An analysis of the international and European Union legal instruments for holding artificial intelligence accountable

LLM Candidate **Thupane J. KGOALE**[1]
Professor **Kola O. ODEKU**[2]

Abstract

Despite being applauded as a great technological breakthrough of the current century, Artificial Intelligence (AI) technology and its operations keep attracting condemnations because of the failure by most countries to regulate and hold AI accountable. This assertion is made against the backdrop that mostly, AI perform functions and activities just like human beings, as such, AI is prone to make mistakes which might even negatively impact human beings and violate human rights. Mistake calls for accountability. This paper accentuates that even if there are no clear provisions in some country's statute books, there are existing international and European Union legal instruments for regulating and holding AI accountable should it erred. Methodologically, using literature review research approach, this paper highlights and discusses selected but salient international and European legal instruments which have direct and indirect impacts on AI, especially pertaining to regulation, liability and accountability.

Keywords*: artificial intelligence systems, regulations, liability, international legal instruments, European Union laws.*

JEL Classification: *K30, K33, K38*

DOI: 10.24818/TBJ/2023/13/3.06

1. Introduction

All over the world, countries are integrating and deploying AI in all sectors to perform different roles usually perfumed by human beings such as part of law enforcement, criminal justice, national security and provision of other private and public services.[3] While AI assist in service delivery there are concerns about how to hold it accountable for its omission or commission.[4] Algorithms are key as they are used in forecasting and analysing large quantities of data to assess the risks and predict future trends.[5] The data in question may relate to crime hot spots, social media posts, communication data and the provision of social services amongst

[1] Thupane J. Kgoale - Faculty of Management and Law, School of Law, Department of Public and Environmental Law, University of Limpopo, South Africa, 9243834@keyaka.ul.ac.za.
[2] Kola O. Odeku - Faculty of Management and Law, School of Law, Department of Public and Environmental Law, University of Limpopo, South Africa, kolawole.odeku@ul.ac.za.
[3] Baker, D. J., & Robinson, P. H. (Eds.). (2020). *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge.
[4] Calo, R. (2017). Artificial intelligence policy: a primer and roadmap. *UCDL Rev.*, *51*, p. 399.
[5] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), p. 160.

others. To complement states, corporate companies are at the forefront of manufacturing and producing a chunk of AI which in turn is sold to public authorities and individuals.[6] As a critical economic actor, countries are obligated to shape and develop policy and legislative instrument on how AI are produced and deployed in order to mitigate harms and damages arising from production, marketing, deployment and use of AI. Part of this includes requiring responsible business conduct and exercise of robust due diligence. A robust due diligence exercise entails overseeing the development and deployment of AI by assessing their risks and accuracy before they are brought to the market. Equally important is that developers, programmers, operators, marketers, and users of AI within the value chain are expected to be transparent about the details and impact of AI at their disposal. There is need to inform the public and affected individuals about how AI arrived at a particular decision autonomously. This would also include notification to individuals about the usage of personal data.[7]

It is against this backdrop that this paper discusses specific international and European legal instruments which have direct and indirect impacts on AI. This includes both binding and non-binding legal instruments. Specific human rights regimes vulnerable to AI disruptions are also identified and examined as they may be affected by corporate governance decision making processes. An evaluation of the legal implications of AI is conducted with reference to selected legal sources in the international and European Union. To understand the impact and challenges posed by AI. It is also important to examine some of the critical fundamental rights sacrosanct to the basic livelihood of humanity.[8]

According to the European Union report, AI systems are fast-evolving family of technologies that can bring a wide range of economic and societal benefits across the entire spectrum of political, social-economic value chain.[9] The systems are regarded as instrumental in terms of improving prediction, optimising operations and resource allocation. The use of AI plays a critical role in supporting socio-economic spinoffs in improving the welfare of the people.[10] This said, regulation and accountability are also imperative for the deployment and use of AI.

---

[6] Muro, M., Maxim, R., & Whiton, J. (2019). Automation and artificial intelligence: How machines are affecting people and places.

[7] Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review*, *81*(5), pp. 825-836.

[8] Završnik, A. (2020, March). Criminal justice, artificial intelligence systems, and human rights. In *ERA Forum*, Vol. 20, No. 4, pp. 567-583. Berlin/Heidelberg: Springer Berlin Heidelberg.

[9] To this extent, on 21 April 2021 the European Union Parliament passed the Artificial Intelligence Act and Proposals for the Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (herein referred to as the Artificial Intelligence Act) and further amending certain Union legislative acts.

[10] Novelli, C., Bongiovanni, G., & Sartor, G. (2022). A conceptual framework for legal personality and its application to AI. *Jurisprudence*, *13*(2), pp. 194-219.

2. International legal instruments on AI

If the international community did not respond appropriately to nascent technologies during successive eras of industrial revolutions, the situation could have been more devastating to humanity.[11] Similarly, failure by the international community would have also rendered some international laws and treaties irrelevant, due to failure to understand the intricacies and complexities of the new technologies. In practical terms, a free reign to self-develop would imply abdicating international legal obligations to multi-national companies and technological innovations as they wished.

To a large extent, international law derives its existence from domestic legal rules informed by international custom, *jus cogens* as well as the creation of treaties.[12] These international norms and rules come into being because of various factors such as political, military, socio-economic and demographic factors amongst others. A combination of these factors plays critical role in the creation of international law. In general, these factors must be more forceful and compelling to warrant the international community to develop internationally acceptable legal norms.

While there are no specific international legal instruments regulating AI, there are various sections of the Universal Declaration of Human Rights 1948 (UDHR) providing solid base in addressing diverse societal concerns that have been raised around AI. The provisions include the right to equal protection in Article 2 and the concerns on the right to life and personal security provided for in Article 3. Similarly, concerns around privacy due to the deployment of AI surveillance and algorithmic content moderation can be addressed in Article 12, while threats to freedom of expression is catered for in Article 19. The unjust treatment and displacement of human workers as well as the adequate standard of living following deployment of AI finds protection in Articles 23 and 25 respectively.

While domestic law is amended from time to time, international law changes over time. This has always been the case with the emergence of the 1st, 2nd and 3rd Industrial Revolutions. It is therefore not surprising that the 4th Industrial Revolution (41R) has emerged with unprecedented advanced technological innovations one of which is the AI.

Following the 1995 European Union Data Protection Directive, the European Union adopted General Data Protection Regulation (GDPR) in 2016 as a primary instrument regulating challenges brought about by data collection and technological and socioeconomic reforms. These regulations are also underpinned by principles that guarantee fundamental rights and ensure people have some forms of control over their personal data. The GDPR binds all member states and all public institutions and companies operating within the EU jurisdiction. However, the regulations and rules apply if the processing of personal data is involved. The

[11] Stearns, P. N. (2020). *The industrial revolution in world history*. Routledge.

[12] Weatherall, T. (2015). *Jus cogens: international law and social contract*. Cambridge University Press.

exception is when such data is used for prevention, detection, or investigation purposes in offenses that are inherently criminal.[13] Regarding cross-border usage of personal data, the GDPR requires that such transfer should only take place if the transaction is consistent with EU privacy laws.

In 2020, the Court of Justice of the European Union (CJEU) handed down a ruling in favour of an Austrian lawyer and privacy activist (Maximilian Schrems) declaring invalid the US-EU Privacy Shield Agreement, in a judgment popularly known as *Schrems II*. The Agreement in question relates to the transfer and commercialization of personal data from the European Economic Community to the US in compliance with data protection laws on both sides of the ocean.[14] The dispute, in this case, emanates from the fact that a subscriber to the social media platform, Facebook, is required to enter into a contract with its parent company before they are admitted to the platform.[15] Mr. Schrems has been subscribing to Facebook since its inception in 2008. The contract in question makes it possible for the transfer of all or some of the personal data of any person within the EU to Facebook servers that are located at its headquarters in the US, where further processing also takes place. In light of this, Mr. Schrems lodged an application with the Commissioner demanding the prohibition of transfers of his personal data to the US amongst others. He argued that the US law and practice do not provide for adequate protection against surveillance activities in line with the provisions of Article 3 (2) of Directive 95/46 issued under the GDPR.[16] The court noted that while the US have several security laws, these laws have shortcomings thus providing no adequate protection to data subjects. The court found that the decisions of the Ombud established in terms of the Privacy Shield Agreement are not binding on the US intelligence services. Against this backdrop, the court ruled that communication of personal data to a third party, the US in this case, constitutes an interference with privacy rights as provided for in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[17] The court further held that the retention and access to such personal data and its usage by the public authorities also interfere with these rights, regardless of whether the information is sensitive or inconvenient to the data subject. Against this backdrop, the European Commission has now moved swiftly to develop and introduce a concrete legal framework as part of the proposal for the regulation of AI

[13] Tupay, P. K., Ebers, M., Juksaar, J., & Kohv, K. (2021). Is European Data Protection Toxic for Innovative AI? An Estonia Perspective. *Juridica Int'l*, *30*, 99.

[14] *Maximillian Schrems v Data Protection Commissioner*) 21 July 2000, the European Commission's Decision 2000/520/EC of 26 July 2020) in October 2020. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems | European Data Protection Board (europa.eu) (15 September 2023).

[15] Ibid 50.

[16] Ibid 52.

[17] Ibid 171. Articles 7 and 8 of the Charter empowers the Commission to ensure that a particular level of protection afforded, known as adequacy decision, in accordance with the European Union. In practical terms, Article 7 of the Charter states that "everyone has the right to respect for his or her private and family life, home and communications. Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her."

in 2020. This culminated with the introduction of the European Union Act on Artificial Intelligence in 2021. The Act provides for the regulations and harmonization rules on AI through mandatory requirements and prohibitory measures within the Union jurisdiction.[18] Amongst others, the regulations clearly define AI, identifies associated risks and compliance measures, and further sets out monitoring and enforcement mechanisms.

Similarly, the relevant instrument in terms of police and security operations, the EU has adopted a Law Enforcement Directive (Directive (EU) 2016/68021), which establishes a comprehensive system of personal data protection for biometric matching, identification and authentication of persons of interest. This is mainly used in cases of terrorism, migration e sectorial EU instruments governing large-scale EU information systems in the field of migration and security.[19] Biometric data is defined as in the EU Directive as the:[20] "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy [fingerprint] data."

The EU data protection law recognizes physical and physiological characteristics as biometric data. The physical characteristics relate to facial features, fingerprints, retina, and iris of the eye, while physiological ones include personality traits, actions, deeply ingrained habits, and addictions amongst others.[21] One of the dire consequences of biometric data collection, through AI, is that it would disadvantage vulnerable groups such as children and elder persons, in that their facial and physical appearance changes with age from time to time.[22] This has the potential to disadvantage these social groups when it comes to access and benefits to public and private services.

3. Holding AI and operators accountable

This aspect looks at some selected aspects of regulations for holding AI and corporate companies and other business entities accountable. Usually, the courts and other regulatory bodies have judicial responsibilities to adjudicate and consider whether there is a violation or a breach of law arising from the deployment and use of AI which will make it liable and accountable.

[18] Regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 2021 COM (2021) 206.

[19] Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

[20] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 as amended by Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89 (Law Enforcement Directive), OJ L 119, 4.5.2016, pp. 89-131.

[21] Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

[22] Walters, R., & Novak, M. (2021). Artificial Intelligence and Law. In *Cyber Security, Artificial Intelligence, Data Protection & the Law*. Singapore: Springer Singapore, pp. 39-69.

3.1 Protection of the right to life and security

The deployment and use of AI may result in breach of both negative and positive obligations relating to the right to life and security, especially in areas of criminal justice system, environmental pollution, and health amongst others.[23] At the centres of production, manufacturing and deployment of these systems are corporate private enterprises with governments playing a limited role. In most cases, public authorities and corporate companies procure these technologies from the private vendors, systems developers and suppliers. By using data analytics and design choices to code policy choices, engineers at these vendors plays a critical role in influencing decisions in both the corporate world and public sector. In a way, governments have literally abdicated its decision-making responsibilities to private entities. It means that unmandated and unelected officials and entities can influence decisions of the public authorities.

While AI provides support for enjoyment of life and related rights, conversely it can also have an adverse effect on these rights.[24] This support can be in the form of diagnosis and treatment of medical conditions. In the medical practice, AI is used to carry out medical procedures and surgery and possibility exist that the technology-equipment and devices may be faulty or even malfunction in the process, thus posing a threat to the right to life, liberty and security of a person. An example of this would relate to medical diagnosis in radiology which uses image analysis systems for mammogram. In a research carried out by Zhou et al., (2021) a generative adversarial network (deep learning models) model was used to modify or fake images that would detect breast cancer.[25] After the modified images were analysed by AI and radiologists, the adversarial samples analysed by AI gave a wrong diagnosis at 69% while images analysed by radiologists identified between 29%-71%.[26] This means that that a wrong cancer diagnosis may result in a wrong prescription for medication and ultimately resulting in serious risks to the right to life and health. The right to life and security of a person is one of the fundamental rights provided for in Article 9 of the International Convention on Civil and Political Rights. The Article provides everyone has the right to life, liberty, and security and that no one shall be subjected to arbitrary arrest, detention, or sentenced to death. The Convention is clear that the right to life is inherent to a human being and as such, no one shall be arbitrarily deprived of this right contrary to the procedure established by law. While some countries still impose death sentences, the Convention asserts that such sentences can only be imposed in exceptional circumstances and following applicable law in force and should not be contrary to the provisions laid out in Article 6.

---

[23] Bajgar, O., & Horenovsky, J. (2023). Negative Human Rights as a Basis for Long-term AI Safety and Regulation. *Journal of Artificial Intelligence Research*, *76*, 1043-1075.

[24] Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial intelligence & human rights: Opportunities & risks. *Berkman Klein Center Research Publication*, (2018-6).

[25] Zhou, Q., Zuley, M., Guo, Y., Yang, L., Nair, B., Vargo, A. & Wu, S. (2021). A machine and human reader study on AI diagnosis model safety under attacks of adversarial images. *Nature communications*, *12*(1), 7281.

[26] Zhou et al., 6.

The mere fact that one's online personal data can be accessed at a whim by authorities for any reason poses a threat to the right to life and personal security. State agents can easily use this to deal with detractors currently or in the not-so-distant future. However, the courts in the EU have been reluctant to grant standing, especially in cases involving data breaches.

3.2 The right to equality and protection from discrimination

The right to equality is rooted in century-old struggles against slavery, colonialism, and racism which have spanned from the Stone Age up until now. Algorithmic discrimination and racial bias have been documented as we enter the transition from the 3IR to the 4IR driven by the deployment of AI. The mannerism of data collection and their orientations remain a fertile ground posing a threat to this right. In all circumstances, discrimination risks must be prevented and mitigated with special attention for groups that have an increased risk of their rights being disproportionately impacted by AI. These includes women, children, older people, racial and minority groupings, and members of the LGBTI community amongst others. Member states must refrain from using AI that discriminates or leads to discriminatory outcomes. Within their jurisdictions, they should protect individuals from the consequences of the use of such AI by the third party.

Equality as a right is guaranteed in Article 9 of the UN Charter on Human Rights. The right to equality is an inalienable right guaranteed in many regional and national instruments in different jurisdictions. In determining criminal charges under any law, a person is entitled to a fair and public hearing by an independent and impartial tribunal without any biases and prejudice. To this end, Article 2(1) of the International Covenant on Civil and Political Rights prohibits discrimination of any form expressly and provides thus:[27] Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or another opinion, national or social origin, property, birth or another status.

In the EU, equality rights and protection from discrimination are protected under Article 14 of the European Convention on Human Rights (ECHR) and accompanying Protocol 2. The provisions are aimed at prohibiting categorizations of AI systems based on new differentiations that may give rise to discriminatory stereotypes.[28] Article 4(1) of the newly adopted EU Employment Equality Directive provides for differential treatment on discrimination-relevant grounds such as sex. This is on the proviso that such treatment shall not constitute discrimination and further be able to meet occupational requirements that are legitimate, justifiable, and proportionate. This is problematic because it throws into open what discrimination

[27] The International Covenant on Civil and Political Rights was adopted by the UN General Assembly in December 1966.

[28] Council of Europe (2020) Preventing discrimination caused by the use of artificial intelligence. https://ennhri.org/about-nhris/human-rights-based-approach/. (20 June 2022).

means in this context. This is because the link between activity, context, and personal trait is factual as they include normative assumptions about appropriateness and reasonableness.

In grappling with a similar matter relating to recruitment in churches, the European Court of Justice restricted this kind of approach.[29] The court decided that a genuine, legitimate, and justified occupational requirement is necessary and resonates with the provisions in Article 4(2). The court further ruled that the occupational requirement justifications should comply with the principle of proportionality, guided by the nature of the occupational activity as well as moral and ethical consideration of the religious institution concerned.[30] In practical terms, this means that religious institutions cannot be allowed to reject job applicants suspected of having divergent religious beliefs.

3.3 The presumption of innocent and fair trial rights

Increasingly, while various levels of public authorities deploy AI to administer the criminal justice systems for efficiency and effectiveness, elements of bias within these systems are concerning.[31] These AI systems are mostly acquired and procured from private vendors. There have been admissions that the databases and algorithm collected and fed into the AI systems reinforces and entrench bias within the criminal justice systems as opposed to its elimination.[32] It is for these reasons that an accused person may challenge the usage and outcomes of AI used in investigative processes of alleged crime. Critical to this is the possibility of the accused in inspecting and testing the computational components and accuracy of algorithm underpinning the AI. Through defence counsel, the accused must be able to challenge, and review raise questions relating to reliability and accuracy of these systems, included embedded bias. The defence team should be entitled to have access to observe and inspect how the black box and source codes arrived at the emergent results to resulted in negative findings against the accused, especially taking into account its opaque nature. According to Reyes (2022), those concerned with access to information about AI systems in order to assist in a proper defence emphasize that due process requires transparency, including a notice and the opportunity to challenge.[33]

---

[29] The European Court of Justice (case C-414/16 as of 17 April 2018). http://www.europeanrights.eu/public/commenti/BRONZINI14-CONTRIBUTO_GORI_NEWSLETTER_DICEMBRE-11_-_Charter_-_Vera_Egenberger_-_Gori.pdf. (21 June 2022).

[30] Ibid.

[31] Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review*, *81*(5), 825-836.

[32] Bagaric, M., Svilar, J., Bull, M., Hunter, D., & Stobbs, N. (2022). The solution to the pervasive bias and discrimination in the criminal justice system: transparent and fair artificial intelligence. *Am. Crim. L. Rev.*, *59*, 95.

[33] Reyes, C. (2022). Emerging Technology's Language Wars: Smart Contracts.

In resolving AI problems threatening fair trial rights in the criminal justice systems, issues of accountability, transparency and fairness must be prioritized and attended to. For this reason, it should be obligatory for creators and producers of AI systems to ensure biased data is not used in order to comply with fairness requirements.

The availability and unfettered access to personal data by corporate companies especially on social media platforms may be used by law enforcement agencies in the future and this is likely to influence prosecutorial and judicial decisions by the courts.[34] The deployment of machine learning tools is susceptible to harnessing and identifying a person's language and behaviour as having a risk propensity to commit certain crimes. As a result, the deployment of AI may have dire implications on the right to be presumed innocent as provided for in Article 14 of the ICCPR.

The increasing usage of risk-scoring software based on AI has been proven to be interfering with the right to personal liberty. This software is used to inform decisions around detention and bail applications in criminal matters.[35] It has been proven that this has resulted in more suspects of African origin being falsely categorized and labelled as high risk with the possibility of ordering stringent bail conditions or receiving longer prison terms if convicted by the courts.

Where predictive policing software is used, potential risks exist that guilt can be wrongly imputed to persons as a result of built-in police biases based on previous data. The possibility exists that such inbuild biases may emanate from the moment an AI device is manufactured and produced because the device itself learns from the sociological make-up of the person who inputted the algorithm and coding. In the US and UK, there have been reports to the effect that some judges rely heavily on software results without a clear understanding of the risk-scoring system works.[36] It is therefore clear that court decisions arrived at based on risk-scoring systems by the software are inherently unfair. To a particular extent, it also shows that the judiciary has capitulated its judicial powers to private vendors and engineers who even lack the titles to prosecute court cases.

A study conducted by the European Court of Human Rights has revealed that, on average, there is accurate prediction of 75% of violation of nine articles of the European Convention on Human Rights.[37] This is not surprising since Article 8 of the European Union Charter on Fundamental Rights recognize the potential for AI to create and reinforce bias and provides that: "Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed

---

[34] Lageson, S. E. (2020). *Digital punishment: Privacy, stigma, and the harms of data-driven criminal justice*. Oxford University Press.

[35] Jackson, M. C. (2021). Artificial Intelligence & Algorithmic Bias: The Issues With Technology Reflecting History & Humans. *J. Bus. & Tech. L., 16*, 299.

[36] The software is AI-powered and produced by tech companies, most of which are owned by conservative companies.

[37] Masha Medvedeva, Michel Vols and Martijn Wieling, Judicial Decisions of the European Court of Human Rights: Looking into the Crystal Ball (A Paper delivered at a Conference on Empirical Legal Studies in Europe, 31 May-1 June 2018). (19 June 2022).

fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by the law."

It is possible that in future, it may be difficult to plead self-defence especially in cases of car accidents at robot intersections. This could be the case because of the inability of AI to deal with the question of nuances. Is it acceptable and justifiable in law to jump a traffic light sign red robot to evade an imminent accident and save a life? While a law enforcement official on duty witnessing the incident may be understanding and not issue a ticket, an AI-powered robot may act on this and issue a traffic violation ticket on the spot. Arguably, it can be concluded that there is a potential risk that the loss of nuances by AI-powered tools in situations like this could have far-reaching implications where extenuating circumstances exist.

3.4 Freedom of movement and usage of surveillance tools

The continued development and deployment of information and communication technologies to generate evidence have equally resulted in the generation of new forms of crime.[38] These forms of technology have been embedded with AI to enhance and support law enforcement agencies in the fight against crime through prevention, detection, investigations, prosecution, and enforcement. As a result, close-circuit televisions (CCTV) are prominently placed in strategic centres in smart cities to assist in this regard. However, evidence obtained from devices requires care to ensure its authenticity and integrity remain intact as it may be easily manipulated, modified, deleted, or even overwritten to conceal evidence.

In some instances, this may result in a deepfake where AI is used to superimpose images or videos of a person onto the body of someone else to create a digital lookalike. The proliferation of deepfakes has presented challenges to the courts in assessing the authenticity of such images. While an independent expert may verify such evidence, it could still leave doubts on interested parties thus prolonging proceedings before the courts. Deepfake manifests itself in acts that encroach on privacy rights, harassment, defamation cases, and intellectual property laws.[39]

Article 12 of the ICCPR provides for the freedom of movement and the right to choose own residence, provided it is necessary to safeguard national security, public order, and public health. These rights cannot be arbitrarily deprived. Amongst others, the use of surveillance tools based on AI involves combining data from satellite images through facial recognition cameras and cell phones, the Live Facial Recognition Technology. This provides detailed information about a person's movement and in the process predicts future movements.

It is possible that GPS mapping will be installed and extended to communities that are not currently covered around the world as part of predictive policing in smart cities and along the highways. In this regard, an automated decision

[38] Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Journal of Police Studies*, *20*(3), 17-40.

[39] Delfino, R. A. (2020). Pornographic deepfakes: the case for federal criminalization of revenge porn's next tragic act. *Actual Probs. Econ. & L.*, 105.

can be made that one is a flight risk in a travel list in real-time. This would prove to be an impairment of the freedom of movement and other connected rights such as tourism amongst others despite legitimate intentions for public safety and security. In *R v. Chief Constable of Wales Police*, the accused alleged that facial recognition technology was used to monitor him on two occasions. This resulted in the violation of his freedoms and privacy rights in contravention of Article 8 of the European Convention on Human Rights.[40] The provision of the Article requires that such facial recognition technology must be used in consistent with the law. The technology in question uses biometrics and other unique biological data obtained from a database of pictures collected indiscriminately in various ways. The technology was used as a pilot project to identify wanted and suspected persons in large crowds. In this case, a decision of the lower court was overturned by the Court of Appeal, which ruled that the deployment of these tools contravened EU law relating to privacy. The court found that the technology used violated the right to privacy and freedom of movement guaranteed in Article 8, which requires the interference to be in accordance with the law.

Similarly, freedom of movement and data privacy can be curtailed even in the workplace. In this regard, the critical question to ask is whether employers can monitor employees when they work from home. Following the imposition of a state of disaster in the wake of Covid-19 pandemic, numerous employers deployed Integral Ad Science (IAS) to monitor employees' productivity working from home. Depending on the AI embedded on the app, monitoring can be conducted in various forms such as the opening of emails; checking online behaviour such as time spent on work-related apps; tracking websites visited; taking screenshots of what was typed on those websites; physical location tracking and, even, webcam surveillance and taking photos of employees whilst they are working. Depending on the legislative framework obtaining in a particular jurisdiction, the legality of employee monitoring using AI is debatable. While it may be accepted under a particular jurisdiction, it is bound to be subject to particular safeguards such as prior notice which may be provided for in another jurisdiction. Yet, even if those safeguards are met, the practice of working from home was never envisaged. Under the circumstances, broader questions of human rights law would then come into the picture. The fundamental question being whether the monitoring can be regarded as a justifiable limitation of employees' reasonable expectation of privacy while working within the confines of their homes.

In the most recent case, a Dutch District court dealt with a matter where an employee was dismissed for refusing to comply with the employer's instruction to leave the webcam on the camera throughout working hours.[41] A US-based software

[40] *R (on the application of Edward Bridges) v Chief Constable of South Wales Police (Respondent) and Secretary of State for the Home Department and the Information Commissioner, the Surveillance Camera Commissioner, and the Police and Crime Commissioner for South Wales (Interested Parties)* [2020] EWCA Civ 1058.

[41] ECLI:NL:RBZWB:2022:5656 - District Court Zeeland-West-Brabant, 28-09-2022/10072897 AZ VERZ 22-61, Rechtbank Zeeland-West-Brabant 28 September 2022, ECLI:NL:RBZWB:2022:5656 (18 June 2022).

development company, Chetu Inc[42], employed a telemarketer in the Netherlands and demanded that for the first 90 days of employment, the employee was required to log on, share screen, and leave his computer screen on. However, the company insisted this to continue even after the completion of the probation period by the employee. In court, the employee argued that the flighting of webcam throughout the working hours make it uncomfortable and this violates privacy rights. The employee further argued that the company already uses share screening function on the laptop to monitor work performance. The employer argued that by doing that, the employee refused to work, and as such this amounted to insubordination. The court found that the dismissal was invalid due to insufficient refusal to work. It also found that the instruction to have the webcam all working hours violated the employee's right to respect for private life and as such unreasonable. The court observed that video surveillance of employees, both covert and overt, is subject to strict conditions and is regarded as a considerable intrusion of employee's private life resulting in the violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The court held that: "any interference with this right may only be justified if it is in accordance with the law, pursues one or more of the legitimate aims to which that provision refers and is necessary in a democratic society in order to achieve any such aim."[43]

The court further asserted that while, in principle, the fundamental right enshrined in Article 8 directly applies between states and citizens, it can also be applied vertically in a private-law employment relationship under certain circumstances.[44] These circumstances may relate to when a state does not sufficiently offer protection of a fundamental right in question. For these reasons, it ruled that the employee must be reinstated and compensated for lost salary and other benefits due to the employee. In addition, the court imposed a fine on the company in question.[45]

That as it may, as indicated above various concerns have been raised on the opacity of most of these AI systems. The concerns are based on the fact that prediction models used by AI systems have demonstrated that these neutral systems are susceptible to replicate biases. These biases are inherent in the data and codes they are trained on thus mimicking the psychological and mental disposition of a person who fed algorithm databases. Therefore, corporate companies and other service providers involved in producing and trading these AI systems would have to be held accountable, jointly and severally guided by existing legislative framework.

[42] Chetu, Inc.V ko Gaming, Inc., 261 So. 3d 605 (2019) January. District Court of Appeal of Florida. No.4D18 – 1551. Chetu, Inc. v. KO Gaming, Inc., 261 So. 3d 605 (2019) | Caselaw Access Project. (28 June 2022).
[43] Article 8(2) of the Convention.
[44] Chetu Incorporated 4.7.
[45] Ibid 4.2.

4. Conclusion

The usage and deployment of AI are bound to dominate every aspect of life as the world tithers on the cusp of the 4IR. The international community is faced with two choices, to legislate or let self-regulation take its course. Equally, both routes have their advantages and disadvantages. Given its propensity to harm while bringing in incentives for the benefit of humanity, a careful approach to legislating it seems to be the option the international community needs to consider. In today's world, a mere click on a technological device may sound more like signing away all your entitlements. If not managed well, data collection methods and mechanisms require an urgent careful approach. Most of the global data for AI takes place in the developed world given their proximity and access to technological aid. Because algorithmic data for AI is sentient and susceptible to subliminal biases, it becomes imperative that the international community intervene urgently and regulate. Failure to act accordingly, may as well result in reversing significant progress made especially in terms of human rights as well as development of humanity. An apparent lack of transparency and accountability by regulatory regimes on intellectual property does not augur well in a world facing a transition to an era dominated by technology and artificially intelligent. It is hoped that the developing world would not face the same situation as when the vaccine for coronavirus was developed and distributed. The development, production, and distribution of AI technologies must be underpinned by principles of accessibility, explainability, openness, and transparency if multi-national corporates are to be held accountable.[46]

Bibliography

1. Bagaric, M., Svilar, J., Bull, M., Hunter, D., & Stobbs, N. (2022). The solution to the pervasive bias and discrimination in the criminal justice system: transparent and fair artificial intelligence. *Am. Crim. L. Rev.*, *59*, 95.
2. Bajgar, O., & Horenovsky, J. (2023). Negative Human Rights as a Basis for Long-term AI Safety and Regulation. *Journal of Artificial Intelligence Research*, *76*, 1043-1075.
3. Baker, D. J., & Robinson, P. H. (Eds.). (2020). *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge.
4. Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review*, *81*(5), 825-836.
5. Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Journal of Police Studies*, *20*(3), 17-40.
6. Calo, R. (2017). Artificial intelligence policy: a primer and roadmap. *UCDL Rev.*, *51*, 399.
7. Delfino, R. A. (2020). Pornographic deepfakes: the case for federal criminalization of revenge porn's next tragic act. *Actual Probs. Econ. & L.*, 105.

[46] Storey, Veda & Lukyanenko, Roman & Parsons, Jeffrey & Maass, Wolfgang. (2022). Explainable AI: Opening the Black Box or Pandora's Box Communications.

8. Jackson, M. C. (2021). Artificial Intelligence & Algorithmic Bias: The Issues With Technology Reflecting History & Humans. *J. Bus. & Tech. L.*, *16*, 299.
9. Lageson, S. E. (2020). *Digital punishment: Privacy, stigma, and the harms of data-driven criminal justice*. Oxford University Press.
10. Muro, M., Maxim, R., & Whiton, J. (2019). Automation and artificial intelligence: How machines are affecting people and places.
11. Novelli, C., Bongiovanni, G., & Sartor, G. (2022). A conceptual framework for legal personality and its application to AI. *Jurisprudence*, *13*(2), 194-219.
12. Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial intelligence & human rights: Opportunities & risks. *Berkman Klein Center Research Publication*, (2018-6).
13. Reyes, C. (2022). Emerging Technology's Language Wars: Smart Contracts.
14. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), 160.
15. Stearns, P. N. (2020). *The industrial revolution in world history*. Routledge.
16. Storey, Veda & Lukyanenko, Roman & Parsons, Jeffrey & Maass, Wolfgang. (2022). Explainable AI: Opening the Black Box or Pandora's Box Communications.
17. Tupay, P. K., Ebers, M., Juksaar, J., & Kohv, K. (2021). Is European Data Protection Toxic for Innovative AI? An Estonia Perspective. *Juridica Int'l*, *30*, 99.
18. Walters, R., & Novak, M. (2021). Artificial Intelligence and Law. In *Cyber Security, Artificial Intelligence, Data Protection & the Law* (pp. 39-69). Singapore: Springer Singapore.
19. Weatherall, T. (2015). *Jus cogens: international law and social contract*. Cambridge University Press.
20. Završnik, A. (2020, March). Criminal justice, artificial intelligence systems, and human rights. In *ERA Forum* (Vol. 20, No. 4, pp. 567-583). Berlin/Heidelberg: Springer Berlin Heidelberg.
21. Zhou, Q., Zuley, M., Guo, Y., Yang, L., Nair, B., Vargo, A. & Wu, S. (2021). A machine and human reader study on AI diagnosis model safety under attacks of adversarial images. *Nature communications*, *12*(1), 7281.