 'The myriad personal details available to the state—whether it be health records or travel history—create a mosaic which, when assembled by AI, can chill associational, expressive, and other types of freedoms that are at the core of democracy.'
Due to shifts in authorities, other concerns include how the wealthy will control voting, how they will govern the nations and 'AI creating, directly or via job loss, the conditions that amplify people's disinterest in democratic processes.'

Violation of Human Rights:

AI operated systems can be used to manipulate human behaviour. This is evident in the Social Credit system in China. It gives citizens a three digit score that reflects how good a citizen they are . First of all, this is a major invasion of privacy, to be tracked and then analysed to see how ethically good a citizen is has way too many controversies and assumptions. People with high score get advantages like the following: [they] can travel freely, rent apartments and bikes with no deposit, get better positioning in online dating sites, jump queues in hospitals, receive discounted energy bills, get better foreign exchange rates, access special waiting rooms in train stations and VIP check-in at airports, get access to loans and better interest rates, have higher internet speeds, and more . \

On the other hand, people with low scores are unable to get plane and train tickets, insurance, travel visas, hotel and restaurant reservations, access to certain jobs, or admission to private schools for themselves or their children. They can also be put on a public black list that serves as a naming and shaming device in which people who are within 500 metres can see their location on a 'deadbeat map' on their smartphones. These consequences therefore determine their behaviour and enforce 'right' political views. The unethical standard is representative in the lack of liberty to speak, think or do as one wishes. It is also divisive.

In India, a biometric system is used to allow citizens access to their rights such as getting a passport or government subsidies. This puts citizens with conditions such as leprosy, handicaps etc at a disadvantage. By denying them access without their biometric data, the government is violating their rights.

Health and Loss of Human autonomy:

Due to reduction in human contact via substitution of bots, interaction time between humans is to decrease. It is likely to make people lazier and eventually become less efficient as most of the work will be done by the bots and humans will become increasingly dependent on it for the most minor chores.
It would have the same effect that calculators have had on the capabilities of persons to do mental math's. Since one will be more dependent on AI operated systems for tasks, they are eventually going to find it harder to survive without these machines. Common drawbacks of technology including weaker eyes and addiction to devices is likely to heighten with the incorporation of AI systems. The consequential adverse health impact cannot be ignored. Comfort comes with a price: lack of freedom and individual autonomy.

A possible and feared future scenario is the dominance of AGI (general artificial intelligence) over the human population. This is something to be kept in mind when developing AI systems. If bots are to rule the human population, it could lead to lack of liberty and individual choice. This could also be a risk to fundamental human rights. Any AI malfunction could have fatal consequences for humans.

Privacy and Lack of Transparency

To train AI systems to behave like humans, the machines need to be fed large amounts of data sets. This is a risk to the privacy of users as the authorities will gain access to their personal information. This can be done without consent as well. Additionally, AI works on the basis of patterns to make predictions, this can initiate further insights to private information of users. The constant tracking and surveillance are a privacy invasion and safety concern.

A study in Finland showed that even though there was a non-disclosure agreement, with surveillance in their houses, people felt unsafe and died to hide nudity, use of illegal substances, alcohol use arguments and more, they felt so uncomfortable, they even tried to block cameras. IoT in conversational devices like Siri, record data and send it back to companies, users complain they feel like it is “creepy” or that they feel like “they are being spied on”, they feel less comfortable. Online poker and gambling sites use built-in facial recognition to understand their next moves which is unethical and a violation of freedom, dignity, anonymity and privacy.

Returning to AI’s application in p2p lending, AI is used to analyse behaviour through social media and SNS(social networking service) - companies can give specific information to the end user, and can be used for mitigating credit risks however gathering data is a violation.

What's more is that while a lot of this data is collected based on uninformed consent.
Schneier states that:

“... every morning when you put your cell phone in your pocket, you’re making an implicit
bargain with the carrier: ‘I want to make and receive mobile calls; in exchange, I allow this
company to know where I am at all times.’ The bargain isn’t specified in any contract, but
it’s inherent in how the service works.”

This raises the concern of surveillance capitalism: the creeping damage of the use of AI in surveillance and algorithm-based decision making

Some researchers also believe that Opacity in AI decision-making is sometimes intentional and done in an effort to protect intellectual property and corporate secrets. However, such opacity can also be the result of technical illiteracy or the complexity of processes like deep learning models. AI can motivate organisations to employ unethical activities with easy access to technologies that support it.

Security

In the field of cybersecurity, AI is to have obvious implications including model poisoning attacks and automated phishing. The ability to harass someone both directly and indirectly now becomes easier. Direct harassment is constituted by spreading hateful messages against the person. Indirect methods include retweeting or liking negative tweets and skewing polls to give a false impression of wide-scale animosity against a person. These activities are likely to increase with the ability of automation. In addition, research showed that verbal abuse and sexual conversations were found to be common elements of anonymous interaction with conversational agents.

It is a two phase process. It begins with using AI to gather personal data and proceeds to using stolen personal data and other AI methods to forge an identity that convinces the banking authorities to make a transaction (that is, involving banking theft and fraud).

The last security threat is caused by the incorporation of AI in warfare. The use of autonomous weapons can lead to more damage and collateral deaths. Kallenborn’s article makes the case that the use of drones during warfare comes with the suggestion that such military weapons at times find it difficult to distinguish the difference between combatants and civilians.

Dilemmas

It is difficult to assess the reliability of these systems. Traditional tests cannot be done on them. Common dilemmas among researchers include the following:
Should they have the rights of humans, of companion animals or non-human persons?
Do they deserve dignity and respect?
Whether regulators need to determine whether the action was intended by the agent to have manipulative effects, or whether the programmer intended the agent to take such actions for such purposes?
Do they get rights?
Machines are to be given more responsibility with delegation however the autonomy of individual machines make it harder to build trust. Researchers suggest: Algorithmic opacity, unfair bias, outcomes leading to discrimination, lack of explicability of algorithms, data quality, etc. are some of the most important problems public policymakers and technologists still need to solve in order to make sure that AI implementation in the public sector is ethical and benefits us all.

II. PROPOSED SOLUTIONS

UNESCO’s Recommendation

The UNESCO Recommendation on the ethics of AI was adopted on the basis of a comprehensive framework involving fundamental human rights, sustainability, fairness and inclusivity for all groups. The UNESCO recommendation discusses three major fields: skills and education; employment and inclusion. On the basis of this, it aims to allow for better policy making.

Skills, ethical awareness and education

As AI advances, people are going to have to consider the appropriate skills to control the technology. The recommendation however states that the labour market should allow for better innovation, well-being and growth and not hinder the advancements in the AI field. They explain that all types of skills will become necessary in the future including cognitive, non-cognitive and digital skills. To start with, employees working in the development of AI are going to require skills like: problem-solving ,creativity, team-work related skills. This is important in order to perform tasks involving: machine learning, data mining, cluster analysis, natural language processing, robotics. This information is given in order to aid policies in regards to training and education in the future. A research paper about the UNESCO recommendation explained that UNESCO did this to:

“promote the acquisition of “prerequisite skills” for AI education, such as basic literacy, numeracy, coding and digital skills, and media and information literacy, as well as critical and creative thinking, teamwork, communication, socio-emotional and AI ethics skills, especially in countries and in regions or areas within countries where there are notable gaps in the education of these skills.”

In addition, even if one is not working in the field of AI,
“Public awareness and understanding of AI technologies and the value of data should be promoted through open and accessible education, civic engagement, digital skills and AI ethics training, media and information literacy and training led jointly by governments, intergovernmental organisations, civil society, academia, the media, community leaders and the private sector, and considering the existing linguistic, social and cultural diversity, to ensure effective public participation so that all members of society can take informed decisions about their use of AI systems and be protected from
undue influence.”

Employment

As mentioned above, the recommendation suggests a shift in the training of future workers. To ensure job security, it states that upskilling, reskilling and training will become essential otherwise the jobs are likely to become redundant resulting in dismissals of a large faction of the population. They also recommend,

“putting in place upskilling and reskilling programmes, finding effective mechanisms of retaining employees during those transition periods, and exploring ‘safety net’ programmes for those who cannot be retrained”

This is done on the basis of a research by Frey and Osborne predicting that 47% of workers might lose their jobs to automation.

The recommendation asks for:
“develop[ment] and implement[ation of] programmes to research and address the challenges identified that could include upskilling and reskilling, enhanced social protection, proactive industry policies and interventions, tax benefits, new taxation forms, among others. Member States should ensure that there is sufficient public funding to support these programmes. Relevant regulations, such as tax regimes, should be carefully examined and changed if needed to counteract the consequences of unemployment caused by AI-based automation.”

This ensures that research is being done to safeguard people from unemployment especially in geographical areas where the work is more labour-intensive while also making sure that people are being retrained in order to aid job employment in the fields of developing AI technology.

Inclusivity

UNESCO pays large attention to the ways in which they can ensure gender equality, fairness and inclusion of all groups while AI makes advancements because as discussed earlier, AI can lead to major bias and discrimination.

The recommendation expects the following:

“Member States should have dedicated funds from their public budgets linked to financing gender-responsive schemes, ensure that national digital policies include a gender action plan, and develop relevant policies, for example, on labour education, targeted at supporting girls and women to make sure they are not left out of the digital economy powered by AI. Special investment in providing targeted programmes and gender-specific language, to increase the opportunities of girls’ and women’s participation in science, technology, engineering, and mathematics (STEM), including

information and communication technologies (ICT) disciplines, preparedness, employability, equal career development and professional growth of girls and women, should be considered and implemented”
They think this is essential and should be controlled via effective policies.

The research paper explained that UNESCO recommends this, “regardless of race, colour, descent, gender, age, language, religion, political opinion, national origin, ethnic origin, social origin, economic or social condition of birth, or disability and any other grounds, in terms of access to and participation in the AI system life cycle”

This recommendation is made hoping for better regulations and policies for the AI world. The recommendation provides a framework for all stakeholders to help secure the lives of citizens in all aspects including social, technological, economical, environmental, political, legal and ethical. It is based on strong statistics and prioritises fundamental human rights. A drawback is that there is no mention of the transhuman impacts or privacy concerns which are major ethical issues in AI development.

EU's Draft AI Act

The EU's draft AI act is a proposal for policies with regards to artificial intelligence that may be enforced on all countries in the EU. It is based on the TFEU(Treaty of the Functioning of the European Union). It's main focus too is on human rights. While it is too abstract and does not specifically target AI, it creates an ecosystem of trust by seeking to ensure protection of safety, fundamental rights and EU values.

This proposal defines AI as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environment they interact" . Creating a singular definition of AI for all nations in the EU can allow for similar policies to be drawn resulting in efficient use of AI as AI machines and systems can be used internationally and contradicting policies can act as a barrier in innovation.

The draft AI act follows a risk based approach thereby classifying AI systems and then putting prohibitions on their development and use. The categories include the following:
Unacceptable risk
High risk
Limited risk
Minimal risk

The drawbacks of this strategy include the fact that certain systems like biometric surveillance fall into all three categories which creates ambiguity for all stakeholders involved in the creation and application of the system. In addition, systems falling under the limited risk and minimal risk categories have close to no restrictions and prohibitions which is a security and safety hazard. For example, emotion recognition systems are considered as limited risk, besides transparency, there are no prohibitions on their use. There is no scientific validity to prove their accuracy, they cannot be considered less risky. The idea of categorisation, in fact, has its own flaws; this is because certain systems will always find loopholes to avoid the prohibitions thereby still remaining a point of risk. The high risk list of systems include just: "biometric identification and categorization of natural persons," "management and operation of critical infrastructure," "education and vocational training," "employment, workers management and access to self-employment," "access to an enjoyment of essential private services and public services and benefits," "law enforcement," "migration, asylum and border control management," and "administration of justice and democratic processes" and still, they are willing to add if the systems "pose a risk of harm to the health and safety or a risk of adverse impact on fundamental rights" . While their open-mindedness is appreciated, the ambiguity of the list of systems is problematic.

To focus on the prohibitions put in the case of unacceptable and high risk, one can study the application of remote biometric surveillance systems. The prohibitions are only put on biometric surveillance systems if they are used for "identification" thereby ignoring systems such as "biometric categorisation, emotion recognition and behavioural detection". Furthermore, there are regulations only on biometric systems used in "real-time" hence ignoring the adverse effects of those used for "non-real" or "post" identification systems which are likely to be just as risky. This allows for a wide range of unethical biometric surveillance activities to still continue thereby not mitigating the actual issue of data integrity and privacy. In addition, the criteria that it is only prohibited in the use in "publicly accessible areas" allows for their use in law enforcement activities including 'activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including safeguarding against and prevention of threats to public security' thus still remaining a point of security concern. With these weak and lenient regulations and prohibitions, the act also entails a massive list of exceptions including:

-'targeted search for specific potential victims of crime;
- prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
-detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence for a wide list of criminal offences allowing issue of a European arrest warrant if those offences are punishable in that Member State by a custodial sentence or a detention order for a maximum of at least three years.'(Article 5 (1) (d)).

Additionally, they may allow these remote biometric surveillance systems for private practices to continue via analysis of the situation and the impact on the society. These decisions must be made by a judicial authority in advance but they may allow for approval during or after if the situation is urgent. Can we give this authority to the member state? and are these regulations enough to prevent the disastrous consequences predicted for the future?

On the other hand, in the case of high risk AI systems, they call the providers in the spotlight. They must perform certain tests to ensure sufficient transparency between the AI technology and the users.

The research paper stated that:
"They must implement a risk management system, use high-quality data sets, draw up technical documentation, enable record keeping, ensure transparency and provide information to users, ensure human oversight and an appropriate level of robustness, accuracy and cybersecurity. After performing a conformity assessment, the provider should register this high-risk AI system in an

EU database managed by the European Commission to increase public transparency and oversight and strengthen ex post supervision by competent authorities. The requirements applicable to design and development of certain AI systems before they are placed on the market will be further operationalized through harmonised technical standards, raising significant concerns as to how they would reflect democratic values and respect fundamental rights Although the draft AI Act sets an obligation to introduce risk management systems, it does not specify what kind of risks should be assessed."

Firstly, there are no regulations or assessments to be performed by the user which is unreliable. Secondly, the responsibility of "mitigation measures" is given entirely to the providers and no other stakeholders considering that they know best. This creates a question of extraterritoriality - third parties will be forced to cooperate. It also creates a "regulator sandbox" , "This would entail a controlled environment to facilitate development, testing, and validation of innovative AI systems prior to placing them on the market or putting them into service"

On the other hand, their strict regulations for transparency sound promising. The EU plans to create a database which involves "set[ting] up and maintain[ing] an EU database containing information on high-risk AI systems. Information in the database would be accessible to the public, and personal data therein would be limited to what is necessary for the purposes of the database, including names and contact details of individuals responsible for registering the system" . What's more is that they have set up appropriate administrative fines which will potentially be based on the revenue of the organisation thereby making them "effective, proportionate, and dissuasive". Their policies on data are also favourable."Special categories of data (sensitive data), as defined in data protection legislation, may be processed by providers, to the extent strictly necessary for bias monitoring, detection, and correction.

However, in that case, safeguards must be used to protect the rights to privacy and data protection and other fundamental rights, such as encryption of data and other technical limitations on re-use and security measures." This may mitigate the damage caused by predictive tools which carry "an inherent risk of perpetuating or even enhancing discrimination, reflecting embedded historic racial and ethnic bias in the data sets used, such as a disproportionate focus on policing certain minorities"

Lastly, it is essential to discuss the social impacts and inclusivity concerns in the case of the implementation of EU's proposal act. The act has prohibited any AI system which uses "subliminal techniques" which may "exploit vulnerabilities of a given group of persons" such as the social scoring system in China. While by having a human rights-based approach, one can assume that they ensure gender equality (there is no mention of any regulations which may lead to sexist bias and discrimination as well), there is no mention of feminist terms such as "feminist AI systems". This implies that "The EU needs to deepen on an openly feminist approach and policy framework for AI. This would call for increasing the number of explicit references to gender related issues or prioritise gender design issues in EU funding projects.". A research paper discusses exactly this but also says that 'the strategies proposed by European and Spanish institutions are in line with both gender in technology and gender of technology.'

While this was a good effort to try and mitigate AI related issues of the future, the prohibitions are too lenient and problems can easily still seek through. In addition their categorization of systems creates a major drawback as it only allows for providers to find loopholes and continue unethical practices. While they have discussed a "human rights approach, "Machine-learning approaches", "logic and knowledge-based approaches" and "statistical approaches" they must consider adding market and technological developments.

III. FDA'S PROPOSAL

The FDA department drew up a proposal to explain possible regulations for medical AI systems and technology in the United States. It is divided into two parts - the discussion paper and a request for feedback.

The FDA classifies AI medical systems in two parts - locked(completely developed) and not locked(undergoing development). For not locked algorithms there is a further risk assessment previously applied for the IMDRF(International Medical Device Regulators Forum) which tests the application of the AI technology on the basis of significance to healthcare decision, healthcare situation or condition.

The FDA recognizes that the AI systems are automated and adaptive hence requires a TPLC(total product life cycle) approach to allow for modifications and innovation in the field while continuing to ensure health and safety. On the basis of medical purpose(treatment, diagnosis, cure, mitigation or prevention of diseases), and a risk-based assessment, the FDA will use their previous SaMD(Software as a Medical Device) model to determine whether the initial marketing of the software requires a 510(k) premarket notification, a De Novo application, or a premarket approval application (PMA).

However, allowing modifications itself is a risk hazard especially in the medical field. It can cause problems between:
Clinical and analytical performance;
Inputs used by the algorithm and their clinical association to the SaMD product's output; and
Intended use, which is defined in terms of the importance of the information provided by the SaMD and its relation to the healthcare condition or situation.

Overall, the FDA uses its previous policies and combines them in hope for providing appropriate regulations for the AI operated future. The request for feedback is an appropriate methodology to further perfect the proposal before implementation. However, the FDA needs to analyse the details of the applications of AI in the future to understand that old policies will simply not suffice and that new policies need to be made. Their efforts towards good machine learning practices, pre-specifications and algorithm change protocol, transparency and performance monitoring is recognised.

UK's Proposal

The DCMS(Department for digital, culture, media and sport) released UK's plans for the AI world in 2021. It defines AI as machines that perform tasks normally requiring human intelligence, especially when the machines learn from data how to do those tasks . It is a 10 year capital intensive strategy focussing on addressing significant global challenges. They have described three core pillars on the basis of which they have formed three main goals. Their core pillars are the following:

Investing in the long-term needs of the AI ecosystem,
Ensuring AI benefits all sectors and regions,
Governing AI effectively
On the basis of which the DCMS has come up with three goals:
To experience significant growth in the number and type of AI systems discovered in the UK,
To benefit from the highest amount of economic and productivity growth due to AI,
To establish the most trusted and pro-innovation system for AI governance in the world.

These allow for further development of short term and long term strategies for all stakeholders including providers, users, owners and the government. For health and social safety, they are organising a NHS AI lab(National Health Service Artificial Intelligence lab) which assesses and tests the dangers and benefits of AI technologies. This allows for innovation while ensuring security and safety for all. However a lot of the major issues have been left out. The English organisations may find it difficult to decide on R&D, digital technologies, data security and privacy, infrastructure, and ethics thereby perhaps leading to unethical practices and applications of AI operated systems.

Recommendations

Here is a study of possible recommendations to be made to mitigate concerns regarding the ethical applications of AI. While the proposals by different organisations look promising, there is scope for improvement.

To eliminate privacy concerns in p2p lending, an FL model can be used. A research explained:
"FL was practised by Google for next-word prediction on mobile devices.Google's FL system serves as an example of a secure distributed learning environment for B2C (business to consumer) applications where all parties share the same data features and collaboratively train an ML model. Besides the B2C paradigm, the FL framework has been extended to support "cross-silos" scenarios and B2B (business-to-business) applications by the AI researchers in WeBank,a where each party has different sets of data features. In a nutshell, a fundamental change in algorithmic design with FL is, instead of transferring raw data from sites to sites or to a server, we transfer ML model parameters in a secure way so that parties cannot access the content of others' data."
This can be used in almost all financial applications of AI and even edge computing.

In terms of transparency, one of the biggest issues, significant policies need to come into place. Transparency needs to be there in all parts of the product life-cycle of an AI system including: before the computational processing, during the processing (to examine how the purpose specifications are processed) and after the decision is made (to see whether the system has performed as expected). This will help build trust between the user and the provider and governments. Pasquale recommended Qualified transparency which he describes as "corporations like Reddit can retain their culture of openness by disclosing their algorithms to third-party experts who can hold them in a safe escrow permitting them to public scrutiny but not allowing the algorithm to be public

To prevent unemployment, job-splitting or government job guarantees need to be incorporated. Job splitting is when one job is divided into two or more people so more people can be employed although it leads to a reduction of income per employee. It will ensure jobs during the process of training and reskilling to protect citizens from poverty and other significant financial issues.

Another focus is on the management of large private corporations to take action. This includes funding social simulation testing - "testing environments to weed out risks - as a common good, and as a replacement for (or in addition to) proprietary safety measures" Another action that corporations can take is the Lier theory. He calls "to address traceability by leaving tell-tale clues in the components that make up AIC instruments.". A paper explained that:

"Adopting this moral-agent and moral-patient distinction, Lier proposes a process to monitor and address crimes and effects that traverse systems, for example, Creating a profile on Twitter (the moral agent) could have relevance to Facebook (the moral patient) concerning identity theft (information-selection). By notifying Facebook of the newly created profile details (utterance), Facebook could determine whether it constitutes identity theft by asking the relevant user (understanding), and notifying Twitter to take appropriate action (feedback)."
Other recommendations include extreme actions like banning high-risk systems completely "to address matters of control, security, and accountability" which is obviously a major barrier for innovation. In fact one of the researchers also suggested that "one of our best hopes to defend against automated hacking is also via AI"

After understanding the possible ethical issues, one can understand that what is most important is to simply provide better education. "to invest in longitudinal studies and multivariate analysis spanning educational, geographical, and cultural backgrounds of victims, and perpetrators or even benevolent AI developers"

IV. CONCLUSION

The advantages of AI are undeniable, especially its global impact on economy, society and citizens. As a process it is a great tool but checks must ensure it does not become a weapon.

In the business world, AI can lead to more satisfied employees, greater prosperity and wealth which ensures better well-being of all stakeholders which is necessary for human growth and flourishment. The profitable consequence would be a more efficient and equitable global society.

There are many factors to consider: social, technological, economic, environmental, political, legal and ethical. All of which must be given importance when weighing the advantages and disadvantages of further integration of AI in our communities and societies. The growth of AI is inevitable but how we use it can change its course from negative to positive. Legalities play a huge role in this control and must take necessary and appropriate measures to ensure that AI operated machines are suitable for global ethical application.

V. REFERENCES

[1]. Belk, Russell. “Ethical Issues in Service Robotics and Artificial Intelligence.” Service Industries Journal, vol. 41, no. 13/14, Sept. 2021, pp. 860–76. EBSCOhost, https://doi.org/10.1080/02642069.2020.1727892.

[2]. Anshari, Muhammad, et al. “Financial Technology with AI-Enabled and Ethical Challenges.” Society, vol. 58, no. 3, June 2021, pp. 189–95. EBSCOhost, https://doi.org/10.1007/s12115-021-00592-w.

[3]. Sparkes, Matthew. “AI Regulation.” New Scientist, vol. 252, no. 3356, Oct. 2021, p. 20. EBSCOhost, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=153083308&site=ehost-live.

[4]. Ramos, Gabriela. “A.I.’s Impact on Jobs, Skills, and the Future of Work: The UNESCO Perspective on Key Policy Issues and the Ethical Debate.” New England Journal of Public Policy, vol. 34, no. 1, Spring/Summer2022 2022, pp. 1–13. EBSCOhost, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=158623848&site=ehost-live.

[5]. Kaminski, Margot E., and Jennifer M. Urban. “The Right to Contest Ai.” Columbia Law Review, vol. 121, no. 7, Nov. 2021, pp. 1957–2021. EBSCOhost,https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=153885824&site=ehost-live.

[6]. Yong Cheng, et al. “Federated Learning for Privacy-Preserving AI: Engineering and Algorithmic Framework to Ensure Data Privacy and User Confidentiality.” Communications of the ACM, vol. 63, no. 12, Dec. 2020, pp. 33–36. EBSCOhost, https://doi.org/10.1145/3387107.

[7]. Guevara-Gómez, Ariana, et al. “Feminist Perspectives to Artificial Intelligence: Comparing the Policy Frames of the European Union and Spain.” Information Polity: The International Journal of Government & Democracy in the Information Age, vol. 26, no. 2, Apr. 2021, pp. 173–92. EBSCOhost, https://doi.org/10.3233/IP-200299.

[8]. Barkane, Irena, et al. “Questioning the EU Proposal for an Artificial Intelligence Act: The Need for Prohibitions and a Stricter Approach to Biometric Surveillance.” Information Polity: The International Journal of Government & Democracy in the Information Age, vol. 27, no. 2, Apr. 2022, pp. 147–62. EBSCOhost, https://doi.org/10.3233/IP-211524.

[9]. King, Thomas C., et al. “Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions.” Science & Engineering Ethics, vol. 26, no. 1, Feb. 2020, pp. 89–120. EBSCOhost, https://doi.org/10.1007/s11948-018-00081-0.

[10]. Voss, W.Gregory. “Ai Act: The European Union’s Proposed Framework Regulation for Artificial Intelligence Governance.” *Journal of Internet Law*, vol. 25, no. 4, Nov. 2021, pp. 1–17. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=154146855&site=ehost-live.

[11]. Ting-Ting Gu, et al. “Can Artificial Intelligence Boost Employment in Service Industries? Empirical Analysis Based on China.” *Applied Artificial Intelligence*, vol. 36, no. 1, Dec. 2022, pp. 1–18. *EBSCOhost*, https://doi.org/10.1080/08839514.2022.2080336.

[12]. Eunyoung Han. “The Application of Delphi–AHP Method in the Priority of Policies for Expanding the Use of Artificial Intelligence.” *Journal of Korean Society for Internet Information*, vol. 22, no. 4, Aug. 2021, pp. 99–110. *EBSCOhost*, https://doi.org/10.7472//jksii.2021.22.4.99.

[13]. Radavoi, Ciprian N. “The Impact of Artificial Intelligence on Freedom, Rationality, Rule of Law and Democracy: Should We Not Be Debating It?” *Texas Journal on Civil Liberties & Civil Rights*, vol. 25, no. 2, Spring 2020, pp. 107–29. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=144704064&site=ehost-live.

[14]. Murillo, Antonio Merchán. “International Legal Aspects of Artificial Intelligence.” *Journal of Internet Law*, vol. 26, no. 4, Nov. 2022, pp. 1–15. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=160569109&site=ehost-live.

[15]. Stix, Charlotte. “Actionable Principles for Artificial Intelligence Policy: Three Pathways.” *Science & Engineering Ethics*, vol. 27, no. 1, Jan. 2021, pp. 1–17. *EBSCOhost*, https://doi.org/10.1007/s11948-020-00277-3.

[16]. O, Sullivan, Andrea. “Don’t Let Regulators Ruin AI.” *MIT Technology Review*, vol. 120, no. 6, Nov. 2017, p. 73. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=125667869&site=ehost-live.

[17]. Walsh, Toby. “Turing’s Red Flag.” *Communications of the ACM*, vol. 59, no. 7, July 2016, pp. 34–37. *EBSCOhost*, https://doi.org/10.1145/2838729.

[18]. Piachaud-Moustakis, Bianca. “An Overview of the UK’s National AI Strategy.” *Pharmaceutical Technology Europe*, vol. 34, no. 3, Mar. 2022, pp. 7–8. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=155990432&site=ehost-live.

[19]. Humble, Kristian P., and Dilara Altun. "Artificial Intelligence and the Threat to Human Rights." *Journal of Internet Law*, vol. 24, no. 3, Oct. 2020, pp. 1–18. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=147041532&site=ehost-live.

[20]. Sampson, D.Kyle, et al. "FDA Proposes Regulatory Framework for Artificial Intelligence/Machine Learning Software as a Medical Device." *Intellectual Property & Technology Law Journal*, vol. 31, no. 7, July 2019, pp. 12–16. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=137351115&site=ehost-live.

[1]LGBT History Month 2021 - Alan Turing - Father of Computer Science." 10 Feb. 2021, https://www.liverpool.ac.uk/electrical-engineering-electronics-and-computer-science/blog/blogposts/lgbt/. Accessed 16 Mar. 2023.

[21]. COMPUTING MACHINERY AND INTELLIGENCE. https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf. Accessed 16 Mar. 2023.

[22]. [1] "Artificial Intelligence (AI) Software Market: The Growing Trend 2029." 14 Mar. 2023, https://www.marketwatch.com/press-release/artificial-intelligence-ai-software-market-the-growing-trend-2029-2023-03-13. Accessed 16 Mar. 2023.

[23]. B. C. Stahl, Artificial Intelligence for a Better Future,

[24]. SpringerBriefs in Research and Innovation Governance,

[25]. https://doi.org/10.1007/978-3-030-69978-9_4

[26]. Accessed 16 Mar. 2023.

[27]. [1] Wiener N (1954) The human use of human beings. Doubleday, New York

[28]. [1]Radavoi, Ciprian N. "The Impact of Artificial Intelligence on Freedom, Rationality, Rule of Law and Democracy: Should We Not Be Debating It?" *Texas Journal on Civil Liberties & Civil Rights*, vol. 25, no. 2, Spring 2020, pp. 107–29. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=144704064&site=ehost-live.

[29]. [1] Belk, Russell. "Ethical Issues in Service Robotics and Artificial Intelligence." *Service Industries Journal*, vol. 41, no. 13/14, Sept. 2021, pp. 860–76. *EBSCOhost*, https://doi.org/10.1080/02642069.2020.1727892.

[30]. [1]Spatt, C. (2014). Security market manipulation. Annual Review of Financial Economics, 6(1), 405–418.

[31]. https://doi.org/10.1146/annurev-fnancial-110613-034232.

[32]. [1] Wellman, M. P., & Rajan, U. (2017). Ethical issues for autonomous trading agents. Minds and Machines,27(4), 609–624.

[33]. Lin, T. C. W. (2017). The new market manipulation. Emory Law Journal, 66, 1253.
[1] King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.

[34]. Ramos, Gabriela. "A.I.'s Impact on Jobs, Skills, and the Future of Work: The UNESCO Perspective on Key Policy Issues and the Ethical Debate." *New England Journal of Public Policy*, vol. 34, no. 1, Spring/Summer2022 2022, pp. 1–13. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=158623848&site=ehost-live.

[35]. https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=144704064&site=ehost-live.

[36]. https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=144704064&site=ehost-live.

[37]. King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.

[38]. https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=144704064&site=ehost-live.

[39]. https://doi.org/10.1080/02642069.2020.1727892.

[40]. Belk, Russell. "Ethical Issues in Service Robotics and Artificial Intelligence." *Service Industries Journal*, vol. 41, no. 13/14, Sept. 2021, pp. 860–76. *EBSCOhost*, https://doi.org/10.1080/02642069.2020.1727892.

[41]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the

[42]. Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free

[43]. Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),

[44]. 2016 O.J. (LI 19) art. 22(1) (establishing an individual's right to an explanation as to automated

[45]. decision-making).

[46]. King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.

[47]. Humble, Kristian P., and Dilara Altun. "Artificial Intelligence and the Threat to Human Rights." *Journal of Internet Law*, vol. 24, no. 3, Oct. 2020, pp. 1–18. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=147041532&site=ehost-live.

[48]. [1] Wellman, M. P., & Rajan, U. (2017). Ethical issues for autonomous trading agents. Minds and Machines,

[49]. 27(4), 609–624.

[50]. [1] (Mittelstadt et al., 2016)

[51]. [1] Ramos, Gabriela. "A.I.'s Impact on Jobs, Skills, and the Future of Work: The UNESCO Perspective on Key Policy Issues and the Ethical Debate." *New England Journal of Public Policy*, vol. 34, no. 1, Spring/Summer2022 2022, pp. 1–13. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=158623848&site=ehost-live.

[52]. https://www.loc.gov/item/global-legal-monitor/2021-05-26/european-union-commission-publishes-proposal-to-regulate-artificial-intelligence/#:~:text=The%20AI%20Act%20defines%20an,recommendations%2C%20or%20decisions%20influencing%20the

[53]. Barkane, Irena, et al. "Questioning the EU Proposal for an Artificial Intelligence Act: The Need for Prohibitions and a Stricter Approach to Biometric Surveillance." *Information Polity: The International Journal of Government & Democracy in the Information Age*, vol. 27, no. 2, Apr. 2022, pp. 147–62. *EBSCOhost*, https://doi.org/10.3233/IP-211524.

[54]. Guevara-Gómez, Ariana, et al. "Feminist Perspectives to Artificial Intelligence: Comparing the Policy Frames of the European Union and Spain." *Information Polity: The International Journal of Government & Democracy in the Information Age*, vol. 26, no. 2, Apr. 2021, pp. 173–92. *EBSCOhost*, https://doi.org/10.3233/IP-200299.

[55]. Sampson, D.Kyle, et al. "FDA Proposes Regulatory Framework for Artificial Intelligence/Machine Learning Software as a Medical Device." *Intellectual Property & Technology Law Journal*, vol. 31, no. 7, July 2019, pp. 12–16. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=137351115&site=ehost-live.

[56]. Sampson, D.Kyle, et al. "FDA Proposes Regulatory Framework for Artificial Intelligence/Machine Learning Software as a Medical Device." *Intellectual Property & Technology Law Journal*, vol. 31, no. 7, July 2019, pp. 12–16. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=137351115&site=ehost-live.

[57]. https://www.fda.gov/medical-devices/premarket-submissions-selecting-and-preparing-correct-submission/premarket-notification-510k

[58]. Sampson, D.Kyle, et al. "FDA Proposes Regulatory Framework for Artificial Intelligence/Machine Learning Software as a Medical Device." *Intellectual Property & Technology Law Journal*, vol. 31, no. 7, July 2019, pp. 12–16. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=137351115&site=ehost-live.

[59]. Piachaud-Moustakis, Bianca. "An Overview of the UK's National AI Strategy." *Pharmaceutical Technology Europe*, vol. 34, no. 3, Mar. 2022, pp. 7–8. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=155990432&site=ehost-live.

[60]. Piachaud-Moustakis, Bianca. "An Overview of the UK's National AI Strategy." *Pharmaceutical Technology Europe*, vol. 34, no. 3, Mar. 2022, pp. 7–8. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=155990432&site=ehost-live.

[61]. Piachaud-Moustakis, Bianca. "An Overview of the UK's National AI Strategy." *Pharmaceutical Technology Europe*, vol. 34, no. 3, Mar. 2022, pp. 7–8. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=155990432&site=ehost-live.

[62]. Piachaud-Moustakis, Bianca. "An Overview of the UK's National AI Strategy." *Pharmaceutical Technology Europe*, vol. 34, no. 3, Mar. 2022, pp. 7–8. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=155990432&site=ehost-live.

[63]. Yong Cheng, et al. "Federated Learning for Privacy-Preserving AI: Engineering and Algorithmic Framework to Ensure Data Privacy and User Confidentiality." *Communications of the ACM*, vol. 63, no. 12, Dec. 2020, pp. 33–36. *EBSCOhost*, https://doi.org/10.1145/3387107.

[64]. Humble, Kristian P., and Dilara Altun. "Artificial Intelligence and the Threat to Human Rights." *Journal of Internet Law*, vol. 24, no. 3, Oct. 2020, pp. 1–18. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=147041532&site=ehost-live.

[65]. Humble, Kristian P., and Dilara Altun. "Artificial Intelligence and the Threat to Human Rights." *Journal of Internet Law*, vol. 24, no. 3, Oct. 2020, pp. 1–18. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=aqh&AN=147041532&site=ehost-live.

[66]. King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.

[67]. King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.

[68]. King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.

[69]. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfnkel, B., Dafoe, A., Scharre, P., Zeitzof,

[70]. T., Filar, B., Anderson, H., Rof, H., Allen, G. C., Steinhardt, J., Flynn, C., Héigeartaigh, S., Beard,

[71]. S., Belfeld, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy,

[72]. R., & Amodei, D. (2018). The malicious use of artifcial intelligence: Forecasting, prevention, and

[73]. mitigation. https://arxiv.org/abs/1802.07228.

[74]. King, Thomas C., et al. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science & Engineering Ethics*, vol. 26, no. 1, Feb. 2020, pp. 89–120. *EBSCOhost*, https://doi.org/10.1007/s11948-018-00081-0.