Athens Journal of Law 2024, 10: 1-27
https://doi.org/10.30958/ajl.X-Y-Z

Artificial Intelligence: A Twenty First Century International Regulatory Challenge

By Ori Igwe[*]

Artificial Intelligence (AI) is a twenty first century evolution. Certain aspects of AI have been integrated into daily living. AI applications have also been incorporated into the aviation, banking, cyber security, educational, employment, health, and military sectors respectively. However, the unpredictable nature of AI is a cause for concern because 'In many instances, AI remains under the control of users and designers, but in increasing numbers of applications, the behaviour of a system cannot be predicted by those involved in design and application […]. Newly developed machines are able to teach themselves and even collect data'. Consequently, 'The potential benefits and harms of AI have led to calls for governments to adapt quickly to the changes AI is already delivering and the potentially transformative changes to come. These include calls to pause AI development and for countries […] to deliver a step-change in regulation'. 'In March 2023, more than 1,000 artificial intelligence experts, researchers and backers signed an open letter calling for an immediate pause on the creation of "giant" AIs for at least six months, so the capabilities and dangers of such systems can be properly studied and mitigated' . What are the benefits of AI? What are the risks of AI? Which crimes can be committed via AI? What are the regulatory challenges? What has been the international response? In this article, we will explore whether there is a justification for regulating AI from ethical, legal and law enforcement perspectives.

Keywords: *Artificial intelligence; Ethics; Regulation; Law enforcement*

Incorporation of AI 1Applications into Various Sectors

This paper investigates the legal challenges to the international regulation of AI. It highlights how AI has been incorporated into daily life and identifies benefits and risks of AI. The origin of AI can be traced to 1950 when Alan Turing commonly known as the founding father of AI introduced a test which gauged the ability of machines to independently copy human actions and answer questions so accurately that it is indistinguishable from humans. He established that computers can implement programmed actions.[1] In 1956 the phrase 'AI' was coined by John McCarthy at a summer conference in Dartmouth college. McCarthy and associates suggested that machines can in principle stimulate every aspect of learning or any

[*]PhD, Senior Law Lecturer, University of West London, London, UK.
Email: Ori.igwe@uwl.ac.uk
[1]Brynjolfsson (2022).

other feature of intelligence.[2] From a broad perspective AI can be defined as 'the theory and development of computer systems able to perform tasks normally requiring human intelligence such as visual perception, speech recognition, decision-making, and translation between languages'.[3] Artificial intelligence (AI) is developing rapidly and will change our lives by improving several aspects.[4] The applications range from AI applications enhancing online shopping and personalised shopping to AI applications in scientific areas[5]. The progress of AI in many sectors has proven to be effective.[6]

Integration of AI into Daily Living

AI technologies have been integrated into daily life ranging from voice assistants which complete specific tasks to security gadgets which engage in surveillance actions. In the United Kingdom (UK), statistical data provided by the Office for National Statistics in 2023 demonstrates that individuals and businesses utilise one or more AI applications daily albeit in varying proportions[7]. Pool and Bozic argue that the invention of AI has advantageously enhanced the lives of individuals.[8] They highlight that AI has been incorporated into the transport sector, employment sector, war zone and everyday living. Specifically, digital voice assistants have become a staple in many households because they are simple to use and assist with daily tasks by utilising AI applications. They are also beneficial to people living with disabilities.[9]

Examples of digital voice assistants include Alexa, Echo, Echo Dot, Siri, Google Assistant and Cortana. Individuals can instruct the gadgets to complete tasks such: play music, read the news, control electronic devices, check bank balances, and complete other tasks.[10] Via simple instructions, they can also be asked to provide information on the weather, answer general knowledge questions and swich on/off lights.[11] The amalgamation of AI and machine learning enables such gadgets to recognise the voice of humans and complete specific commands. Given their compatibility with washing machines, light bulbs, ovens, air conditioning units and so on, it has been argued that gadgets such as Alexa, Siri,

[2]Moor (2006).
[3]Tobin (2023).
[4]https://digital-strategy.ec.europa.eu/en/consultations/white-paper-artificial-intelligence-european-approach-excellence-and-trust
[5]https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/key-enabling-technologies/artificial-intelligence-ai-science_en#:~:text=AI's%20role%20in%20science,the%20reach%20of%20current%20tools
[6]Wubineh, Deriba & Woldeyoannis (2024).
[7]https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/articles/understandingaiuptakeandsentimentamongpeopleandbusinessesintheuk/june2023#:~:text=In%202023%2C%2034%25%20of%20UK,study%20(PDF%204.5%20MB)
[8]Poola & Bozic (2017).
[9]Ibid.
[10]Ibid.
[11]Santander (2022).

Google Assistant and Bixby are taking control of our homes.[12] Further, companies such as Amazon, Netflix, and Spotify also utilise algorithms to recommend products and offer personalised customers shopping experiences based on listening and viewing histories. Suffice it to say that AI assists in various tasks ranging from finding routes to industrial process management.[13] Consequently, Caldwell et al assert that AI has pervaded the twenty first century connected world at numerous levels.[14] However from a critical perspective, the actions of AI are unpredictable because although AI is still under the control of users and designers, in a growing number of applications, those people involved in the design and application cannot predict the behaviour of a system.[15] Therefore, the unpredictable feature of AI is concerning given that data is inputted into a "blackbox" that generates output which may adversely affect the daily lives of several individuals. Additionally, new machines can teach themselves and even collect data.[16]

Benefits and Potential Risks of AI

Aviation Sector

In a bid to improve efficiency, safety, and competitiveness, major organisations have put immense pressure on the aviation sector to adopt artificial intelligence technologies (AI).[17] Consequently, the rapid development and implementation of AI technologies in the aviation sector is significantly transforming the aviation eco system.[18] It is envisaged that the adoption of AI technologies will revolutionise operations and resolve challenges[19]. In particular, AI driven tools such as machine learning, natural language processing are being leveraged in the almost all areas of modern aviation from flight planning to aircraft maintenance.[20] Therefore, Kashyap acknowledges that machine learning plays vital roles ranging from traffic management to the identification of passengers.[21] Likewise, Abubakar et al highlight that employing AI in the aviation industry enhances air traffic management, identification of threats, passenger identification, customer services and training and practices.[22] Importantly, Kirwan asserts that leveraging AI in aviation has numerous advantages such as minimising fuel traffic consumption thereby reducing carbon footprint, helping flight crew members in

[12]Ibid.
[13]Caldwell, Andrews, Tanay & Griffin (2020).
[14]ibid
[15]Stahl (2021).
[16]Ibid.
[17]Kabashkin, Misnevs & Zervina (2023).
[18]Kashyap (2019).
[19]Ibid.
[20]Yang & Huang (2003).
[21]Kashyap (2019).
[22]Abubakar, Odunlmi, Mangei & Al-Turjman (2022).

emergencies to identify solutions and analysing voluminous data.[23] Utilising AI in the aviation industry is increasingly widespread and has equipped the industry to "better predict flight demand, optimise schedules and pricing, analyse aircraft data to predict maintenance needs, optimise slot distribution for landing aircraft, facilitate air traffic management, plan fuel efficient routes, and enhance the passenger experience through AI-powered chatbots and virtual assistants"[24].

From an ethical perspective, there are concerns that the integration of AI into the aviation sector poses several risks. Some concerns are that AI technologies can ignore human instructions and act autonomously leading to unintended outcomes like accidents and fatalities. Additional concerns relate to cyber criminals targeting AI enabled aircrafts, air traffic control systems, AI generated aviation programmes, airports, and in-flight entertainment. Also from a cyber security perspective, vulnerabilities in aviation systems can be exploited by threat actors such as hackers, terrorists and state backed actors. This could happen due to various reasons ranging from modifications (patches) not being applied to commercial software to the spoofing of flight data[25]. Further, cyber criminals can exploit vulnerabilities by hacking into aviation technologies such as weak airport telecommunication systems, air traffic controls, data communication systems, Wi-fi networks, entertainment systems, satellite navigation systems, aeroplane, and airports among others.[26] The effects of such cyber-attacks range from increased passport control security checks to cancellation of flights. Consequently, Ishtiaq and Rahman recommend the implementation of defence techniques ranging from an Incident Response Plan to a set of protocols and procedure.[27]

Bank Sector

Some AI applications have been incorporated into the banking sector which have impacted how customers engage in bank transactions daily. Moreover, studies have shown that in the banking sector, AI has been used in several ways in addition to crediting rating models and predication of bank collapses.[28] Importantly, Farishy conducted a study on the use of AI in the banking sector utilising system literature review and found that AI can enhance the banking business by improving accuracy, decision making procedures and efficiency.[29] Additionally, AI can perform customer service tasks in banks and enhance security checks via the use voice recognition AI tools. Further, chatbots can be used in the banking sector to enhance customer performance, streamline sales thereby increasing profits via precise decision making processes.[30] Further, time consuming jobs can be automated by AI resulting in productivity.[31] AI is

[23]Kirwan (2024).
[24]Sadou & Njoya (2023) at 6.
[25]https://www.gao.gov/assets/gao-21-86.pdf
[26]Ishtiaq & Rahman (2021).
[27]Ibid.
[28]Farishy (2023).
[29]Ibid.
[30]Ness & Muhammad (2024).
[31]Khan (2023).

beneficial because it can provide insights into the requirements of customers and notify customers of suspected fraud and increase in subscriptions.[32] Further, via leveraging natural language processing and machine learning algorithms, chatbots have assisted banks greatly by providing tailored and conversational experiences to many user areas.[33] Therefore, Gadhoume highlights various ways in which AI has been successfully integrated into the banking sector ranging from the use of AI to improve customer experience to the use of algorithm trading which enables banks to identify trade patterns, predict trends and undertake profitable trading of stock choices.[34] From an ethical perspective, the use of AI algorithms which are trained on biased datasets can result in discriminatory banking practices which lead to unfair and biased decisions in this sector. Therefore, D'Antonoli reiterates that human biases can be perpetuated by AI algorithms and given their 'blackbox' feature, there is often insufficient transparency in their decision making process.[35] The ability of algorithms to exhibit social biases when considering bank loan applications for example devoid of human input illustrates the risks associated with enabling machines to make such grave decisions.[36]

Cyber Security Sector

There are numerous benefits of integrating AI in the cyber security sector. Some of the benefits include identifying potential threats, preventing fraudulent activities, monitoring network data, responding to potential threats, analysing voluminous network data, predicting threats, identifying vulnerabilities, generating reports, notifying cyber security officials of potential threats, and undertaking difficult time-consuming routine tasks. Specifically, deep learning technologies are AI technologies which can improve cyber security defences and safeguard against a wide selection of cyber threats, including malware, phishing attacks, and insider threats.[37] Importantly, research on the effectiveness of AI-based technologies on organisational cyber security in comparison to traditional cyber security approaches provided key findings.[38]

The research which was based on a systematic literature review of peer reviewed articles from 2013 to 2018 found that AI can have a positive effect on organisational cyber security and can be advantageous in terms of automation, threat intelligence and enhanced cyber defence.[39]

Although AI can enhance the safety of customers and businesses by hindering cyber crime, from an ethical perspective research has found there are several drawbacks ranging from increased adversarial attacks to issues with implementing AI in organisations such as obsolete technological infrastructure

[32]Ibid.
[33]Gadhoum (2022).
[34]Ibid.
[35]'Antonoli (2020).
[36]Owczarczuk (2023).
[37]Jawaid (2023).
[38]Ibid.
[39]Ibid.

lack of good quality 'error-free & clean data.[40] This is significant given that datasets comprising of high quality data are required to train AI models and avoid the inadequacy of AI.[41] Against this backdrop from a social engineering perspective, a study into the utilisation of multifaceted applications of generative AI in social engineering attacks investigated the threat environment. The study which was conducted via the "blog mining technique" found that hackers are utilising generative AI tools such as WormGPT, WolfGPT and FraudGPT to engage in phishing, deepfakes, misinformation, scams, vishing and autonomous industrial scale social engineering attacks.[42] The study emphasised that these cyber security attacks can lead to hacking, data breaches, financial loss, reputational damage and legal implications.[43]Additionally, numerous disadvantages of using AI in cyber security have been identified ranging from adversaries utilising AI for crime to the fact that substantial financial investment/resources are required to integrate AI into the cyber security field.[44] Further, Jawaid reiterates that the challenges of using AI in cyber security range from lack of cyber security professionals with AI expertise to ethical concerns given that AI systems can generate unfair outputs if trained on bias or data.[45] Therefore, vital strategies including promoting trustworthy AI development should be implemented.[46]

Education Sector

The integration of AI into the academic field can have several impacts encompassing education and research. AI can enhance the effectiveness and accuracy of research, improve collection of data and quickly process voluminous data.[47] In terms of AI applications, incorporating various applications like "intelligent tutoring systems, adaptive learning platforms and automated grading tools" can individualise learning, streamline processes and improve accessibility[48]. Further, AI can enhance student engagement, improve student motivation**,** provide individualised learning trajectories[49] and provide individualised student feedback via voice and gesture recognition.[50] Additionally, AI automates boring and lengthy teaching tasks.[51] The utilisation of AI in education has numerous benefits in relation to personalised learning.[52] Significantly, a study which explored the use of artificial intelligence in education found that utilising AI in education created personalised learning pathway like regular access to training in virtual contexts,

[40]Jada & Mayayise (2024).
[41]Ibid.
[42]Falade [2023]
[43]Ibid.
[44]https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity
[45]Jawaid (2023).
[46]Ibid.
[47]Kooli (2023).
[48]Chaushi, Ismaili & Chaushi (2024) at 51.
[49]Ibid.
[50] Ting-Chia, Hsiu-Ling, Gwo-Jen & Mu-Sheng (2023).
[51] Ibid.
[52] Tapalova & Zhiyenbayeva (2022).

adaptation of educational content to personal needs of students, real-time and regular feedback, improvements in the education process and mental stimulations. Likewise, Yang and Zhang note that AI robots can promote the acquisition of knowledge and skills devoid of any guidance from teachers.[53] Additionally a recent study on the pros and cons of Artificial Intelligence in education' found that AI "personalises education, streamlines processes and enhances accessibility with the use of diverse AI applications encompassing intelligent tutoring systems, adaptive learning platforms, and automated grading tools".[54] However from a critical perspective, the recent study conducted by Chaushi et al also found that potential biases and data privacy are ethical challenges of utilising AI in education.[55] Similarly, Kooli emphasises that the use of AI in the academic sector raises ethical challenges in education and research such as perpetuating inherent bias and discrimination, manipulation of AI tools to produce biased results and cheating in assessments.[56] Specifically, Kooli highlights several disadvantages of chatbots specifically ranging from facilitating cheating to a reduction in critical thinking and independent problem solving skills.[57]

Employment Sector

The integration of AI into the job sector is expected to lead to a reduction in arduous lengthy tasks which can be performed autonomously and speedily by AI and to AI performing dangerous jobs. It is also envisaged that AI will create jobs, perform tasks speedier and more efficiently in addition to boosting economic growth and labour productivity via the creation of new jobs and faster working.[58] Although it has been suggested that AI can displace certain jobs, act as a cheaper substitute for employees and perform jobs previously completed by employees, it has nevertheless been acknowledged that the technology can also increase the demand for employees through the creation of new AI related industries for example.[59] Importantly, Liang stresses that AI has changed jobs thereby requiring people to obtain new skills and jointly work efficiently with AI systems. Moreover, Liang argues that AI has created new jobs in areas ranging from AI engineering to AI regulation.[60] Likewise, Bian asserts that via reinstatement in AI related industries, new tasks and jobs may be created thereby increasing labor demand.[61] Similarly, Daniel suggests that AI could create new jobs in machine learning engineering, data science and AI ethics in addition to transforming current jobs which will entail undertaking tasks requiring creativity, critical thinking, emotional intelligence, lifelong learning and upskilling.[62]

[53]Yang & Zhang [2019].
[54]Chaushi, Ismaili & Chaushi (2024) at 51.
[55]Chaushi, Ismaili & Chaushi (2024).
[56]Kooli (2023).
[57]Kooli (2023).
[58]Du (2024).
[59]Bian (2024).
[60]Du (2024).
[61]Bian (2024).
[62]Daniel (2023).

From a critical perspective, there are concerns that the integration of AI and automation into the employment sector will lead to shortage of skills, skills gap, replacement of humans with robots, job loss and revaluation of jobs. Some of the concerns relate to potential job displacements, substitution of jobs, and changes of job structure.[63] Liang emphasises that the integration of AI into industries has had an outstanding effect on employment by enabling the automation of routine and repetitious tasks thereby leading to displacements specifically in the manufacturing sector.[64] Additional potential challenges identified include ethical concerns, lack of comprehensive policies, the threat of AI completing jobs previously held by people and job loss.[65] Sharif et al note that certain AI applications such as automation which are utilised specifically in the e-commerce sector complete predictive analysis tasks speedier than humans. As a result, they argue that certain jobs such as cashiers are being replaced with automated checkout scanners which could lead to job instability if AI completely takes over countless jobs.[66] Likewise, Bian asserts that language models have a significant effect on the employment market and that the displacement effect, productivity effect and reinstatement effect of AI cause instability in the labour market. Hence, Bian suggests that policies should be introduced by authorities to regulate AI.[67]

Health Sector

AI will be increasingly implemented in health care because of the convolution and increase in data in this sector.[68] AI can be deployed for the following: diagnosing illness, analysis of voluminous digital health data, drug development, research, monitoring health, delivering personalised care, performing surgery, and measuring body parts.[69] The various benefits of leveraging AI applications in healthcare range from enhanced patient experience to reduction of mistakes in diagnosis and mistakes.[70] Crucially, medical robots can be used in surgical operations, rehabilitation, social interaction and assisted living.[71] Furthermore, AI assisted robots can perform the task of analysing data "from pre-operative medical records to physically guide a surgeon's instrument in real time during a procedure".[72] The automation of lengthy repetitive tasks via AI can save time thereby enabling health and social care professionals time "to care".[73] Remarkably, algorithms are already exceeding radiologists in spotting malignant

[63]Du (2024).
[64]Liang (2024).
[65]Sharif, Gurbuz & Ay (2023).
[66]Ibid.
[67]Bian (2024).
[68]Davenport & Kalakota (2019).
[69]Naik, Zeeshan, Shetty, Swain, Shah, Paul Aggarwal, Ibrahim, Patil, Smriti, Shetty, Rai, Chlosta, & Somani (2022).
[70]Chen & Decary (2019).
[71]Ibid.
[72]Chen & Decary (2019) at 12.
[73]https://digital-transformation.hee.nhs.uk/building-a-digital-workforce/dart-ed/horizon-scanning/ai-and-digital-healthcare-technologies/introduction/the-impact-of-ai#:~:text=AI%20will%20impact%20the%20health,easily%20be%20automated%204%2C%205

tumours and helping researchers in the construction of groups for clinical trials.[74] For example on 27 June 2023, it was announced in the UK, that an AI machine learning technology named 'Osairis' had been developed by and for the National Health Service (NHS) at Addenbooke's hospital for treating cancers and analysing scans. Significantly, it was reported that 'Osairis' which is the first AI technology to be developed and deployed within the NHS had been vital in decreasing waiting time for cancer patients thereby curtailing doctors' time in preparing scans.[75] A study which was conducted in 2024 by Wubineh, Deriba and Woldeyohannis on the opportunities and challenges of implementing artificial intelligence in healthcare was insightful.[76] The study which analysed 33 published articles between 2015 to 2022 found that leveraging AI leads to several benefits inclusive of "teamwork and decision-making, technological advancement, diagnosis and patient monitoring, drug development, and virtual health assistance".[77] Despite the various beneficial uses of AI in the health sector as discussed above, the use of AI in health care poses challenges regarding who controls the data that is used for AI systems and privacy issues. Additional challenges range from ascertaining who controls the data used by AI systems to the lack of explainability (the black box) of algorithms.[78]

Military Sector

AI can be leveraged in the military sector to mount defence and attack measures in response to malware, virus, hacking, phishing, spyware, and other cyber attacks. Essentially, AI assists in analysing historical data, identifying potential threats and establishing response capabilities in this period of constant cyber threats thereby enabling organisations to manage vulnerabilities, identify vectors, monitor patterns, and implement safety measures. Furthermore, AI plays a vital role in analysing military intelligence in addition to planning and supporting military operations.[79] Critically, AI can enhance the operation of autonomous systems such as unmanned vehicles, increase the abilities of robots to navigate unmanned platforms and enhance the ability to identify and categorise threats.[80] From a defence perspective, the application of AI in the military sector such as machine learning has improved safety practice, identification of targets, threat assessments, security protection, data processing, gathering of intelligence, battlefield decisions and accurate military guidance.[81] In particular, network security is enhanced because cyber attacks can be identified and defined by leveraging machine learning models to analyse network traffic, identify abnormal

[74]Davenport & Kalakota (2019).
[75]https://www.cuh.nhs.uk/news/ai-cuts-waiting-times-for-cancer-patients-in-nhs-first/
[76]Wubineh, Deriba,& Woldeyohannis (2024).
[77]Ibid.
[78]https://digital-transformation.hee.nhs.uk/building-a-digital-workforce/dart-ed/horizon-scanning/ai-and-digital-healthcare-technologies/introduction/the-impact-of-ai#:~:text=AI%20will%20impact%20the%20health,easily%20be%20automated%204%2C%205
[79]Szabadfoldi (2021).
[80]Ibid.
[81]Li (2024).

patterns and promptly respond to detected risks.[82] Also, drones can be used for military wars and ChatGPT can be used to make data driven decisions. From a transportation perspective, the utilisation of autonomous vehicles and Unmanned Aerial Vehicles (UAVs) have become increasingly widespread in the military sector. Further, AI can be used for facial recognition, identification of enemies and the monitoring of targets. Fundamentally, AI can also be used in conflict, intelligence gathering and defence.

Despite the benefits highlighted above, the use of automated tools like robots and drones have raised safety concerns. There are also concerns that cyber criminals like terrorists and hackers can exploit AI systems to engage in robotic assassinations, activate mobile robotic explosive devices and hijack lethal autonomous weapons. These fears are compounded by the fact that there is a lack of human judgement in the leveraging of AI autonomous technologies. Against this backdrop, a report which explored the military applications of AI and its utilisation in war and peace, found that a major opposition was the potential of people being killed by machines with the consent of human operators. [83] Additional issues which were identified were 'decision support systems' which make decisions that choose controversial targets without commanders being able to analyse the complicated assessments for such decisions, facial recognition systems leading to the killing or detaining of citizens and intricate AI predictions misrepresenting them as terrorists or criminals.[84] Li therefore asserts that AI technologies are "potentially disruptive" in the military stage leading to a requirement to set up and support a framework dependent on trust and cooperation between nations.[85] Li argues that the international community is consequently required to establish and follow relevant regulations and guidelines to avoid technological development resulting in unfair competitive advantage.

Ethical and Legal Considerations

The invention, development, and integration of AI into various sectors has raised ethical and legal concerns because AI systems can cause various potential harms ranging from bias and discrimination to unreliable, unsafe, or poor-quality outcomes.[86] As a result, society is dealing with legal and ethical issues emanating from AI encompassing privacy and surveillance, bias or discrimination. Potentially, the philosophical challenge faced is the role of human judgment.[87]

From a legal perspective, concerns have been raised because AI technologies or robots which make decisions leading to accidental deaths cannot be held criminally liable. For example, erroneous decision made by self-driving cars,

[82]Ibid.
[83]Morgan, Boudreaux, Lohn & Ashby (2020).
[84]Ibid.
[85]Li (2024) at 316.
[86]Ibid.
[87]Naik, Zeeshan, Shetty, Swain, Shah, Paul, Aggarwal, Ibrahim, Patil, Amriti, Shetty, Rai, Chlosta & Somani (2022).

automated planes, drones and medical robots leading to accidents or fatalities. In such situations, questions of accountability, liability and responsibility arise because it is debatable if the manufacturer, programmer, operator, human controller, and or retailer should be blamed. Although AI has transformed the banking industry in several ways as discussed above there are numerous ethical risks. The risks include data privacy concerns, bias and unfair outcomes, cyber security concerns, transparency concerns, conflicts with financial institution policies and governance framework due lack of transparency in AI models.[88] In relation to bias, AI systems can generate unfair or inequitable outputs if they are trained on data which is biased or discriminatory.

From a cyber security perspective, data privacy, effects on the ability of humans to make decisions and the prospect of adversaries engaging in cyberattacks constitute serious ethical concerns.[89] Given the ethical challenges which emanate from leveraging AI in the cyber security sector, there is an urgent requirement for "responsible AI practices, transparency and human oversight" to tackle risks and ensure that technologies within the cyber security sector are used ethically.[90] Essentially, AI models need to be constantly monitored in the future, updated and modified to changing cyber threats.[91]

From an educational perspective, the utilisation of AI in education can lead to ethical challenges in relation to data privacy and potential bias.[92] In particular, the utilisation of AI and chatbots in research poses ethical challenges in relation to data collection, use and dissemination in addition to the likelihood of misuse and exploitation.[93] The ethical issue of discrimination can result in biased machine learning algorithms making unfair recommendations for marginalised groups. Further, personal data of young students may be breached if they cannot provide consent.[94]

From an employment perspective, AI can unjustly affect decisions based on factors such as race, gender, sexual orientation and age when hiring or sacking employees. Specifically, the use of AI algorithms which are trained on biased datasets can result in discriminatory employment practices which lead to unfair and biased decisions in these sectors. Therefore, D'Antoni emphasises that inequalities can exits or be reinforced when AI algorithms which are trained on data that inherit biases or include under-represented population characteristics.[95] Further, the impact of leveraging AI and robotics in the employment sector and the prospect of AI systems attaining or surpassing human-equivalent capabilities have raised ethical concerns.[96]

[88]https://www.openaccessgovernment.org/ai-in-the-financial-industry-machine-learning-in-banking
[89]Ali (2024).
[90]Ali (2024) at 80.
[91]Ibid.
[92]Chaushi, Ismaili & Chaushi (2024).
[93]Kooli (2023).
[94]Ibid.
[95]Ibid.
[96]https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

From a healthcare perspective**,** the utilisation of AI in clinical practice raises the specific ethical issues of informed consent to use data, safety and transparency, algorithmic fairness and biases, and data privacy.[97] Davenport asserts that the use of AI in healthcare raises the following varied ethical implications: accountability, transparency, permission, and privacy.[98] Importantly, a recent study which was conducted by Wubineh, Deriba and Woldeyohannis on the opportunities and challenges of implementing AI in health care found that in addition to providing several benefits, using AI in the health sector impedes multifaceted difficulties, encompassing 'ethical and privacy-related issues, lack of awareness, unreliability of technology, and professional liability'.[99]

Similarly, from a military perspective, Li highlights that the extensive use of machine learning has led to issues with personal privacy and data security.[100] Furthermore, machine learning models can generate unfair and unjust outcomes if they are trained on data which are inherently biased.[101] Moreover, autonomous technology operated via machine learning such as drones which search for, identify hidden targets and hit enemy targets can make erroneous judgments or choose to ignore human instructions thereby leading to unintended fatalities. Such errors raise the issues of accountability for crimes committed and transparency. The concern is justifiable given that autonomous robotic vehicles, and autonomous robots otherwise referred to as 'killer robots' sometimes act without control.[102] There is also the added issue of innocent people being wrongly identified as targets by facial recognition. Against this background, Morgan et al conducted a study which investigated the military application of AI and explored the ethical effects of utilising them in war and peace. The study found that participants identified several ethical risks ranging from accountability and moral responsibility to human rights and privacy.[103] Therefore, Ali stresses the need to develop AI tools that 'augment human capabilities, provide explainable insights, and enable effective collaboration between human experts and algorithms.[104]

Crimes Committed by Artificial Intelligence

AI can play a growing role in the commission of criminal acts given that the digital nature of AI enables it to be used legitimately and for crimes.[105] King et al conducted a study on foreseeable threats posed by AI crimes. Crucially the study revealed that AI can be used for committing crimes ranging from sexual offences

[97]Naik, Zeeshan, Shetty, Swain, Shah, Paul, Aggarwal, Ibrahim, Patil, Amriti, Shetty, Rai, Chlosta & Somani (2022).
[98]Davenport & Kalakota (2019).
[99]Wubineh, Deriba & Woldeyohannis (2024) at 1.
[100]Li (2024).
[101]Ibid.
[102]Morgan, Boudreaux, Lohn & Ashby (2020).
[103]Ibid.
[104]Ali (2024) at 83.
[105]King, Aggarwal, Taddeo & Floridi (2019).

to theft.[106] Further, a study conducted by Caldwell, Andrews & Griffin, on AI-enabled future crimes highlighted eighteen categories of threats ranging from Audio/Video impersonation to forgery.[107] Although the study acknowledged that AI can be advantageous to individuals and organisations, it revealed that AI can also be used to commit offences such as blackmail via the use of fake videos, theft, extortion, intimidation, and terror.[108] Crucially, the study identified several means via which AI can assist criminals ranging from deepfakes to tailored phishing.[109] Consequently, from a criminal perspective, Dupuont et al suggest that three imminent consequences regarding the risks created by AI are the expansion of existing threats, creation of entirely new threats and modification of the nature of threats.[110] Additionally, Brundage et al identify potential scenarios for the malicious use of AI and make various policy recommendations which include the requirement for a multilateral cooperation.[111]

Specifically, criminals can use AI to engage in criminal activities such as fraud, hacking, phishing, vishing, stalking, sexual offences, terrorist offences, intellectual property offences and smuggling of drugs and offensive weapons via unmanned cars. From a global perspective, the ability of criminals to leverage AI for crimes is concerning because they can commit crimes via AI automation such as using drones, lethal autonomous weapons, and self-driving cars to commit murder globally. Hence Stahl stresses that autonomous weapons which can decide who and when to attack are available by extension to terrorists in addition to governments.[112]Against this background, Falade carried out a study into how several applications of Generative AI are leveraged in social engineering attacks using the technique of blog mining method to obtain data on social engineering attacks involving generative AI.[113] The research explored how cybercriminals can engage in cyber attacks using ChatGPT, FraudGPT and WormGPT AI models. Significantly, the study found that the types of social engineering attacks generated by AI are phishing, pretexting, scams and deepfakes. In particular, the research revealed that such attacks can lead to various offences ranging from disinformation to cyber security challenges.[114] Pivotally, the study established that threat actors engage in such offences by crafting tailored phishing emails, crafting undetectable malwares, creating deepfake videos and virtual identities, creating deepfake websites, engaging in voice cloning and vishing attacks, using AI

[106]Ibid.
[107]Caldwell, Andrews & Griffin (2020).
[108]Ibid.
[109]Ibid.
[110]https://www.researchgate.net/publication/337402608_Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice/link/5dd57d34299bf11ec866c413/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
[111]https://www.researchgate.net/publication/323302750_The_Malicious_Use_of_Artificial_Intelligence_Forecasting_Prevention_and_Mitigation/link/5a942764aca2721405668800/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
[112]Stahl (2021).
[113]Falade (2023).
[114]Ibid.

phishing tools, using automation for cyber attacks and relying on the adaptive learning abilities of AI.[115]

Regulation

There are numerous ethical and legal concerns about leveraging AI technologies in different sectors such as algorithmic bias, accountability, privacy, transparency, explainability and job loss. There is also a growing fear that humanity faces existential risks because AI technologies can reason, understand, learn and utilise their own intelligence to solve problems. Against this background, Mclean et al stress that Artificial General Intelligence (AGI) which is the forthcoming generation of AI, is anticipated to exceed human intelligence in every way.[116] There is currently no international unified AI strategy.[117] Thus, there have been calls for the regulation of AI to ensure that it is designed ethically, responsibly and safely. Particularly, Chavali, Baburajan, Kumar & Chandana Katari argue that the creation of a strong regulatory system is required to combat the ethical, legal and societal issues which emanate from using AI.[118] They suggest that this is vital to engineer the trustworthy development and deployment of AI tools.

From a legal perspective, the challenge of accountability has been raised in the healthcare sector. Importantly, D'Antonoli questions who will be accountable for an unintended result if an error is made by an AI system given that it is not certain if is the user, the auditor, or the producer of the algorithm will be deemed responsible.[119] Similarly, Kirwan highlights that the application of AI in the aviation industry produces adverse results and leads to safety issues.[120] Further, AI may lead to no one being held accountable for any damage done given that the extent of danger is unascertained and utilisation of machines will restrict the ability of people to find someone at fault and responsible for the decision making.[121] From a safety perspective, the conundrum of who is to blame when pilots act on their own judgements instead of AI tools or follows unsafe advice from AI technologies resulting in accidents and fatalities is an ethical issue.[122] Additionally, the militarisation of AI has very serious implications for global security and warfare.[123] Against the above background, governments will have to decide to hold either designers of AI or their owners and users liable.[124]

From a cyber security perspective, because the integration of AI into the cyber security sector specifically has raised several ethical issues, it has been

[115]Ibid.
[116]Mclean, Read, Thompson, Baber, Stanton & Salmon (2023).
[117]Panait, Lubenkov & Alic (2021).
[118]Chavali, Baburajan, Kumar & Chandana katari (2024).
[119]D'Antonoli (2020).
[120]Kirwan (2024).
[121]Naik, Zeeshan, Shetty, Swain, Shah, Paul, Aggarwal, Ibrahim, Patil, Amriti, Shetty, Rai, Chlosta & Somani (2022).
[122]Kirwan (2024).
[123]https://unu.edu/article/militarization-ai-has-severe-implications-global-security-and-warfare
[124]Khalaileh (2023).

suggested that a balance ought to be struck between utilising the strength of AI for cybersecurity and instituting strong regulatory measures to ensure responsible and ethical use.[125] From an employment perspective, on 17 July 2023, Hollywood stars went on a strike in front of NETFLIX and Disney headquarters.[126] Two main reasons for the strike were the advent of AI in the acting industry and the financial impact of streaming services on staff payments. Similarly on 21 July 2023, UK actors and actresses held a London rally in Leicester Square in support of the US actors and actresses.[127] There have also been recent renewed calls for AI to be regulated. For example, on 14 June 2024 during the recent G7 summit in southern Italy, Pope Francis urged G7 leaders to ban the use of autonomous weapons.[128] He asserted that such weapons should not be empowered to decide who will live or die. He requested for an AI treaty to ensure that AI is developed ethically and morally.

UK's Repones to the Regulation of AI

In 2021, the UK government published a National AI Strategy which is a 10-year plan to make the UK a "global AI superpower" by focusing on three specific aims ranging from investing and planning to ensuring that the UK is on board with the national and international governance of AI technologies.[129] On 29 March 2023, the government published a White Paper titled 'Pro-Innovation Approach to AI Regulation' which highlighted that regulators should apply five principles in regulating AI ranging from safety, security and robustness to contestability and redress.[130] The UK government confirmed that it intends to encourage regulators to use powers and resources available to them in implementing the cross sectoral principles to govern the safe and innovative use of AI.[131] Significantly on 1 and 2 November 2023, UK hosted the first global AI Safety Summit at Bletchely Park which discuss safety measures for addressing risks from AI. Importantly, the global summit was attended by representatives from 28 nations, including the US, EU, and China which endorsed the Bletchley Declaration.[132] The declaration is a committed agreement to support a globally inclusive network of scientific research on advanced AI safety and promote the advantageous use of technology for the good of all. [133]

[125]Ali (2024).
[126]Sankaran (2023).
[127]https://www.theguardian.com/culture/2023/jul/21/uk-star-london-rally-support-striking-us-actor-brian-cox-equity-union
[128]https://www.theguardian.com/world/article/2024/jun/14/pope-tells-g7-leaders-ai-can-be-a-both-terrifying-and-fascinating-tool#:~:text=Pope%20Francis%20has%20made%20a,of%20autonomous%20weapons%20in%20war
[129]https://researchbriefings.files.parliament.uk/documents/CDP-2023-0152/CDP-2023-0152.pdf
[130]Department for Science, Innovation and Technology (2023a).
[131]ibid
[132]Department for Science, Innovation and Technology (2023b).
[133]https://data.parliament.uk/DepositedPapers/Files/DEP2024-0504/Annex_A_-_Call_for_Views_on_the_Cyber_Security_of_AI__1_.pdf

Australia, Canada, China and US's Responses to the Regulation of AI

Australia

On 24 January 2024, the Australian Government Productivity Commission published a research paper on the challenges of regulating AI.[134] The paper identified four essential steps for regulating AI. The first step is establishing how the technology is currently being used or probably to be used in the imminent future. The second step is determining if the use of the technology leads to heightened risks of serious harm in comparison to the counterfactual. The third step is ascertaining the people who can influence risks and outcomes. The fourth step is to establish if the risk is being tackled by existing regulation or if legislation ought to be extended or amended.[135] It is anticipated that in addition to formal regulation, industry self-regulation will contribute to the regulation of AI in Australia.

Canada

In comparison to Australia, Canda is expected to regulate AI via the Artificial Intelligence and Data Act (AIDA).[136] Importantly, the Act will define the basis for the responsible design, development and deployment of AI which affect the lives of Canadians. The AIDA was established as part of the Digital Charter Implementation Act 2022.[137] Significantly, in September 2023, a Voluntary Code of Conduct was publicised by Canadian government. The code highlights general standards for companies and enables companies to prove that their companies are developing AI technologies trustworthily prior to the enactment of formal regulation.[138]

China

In China, attempts have been made to introduce regulatory measures. For example, in 2017, the Peoples Republic of China state council approved the *New Generation Artificial Intelligence Development Plan.* [139]The plan is significant because it highlights the development of AI as a priority and discusses the national AI strategy with a view to model China as the global leader in AI by 20230.[140] Additionally, in September 2022 Shanghai enacted a law to regulate the development of the AI industry which arguably promotes the innovative AI development in by the industry sector.[141] Further in September 2022, the Shenzhen regulation was passed which supports Chinese governmental

[134]https://www.pc.gov.au/research/completed/making-the-most-of-the-ai-opportunity/ai-paper2-regulating.pdf
[135]ibid
[136]Hereinafter - Artificial Intelligence and Data Act.
[137]Ibid.
[138]https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems
[139]Filipova (2024).
[140]Ibid.
[141]https://www.sidley.com/-/media/resource-pages/ai-monitor/laws-and-regulations/20220922-shanghai-regulations-on-promoting-the-development-of-artificial-intelligence-industry.pdf?la=en

organisations to lead AI implementation and development.[142] Moreover via the Personal Information Protection Law[143], Cyber Security law[144] and the Data Security Law[145], specific aspects of designing and using AI have been regulated.

USA

In the US, boosting leadership in AI is an uppermost prime concern which is promoted by the Biden Administration. [146] Consequently in 2019, a senate taskforce on AI was set up which has since passed 15 bills into law that prioritises research and risk assessment. Additionally, in January 2021, the Artificial Intelligence Initiative Office was established by the White House Office of Science and Technology Policy. Further, on 23 October 2023, President Joe Biden signed an Executive Order "to advance efforts across the federal government, building on previous actions to harness the benefits and mitigate the risks of AI". The Executive Order is expected to promote the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence.[147] On 28 March 2024, it was reported that the Biden Administration issued 3 new policies.[148] The policies were introduced in response to increasing concerns ranging from risks created by AI in the US workforce sector to potential discrimination in decision-making.[149] Additionally, on 28 March 2024 a memorandum which identified new agency requirements and guidance for AI governance, innovation, and risk management was signed for the heads of executive departments and agencies.[150]

European Union's Repones to the Regulation of AI

The European Union (EU) has taken several steps to regulate AI between 2018 and 2024 specifically. In 2018, the European commission published a European strategy aimed at tackling issues and maximising benefits offered by AI. The strategy has a three-pronged approach to 'boost the EU's technological and industrial capacity and AI uptake across the economy, prepare for socio-economic changes, and ensure an appropriate ethical and legal framework'.[151] Additionally in 2018, the European AI Alliance was set up by the European Commission in 2018 to start a conversation on AI. The alliance which promotes trustworthy AI by sharing best practices among the members and helping developers of AI and other

[142]Filipova (2024).
[143]https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/
[144]ibid
[145]https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/
[146]Panait, Lubenkov & Alic (2021).
[147]https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence
[148] https://eu.usatoday.com/story/news/politics/2024/03/28/biden-unveils-new-policies-for-use-of-ai-by-federal-government/73122365007/
[149]ibid
[150]https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf
[151]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0168

stakeholders to apply vital requirements has engaged approximately 6000 stakeholders via regular events, public consultations, and online forum exchanges. The 4th AI Alliance Assembly was held in Madrid n 16 and 17 November 2023, and focused on policy aspects that are leading trustworthy AI globally.[152] Further in 2018, the European Commission appointed the High-Level Expert Group on Artificial Intelligence (AI HLEG) to advise on the implementation of a European Artificial Intelligence Strategy. Importantly, a report on the Ethics Guidelines for Trustworthy AI was produced by the group which identified 7 crucial requirements, which every AI technology should meet before it is deemed safe and trustworthy.[153] The requirements range from human agency and oversight to accountability.

In response to the calls for the regulation of AI, the EU commission put forward the Artificial Intelligence Act (AIA) in a bid to balance the AI development by the police against the safeguarding of fundamental human rights and societal values.[154] The Act is revolutionary because it highlights that accountability and transparency are important pillars in democratic societies.[155] On 13 March 2024, the AIA was adopted by the European commission. The Act is the first global legal framework for AI. The AIA sets out a cross-sectoral regulatory approach to the use of AI systems across the European Union (EU) and its Single Market. The legal framework incorporates a risk-based approach which promotes the regulation of AI applications which are considered high risk. The AIA identifies a four-tiered risk approach which acknowledges the different categories of risks created by AI to health, Safety and/or fundamental human rights. The levels of risks are unacceptable, high, limited and minimal.[156] The four categories of risks protect "fundamental rights, consumer rights and safety"[157]. Further, the AIA sets out proportionate requirements and obligations per risk level. However, critics have argued that the Act is problematic. Specifically, Vainionpää, Väyrynen, Lanamäki and Bhandari conducted a study on the challenges and criticisms of the European Artificial Intelligence Act. The study was based on a "disciplined -agnostic systematic literature review that captured all relevant peer reviewed English-language research on the AIA"[158]. Crucially, the study identified the following problems regarding the AIA:

1. Premise and approach of the AIA
2. Scope of the AIA
3. Formation and wording of the AIA
4. Requirements of the AIA
5. Compatibility and alignment with the existing regulatory landscape

[152]https://digital-strategy.ec.europa.eu/en/events/4th-european-ai-alliance-assembly-leading-trustworthy-ai-globally>
[153]https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf
[154]AIA – hereinafter Artificial Intelligence Act. https://www.policechiefmagazine.org/policing-ai-driven-world-europol/
[155]ibid
[156]https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[157]Penait, Lubenkov & Alic (2021) at 30.
[158]Vainionpää, Väyrynen, Lanamäki & Bhandari (2023) at 3.

6. Compliance with and enforcement of the AIA
7. Expected impact of the AIA

Against the above background, it was highlighted that: "The complexity and potential risks of AI make it essential to establish regulatory frameworks to ensure responsible and ethical development and use of AI aligned with societal values"[159].

Additionally, the EU has implemented the General Data Protection Regulation which governs the processing and free movement of personal data.[160] The regulation constitutes a legal guide on data protection and privacy when utilising AI. It provides instructions on the processing of personal data and the free movement of such data with a view to safeguarding privacy.

Due to a lack of global regulation of AI, several independent initiatives have been launched internationally.[161] Consequently, in March 2021 specifically, the European parliament published a study which revealed twenty one international initiatives that had been initiated by the following countries, Germany, United Kingdom, United States, Japan, The Netherlands, Belgium Finland, Europe, Canada, and Switzerland.[162] The study was pivotal because it provided useful information on initiatives, locations, key issues tackled, publications and sources of funding. Additionally, the study revealed numerous ethical harms tackled by the various international initiatives. Specifically, the study identified key issues which emerged from the initiatives and categorised them into twelve. The twelve categories range from human rights and well-being to existential risk. Importantly, five out of the twelve categories are regularly discussed in academic literature. The categories are Accountability and responsibility; Security, privacy, accessibility, and transparency; Safety and trust; Lawfulness and justice; and Control and the ethical use-or misuse-of AI.

Ethical, Legal and Law Enforcement Justifications for Regulating AI

From an ethical perspective, the design, manufacturing, programming, implementation, and utilisation of AI technologies should be regulated to ensure the fair, safe, trustworthy, and transparent use of AI for the common good. Regulating AI will promote the safe, responsible, trustworthy use and design of technologies.

From a legal standpoint, regulatory measures will provide a legal basis for prosecutors to hold people accountable for crimes and mistakes that are engaged in via leveraging or instructing AI. In effect, the introduction and implementation of regulatory measures will mitigate risks ranging from bias to lack of accountability. Significantly, the issue of establishing who should be held accountable and culpable for mistakes made by AI can be resolved via either the enactment of robust laws or the implementation of existing adequate laws given that there is an

[159]Vainionpää, Väyrynen, Lanamäki & Bhandari (2023) at 1.
[160]https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en
[161]https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf
[162]Ibid.

ongoing debate on whether AI should be recognised as having 'legal personhood' or 'legal autonomy'.[163]

From a law enforcement perspective, the regulation of AI will promote safety, security, governance contestability and the seeking of redress. Crucially, the regulation of AI will enable law enforcement officials such as police officers to hold people accountable and investigate AI generated cyber crimes, such as fraud, misinformation, terrorism, intellectual property offense and manslaughter. Additionally, when mistakes are made by AI technologies or inherent flaws lead to unintended outcomes, culprits will be hindered from evading criminal or tortious liability by arguing that they did not anticipate that AI would engage or not engage in an act.[164] To this effect, from a military perspective, it has been highlighted that the development of AI technologies such as 'autonomous weapons, drone technologies, robotic assassinations and mobile-robotic improvised explosive devices' ought to be scrutinised.[165] Moreover, it has been emphasised that the immediate need for regulation is demonstrated by the following additional concerns: privacy violation, algorithmic bias, employment displacement.[166] It is anticipated that the various justifications for regulating AI will ensure that such technologies are designed and deployed for the common good.

Challenges to the Regulation of AI and Justifications for regulation

Although ethical and legal concerns posed by AI technologies have led to calls for regulation, several challenges could impede the regulation of AI. This is more so because there are various actors, implications of AI, technical terminologies and evolving applications.

Definition of AI

There is no globally agreed definition of AI. Consequently, any possible global progress on this is impeded because countries are "oblivious of the scope of commitment shall always be rooted to the absence of clear definition of the subject matter"[167]. There is also a wide range of definitions which changes with the passage of time.[168] An additional dilemma is ascertaining if AI should be defined from a broad perspective which promotes a flexible interpretation or a narrow perspective which offers a specific interpretation.

[163]Stahl (2021).
[164]Ibid.
[165]Ibid.
[166]Chavali, Baburajan, Kumar & Chandana Katari (2024).
[167]Khalaileh (2023) at 23.
[168]Schuett (2019).

Cross Jurisdictional Feature of AI

Given the borderless feature of AI, variations can exist in definitions adopted by several governments because there is no consensus on a global definition of AI. Moreover, the lack of a clear agreement on the legal definition can lead to ambiguity if different governments adopt varied definitions. Further, the effects of AI in regions will be different thereby requiring the creation of distinct regulations. Consequently, Walter asserts that although the borderless feature of AI requires international cooperation, this may not be possible due to various cultural, ethical and legal standards that exist in several nations.[169]Against this backdrop, Shuett suggests that the legal definition. of AI should contain the following requirements: inclusiveness, precision, comprehensiveness, practicability and permeance.[170]

The Rapid Advancement of AI and Lack of Legal Expertise

The swift advancement and evolution of AI poses another challenge because it necessitates constant regulatory changes to ensure that AI regulations are up to date. The speedy development of AI tools frequently outpaces the rate at which legislation can be developed and enforced.[171] To this effect, it has been highlighted that "the largely unpredictable and dynamic nature" of AI are factors which constitute problems with regulating such technologies in addition to the "traditional approach to legislation which is reactionary and too slow to be adopted or amended"[172]. The rapid evolution of AI is a huge obstacle which hinders prompt introduction of regulatory measures which can match the pace of AI development. Crucially, Walter acknowledges that there is an inconsistency between technological advancements and the capacity of regulatory structures in protecting democratic values and human rights particularly. [173] Walter writes from a perspective which suggests that there are socioeconomic consequences which can emanate from creating a global policy and promoting governance in AI regulation.

Another regulatory challenge is the lack of legal expertise required to draft adequate laws which are sufficiently detailed and fulfil the legal certainty fundamental law requirement.[174] This challenge is compounded by the technological intricacies, complexities and non-transparent features of AI. Collectively, the numerous challenges discussed above are worsened by the fact that there is an onus on regulators to arguably balance the need to promote innovation against the adequate regulation of AI.

[169]Walter (2024).
[170]Schuett (2019).
[171]Walter (2024).
[172]Owczarczuk (2023) at 300.
[173]Walter (2024).
[174]Kaal (2016).

Conclusion

The integration of AI into the aviation, banking, cyber security, education, employment, health, and military sectors respectively has several benefits and potential risks. The continuous advancement of AI necessitates the urgent requirement for regulation to tackle ethical and legal concerns. From a law enforcement perspective, given that many criminals can target victims globally via AI, robust legislative measures need to be introduced at national and international levels to address such deviant acts. In regulating AI, a balance should be struck between integrating the strengths of AI into various sectors and implementing effective regulatory measures to ensure the responsible and ethical use of AI. Regulations should evolve as AI advances to ensure that the measures are up to date. This is imperative given the fears over AI becoming conscious, cleverer than humans and leading to the extinction of humans. Given the constant advancement of AI, it is vital that regulatory measures cover current and anticipated individual and societal implications to avoid being obsolete or inadequate. Regulators should perform a balancing exercise between innovation and mitigation of risks in a bid to promote enforcement and compliance.

Acknowledgements

Our thanks to Athens Institute for Education and Research for allowing us to modify templates they had developed.

References

Abubakar, E., Odunlmi, E., Mangei, T. & F. Al-Turjman (2022). *AI Application in the Aviation Sector*. https://www.researchgate.net/publication/370177151_AI_Application_in_theAviation_Sector

AIA. https://www.policechiefmagazine.org/policing-ai-driven-world-europol

Ali, B. (2024). 'Revolutionizing Cybersecurity: The Role of Artificial Intelligence in Advanced Threat Detection and Response' in *International Journal of Applied Mathematics and Computer Science* 3(7):77-85.

Australian Government Productivity Commission (2024). '*Making the most of the AI opportunity Research Paper 2 The Challenges of regulating AI'*. https://www.pc.gov.au/research/completed/making-the-most-of-the-ai-opportunity/ai-paper2-regulating.pdf

Belani, G. (2016). 'The use of Artificial Intelligence in Cyber Security: A review'. https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

Bian, Z. [2024]. 'Research on the impact of Artificial Intelligence on the Labor Market' in *Highlights in Business, Economics and Management* 24:1036-1041.

Brundage, M., Avin, S,. Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allem,G.C., Steinhardt, J., Flynn, C., dEigeartaigh, S.O., Beard, S., Balfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O, Page, M., Bryson, J., Yampolsky, D. & D. Amodei (2018). 'The

Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation'. https://doi.org/10.48550/arXiv.1802.07228

Brynjolfsson, E. (2022). 'The Turing Trap' in *AI & Society* 151(2):272-287.

Caldwell, M., Andrews, J.T.A., Tanay, T. & L.D. Griffin (2020). 'AI-enabled future crime' in *Crime Science* 9(1), art. 14. DOI: 10.1186/s40163-020-00123-8

Chen, M. & M. Decary (2019). 'Artificial Intelligence in healthcare: an essential guide for health leaders' in *Healthcare Management Forum* 33(1):10-18.

Chavali, D., Baburajan, B., Kumar, V. & S. Chandana Katari (2024). 'Regulating Artificial Intelligence Developments and Challenges' in *International Journal of Pharmaceutical Sciences* (3)2:1250-1261.

Chaushi, B.A., Isamaili, F. & A. Chaushi (2024). 'Pros and Cons of Artificial Intelligence in Education' in *International Journal of Advanced Sciences and Engineering Researches* 8(2):51-57.

Davenport, T. & R. Kalakota (2019). 'The potential for artificial intelligence in healthcare' in *Future Healthcare Journal* (6)2:94-98.

D'Antonoli, T. (2020). 'Ethical Considerations for artificial intelligence: an overview of the current radiology landscape' in *Diagn Interv Radio* 26(5):504-511.

Du, J. (2024). 'The Impact of Artificial Intelligence Adoption on Employee Unemployment: A Multifaceted Relationship International' in *Journal of Social Sciences and Public Administration* (2)2:321-327

Daniel, S. (2023). The Impact of Artificial Intelligence on Employment and Workforce Dynamics in Contemporary Society Authors [Online] https://www.researchgate.net/publication/376795973_The_Impact_of_Artificial_Intelligence_on_Employment_and_Workforce_Dynamics_in_Contemporary_Society_Authors

Data Security Law of the Peoples Republic of China-Effective Nov.1 2021 (2021) [translation]. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

Dupont, B., Westermann, H., Stevens, Y.Y. & M. Joyce (2019). Artificial Intelligence in the Context of Crime and Criminal Justice. https://www.researchgate.net/publication/337402608_Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice/link/5dd57d34299bf11ec866c413/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19>

Department for Science, Innovation and Technology - [A pro -innovation approach to AI regulation (2023a). https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

Department for Science, Innovation and Technology (2023b). The Blethchely Declaration by Countries Attending the AI Safety Summit 1-2 November 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Dupont, B., Stevens, V., Westermann, H., & Joyce, M., (2019). 'Artificial Intelligence in the Context of Crime and Criminal Justice' https://www.researchgate.net/publication/337402608_Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice

European Commission (2019). Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee of the Regions [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0168

European Commission (2024). Artificial Intelligence (AI) in Science. https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/artificial-intelligence-ai-science_en

European Commission (2020). White Paper on Artificial Intelligence-A European Approach to Excellence and Trust. https://eur-lex.europa.eu/legal content/EN/TXT/ PDF/?uri=CELEX:52020DC0065

European Parliament (2020). The Ethics of artificial intelligence: Issues and Initiatives. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

Falade, V.P. (2023). 'Decoding the Threat Landscape: ChatGPT, FraudGPT and WormGPT' in *International Journal of Scientific Research in Computer Engineering and Information Technology* 9(5):185-198.

Filipova, I. (2024). 'Legal Regulation of Artificial Intelligence: Experience of China' in *Journal of Digital Technologies and* Law (2)1:46-73.

Farishy, R. (2023). 'The Use of Artificial Intelligence in Banking Industry' in *International Journal of Social Service and Research* 3(7):1724-1731.

Gadhoum, Y. (2022). 'Artificial Intelligence Trends and Ethics: Issues and Alternatives for Investors' in *Intelligent Control and Automation* 13(1):1-15.

Garrison, J. (2024). 'Biden administration unveils new rules for federal government's use of artificial intelligence' USA Today 28 March 2024. https://eu.usatoday.com/story/news/politics/2024/03/28/biden-unveils-new-policies-for-use-of-ai-by-federal-government/73122365007/

Government Accountability Office (2020). 'Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks' [Online] https://www.gao.gov/products/gao-21-86

Government of Canada (2023). 'Artificial intelligence and Data Act'. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act

Hern, A. (2023). Elon Must joins calls for pause on creation of giant AI 'digital minds'. https://www.theguardian.com/technology/2023/mar/29/elon-musk-joins-call-for-pause-in-creation-of-giant-ai-digital-minds

Ishtiaq, S. & N.A.A. Rahman (2021). 'Cyber security Vulnerabilities and Defence Techniques in Aviation Industry' in *Atlantis Insights in Computer Sciences Proceedings of the 3rd International Conference Integrated International Computing Communication & Security*. https://www.researchgate.net/publication/374985143_Artificial_Intelligence_in_Aviation_New_Professionals_for_New_Technologies

Jawaid, A.S. (2023). 'Artificial Intelligence with Respect to Cyber Security' in *Journal of Advances in Artificial Intelligence* 1(2):2-12.

Jada, I. & T.O. Mayayise (2024). 'The Impact of artificial intelligence on organizational cyber security: an outcome of a systematic review' in *Data information management* 8(2). https://doi.org/10.1016/j.dim.2023.100063

Kaal, W. (2016). 'Dynamic Regulation for Innovation'. SSRN Electronic Journal. DOI:10.2139/ssrn.2831040

Khan, H. (2023). 'AI in the financial industry: Machine Learning in Banking' https://www.openaccessgovernment.org/ai-in-the-financial-industry-machine-learning-in-banking/165122/

Kooli, C. (2023). 'Chatbots in Education and Research: A Critical Examination of Ethical Implications and Solutions' in *Sustainability* 15(7):1-15.

Kabashkin, I., Misnevs, B. & O. Zervina (2023). 'Artificial Intelligence in Aviation: New Professionals for New Technologies' in *Appl. Sci*. 13(21), 11660**.** https://doi.org/10.3390/app132111660

Khalaileh, Y. (2023). 'Accommodating Artificial intelligence in international law: An Overview and New Frontier' in *Journal of Human Security* (19)1:22-31.

Kashyap, R., (2019). 'Artificial Intelligence Systems in Aviation'. https://www.researchgate.net/publication/330573828_Artificial_Intelligence_Systems_in_Aviation

Khomami, N. (2013). 'UK Stars hold London Rally in support of striking US stars'. https://www.theguardian.com/culture/2023/jul/21/uk-star-london-rally-support-striking-us-actor-brian-cox-equity-union

Kirwan, B. (2024). 'The Impact of Artificial intelligence on Future Aviation Safety Culture Future' in *Transportation Future Transp*. 4(2):349-379.

King, T.C., Aggarwal, N., Taddeo, M. & L. Floridi (2019). 'Artificial Intelligence Crime: An interdisciplinary analysis of Foreseeable Threats & Solutions' in *Sci. Eng. Ethics* 26:89-120.

Li, L. (2024). 'AI and the Future of War: The Impact of Machine Learning in Security Space' in *The International Journal of Computer Science and Information* Technology (2)1:315-318

Liang, Y. (2024). 'The Impact of Artificial Intelligence on Employment and Income Distribution' in *Journal of Education, Humanities and Social Sciences* 27:166-171.

Marwala, T. (2023). 'Militarization of AI Has Severe Implications for Global Security and Warfare'. https://unu.edu/article/militarization-ai-has-severe-implications-global-security-and-warfare

Mclean, S., Read J.G.M., Thompson, J., Baber, C., Stanton, N.A. & P.M. Salmon (2023). 'The risks with Artificial General Intelligence: A systematic review' in *Journal of Experimental & Theoretical Artificial Intelligence* 35(5):649-663.

Morganm, F., Boudreaux, B., Lohn, A. & M. Ashby (2020). 'Military Application of Artificial Intelligence: Ethical Concerns in an Uncertain World'. DOI:10.7249/RR3139-1

Moor, J. (2006). 'The Dartmouth College of Artificial Intelligence Conference: The Next Fifty Years'. *AI Magazine, 27(4), 87*. https://doi.org/10.1609/aimag.v27i4.1911

Naik, N., Zeeshan H. Shetty, D.K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B.P., Chlosta, P. & B.K. Somani (2022). 'Legal and Ethical Concerns in Artificial Intelligence in Healthcare: Who Takes Responsibility?' in *Front Surg. 2022 Mar 14;9:862322*. Doi: 10.3389/fsurg.2022.862322.

Ness, S. & T. Muhammad (2024). 'Banking 4.0: The Impact of Artificial Intelligence on the Banking Sector and its Transformation of Modern Banks' in International Journal of Advanced Scientific Research & Development (IJASRD) 9(2):5. DOI:10.5281/zenodo.10707418

NHS (2023). The Impact of Artificial Intelligence (AI) https://digital-transformation.hee.nhs.uk/building-a-digital-workforce/dart-ed/horizon-scanning/ai-and-digital-healthcare-technologies/introduction/the-impact-of-ai#:~:text=AI%20will%20impact%20the%20health,easily%20be%20automated%204%2C%205

NHS Cambridge (2023). 'AI cuts waiting time for cancer patients in NHS first'. https://www.cuh.nhs.uk/news/ai-cuts-waiting-times-for-cancer-patients-in-nhs-first/

Owczarczuk, M. (2023). 'Ethical and regulatory challenges amid artificial intelligence development: an outline of the issue' in *Economics and Law* 22 (2):296-305.

Panait, C., Lubenkov, D. & D. Alic (2021). 'Striking the balance between innovation and regulation in AI - is Europe leading the way or lagging behind?' in *Europuls Policy Journal* 1:27-45.

Personal Information Protection Law of the Peoples Republic of China-Effective Nov.1 2021 (2021) [translation]. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Poola, I. & V. Bozic (2017). 'What an Artificial Intelligence in Impacting Real Life' in *International Journal of Advance Research and development* 2(10):96-100.

Rough, E. & N. Sutherland (2023). 'Debate on Artificial Intelligence'. https://researchbriefings.files.parliament.uk/documents/CDP-2023-0152/CDP-2023-0152.pdf

Sadou, A. & E. Njoya (2023). 'Applications of Artificial Intelligence in the Air Transport Industry: A Bibliometric and Systematic Literature Review' in *Journal of Aerospace Technology and Management* 15(1):1-24.

Sankaran, V. (2023). 'Hollywood AI backlash: What striking writers and actors fear about tech replacing role – Concerns emerges over AI proposal that could allow studios scans of actors in perpetuity'. Independent 14 July 2023, https://www.independent.co.uk/arts-entertainment/tv/news/why-are-actors-and-writers-on-strike-b2376397.html

Santander (2022). 'Everything you need to know about voice assistants' https://www.santander.com/en/stories/everything-you-need-to-know-about-voice-assistants

Sharif, A., Gurbuz, E. & S. Ay (2023). 'The impact of AI on employment and jobs: A comprehensive analysis' [Online] 10th London International Conference, 173-176. https://www.researchgate.net/publication/377347810_The_impact_of_AI_on_employment_and_jobs_A_comprehensive_analysis

Shuett, J. (2019). 'A Legal Definition of AI' at SSRN Electronic Journal. https://www.researchgate.net/publication/336198524_A_Legal_Definition_of_AI

Stahl, B.C. (2021). 'Perspectives on Artificial Intelligence' in Artificial Intelligence for a Better Future. SpringerBriefs in Research and Innovation Governance. Springer, Cham. https://doi.org/10.1007/978-3-030-69978-9_2

Szabadföldi, I. (2021). 'Artificial Intelligence in Military Applications-Opportunities and Challenges' in *Land Forces Academic Review* 26(2):157-165.

Shanghai Enterprise Service Cloud (2022). "Shangai Regulations on promoting the Development of Artificial Intelligence Industry". https://www.sidley.com/-/media/resource-pages/ai-monitor/laws-and-regulations/20220922-shanghai-regulations-on-promoting-the-development-of-artificial-intelligence-industry.pdf?la=en

Tapalova, O. & N. Zhiyenbayeva (2022). 'Artificial Intelligence in Education: AIEd for personalised Learning Pathways' in *Electronic Journal of e-Learning* 20(5). DOI**:** https://doi.org/10.34190/ejel.20.5.2597

The White House (2023). 'Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence' https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

The White House (2024). 'Memorandum for the heads of executive departments and agencies'. https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf

Ting-Chia, H., Hsiu-Ling, H., Gwo-Jen, H. & C. Mu-Sheng (2023). 'Effects of Incorporating an Expert Decision-Making Mechanism into Chatbots on Students' Achievement Enjoyment, and Anxiety' in *Educational Technology & Society* 26(1):218-231

Tobin, J. (2023). 'Artificial Intelligence: Development, risks and regulation'. https://lordslibrary.parliament.uk/artificial-intelligence-development-risks-and-regulation

UK Parliament (2024). 'Calls for views on Cybersecurity of AI'. https://data.parliament.uk/DepositedPapers/Files/DEP2024-0504/Annex_A_-_Call_for_Views_on_the_Cyber_Security_of_AI__1_.pdf

Vainionpää, F., Väyrynen, K., Lanamäki, A. & A. Bhandari (2023). 'A Review of Challenges and Criticisms of the European Intelligence Act (AIA)'. Conference Paper: Forty-Second International Conference on Information Systems, at Hyderabad, India [Online]. https://www.researchgate.net/publication/374845942_A_Review_of_Challenges_and_Criticisms_of_the_European_Artificial_Intelligence_Act_AIA

Walter, Y. (2024). 'Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation-A contemporary overview and analysis of socioeconomic consequences' in *Discover Artificial Intelligence*, 4(1 Publication 14.

Wintour, P. (2024). 'Pope calls on G7 Leaders to ban use of autonomous weapons' https://www.theguardian.com/world/article/2024/jun/14/pope-tells-g7-leaders-ai-can-be-a-both-terrifying-and-fascinating-tool#:~:text=Pope%20Francis%20has%20made%20a,of%20autonomous%20weapons%20in%20war

Wubineh, B.Z., Deriba, F.G. & M.M. Woldeyohannis (2024). 'Exploring the opportunities and challenges of implementing artificial intelligence in healthcare: A systematic literature review' in *Urologic Oncology: Seminars an Original Investigations* 42(3):48-56.

Yang, C. & C. Huang (2023). 'Natural Language Processing (NLP) in Aviation Safety: Systematic Review of Research and Outlook into the Future' in *Aerospace 10* (7):600. https://doi.org/10.3390/aerospace10070600

Yang, J. & B. Zhang (2019). 'Artificial intelligence in intelligent tutoring robot: A systematic review and design guidelines' in *Applied Sciences* 9(10):2078. https://doi.org/10.3390/app9102078