BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 1 (2022)
ISSN 2029-0454

Cite: *Baltic Journal of Law & Politics* 15:1 (2022): 281-304
DOI: 10.2478/bjlp-2022-00020

The effectiveness of traditional legal rules in addressing the legal responsibility for the actions resulting from artificial intelligence system

Leila bekouche

College of law, Ajman University, Ajman, United Arab Emirates, lawyer.leila@yahoo.com.

Received: December 5, 2021; reviews: 2; accepted: June 21, 2022.

Abstract

Artificial intelligence has become an influential part of life for people all over the world. With the age of technology, there is concern on whether the traditional legal can fairly deal with the legal ramification of automation. The key artificial intelligence issues that might prompt a legal response in society today are algorithmic transparency, infringement of data privacy, artificial intelligence bias, cyber security vulnerabilities, and the adverse impact of automation in the workplace. The research will focus on global jurisdictions that have widely implemented the use of artificial intelligence and available law concerning artificial intelligence. These jurisdictions include the People's Republic of China, the United States of America (both the federal and local governments), the United Arabs Emirates, and the European Union. Sources of data for the research journal articles and case law reports on artificial intelligence and the law. Information will be extracted from google scholar, lexis advance and Westlaw for journal articles and the case law reports will be obtained from Westlaw, LexisNexis, and case law data for the European Union. Besides the electronic database searches, a target website search will also be performed to assist in accessing grey literature that mostly will be composed of the different data protection and implementation of AI. A comprehensive examination and evaluation of the articles and judicial decisions will be conducted to determine their relevance in the study. Thereafter relevant material incorporated in the study will be arranged in a table for easier access and explanation of findings. An extensive review of the materials will be done to combine and summarize the

results included in the selected studies and journal articles. The researcher will then provide a conclusion on the research topic based on the evidence gained from the review.

Keywords

artificial intelligence and law, algorithmic transparency, infringement of data privacy, artificial intelligence bias, cyber security vulnerabilities, and the adverse impact of automation in the workplace.

1. Introduction

Artificial intelligence is the application of machine learning, deep learning, and computer algorithms to perform data processing on tasks and provide decisions that were previously performed by a human being. Artificial intelligence is widely implemented in various aspects of society including healthcare, military, finance, law enforcement, and production. The accuracy and efficiency of artificial intelligence have led to companies and government automating their processes. With the age of technology and artificial intelligence, there is concern on whether the traditional legal can fairly deal with the legal ramification of automation. This study conducts a systematic review to understand the effectiveness of the traditional legal system in dealing with the legal responsibility of artificial intelligence. Artificial intelligence has become an influential part of life for people all over the world. With the age of technology, there is concern on whether the traditional legal can fairly deal with the legal ramification of automation. The issues that prompt legal response in society include algorithmic transparency, infringement of data privacy, artificial intelligence bias, cyber security vulnerabilities, and the adverse impact of automation in the workplace. The research will focus on global jurisdictions that have widely implemented the use of artificial intelligence and available law concerning artificial intelligence. These jurisdictions include the People's Republic of China, the United States of America (both the federal and local governments), the United Arabs Emirates, and the European Union.

The legal implications arising from algorithmic transparency are based on the question of whether artificial intelligence algorithms widely applied in the public should be made transparent. The most widely used algorithms are those that determine credit scores and those that manage electronic health records. The major legal concerns arising from credit scoring algorithms are the accuracy and transparency of the algorithms as a result of their secrecy, the legal protection, and the implementation of discriminatory and scoring actions that are biased for consumers with the use of non-traditional behavioral data (Chopra, 2020). The major legal responsibilities arising from the use of Electronic Health Records are the extent to which medical professionals are liable to the negative risks of this artificial intelligence and the possible risks that may occur due to going against clinical decision support systems (Sittig & Singh, 2011). Cyber securities vulnerabilities arise with the usage of computers and the internet. The global

revolution which is an era of communication and information technologies has significantly increased the rate of cyber-crime (Choi et al., 2018). Cyber-crimes all over the world are made possible through the strength of internet security, organized criminals and hackers can bypass whatever form of security is implemented and easily access unauthorized information (Choi et al., 2018).

Privacy of personal information is a concern of people worldwide. The operation of artificial intelligence is highly dependent on personal information whether it is developing this information or using the existing data for decision-making processes (Boronow et al., 2020). This has led to increased concern among consumers about the information on their internet search histories, credit backgrounds, a location visited and their interest and the information collected is used. Artificial intelligence bias is also a major issue with possible legal ramifications. Bias is introduced in artificial intelligence algorithms during the development process before being tested and also through the data collecting process (Challen et al., 2019). Artificial intelligence bias and discrimination impact consumers in various ways including, access to credit, the hiring process, and law enforcement. The victims of these biases may be forced to find legal solutions for their concerns.

The research is a systematic review and will focus on analyzing data published in journal articles and case law from well-established databases. The articles will be obtained from the most used databases including Westlaw, Lexis Advance, and google scholar (Anteby et al., 2021). Information on case law from the various jurisdictions will be obtained from Westlaw, LexisNexis, and case law data for the European Union. The study will cover available materials from the People's Republic of China, the United States of America (both the federal and local governments), the United Arabs Emirates, and the European Union. A systematic review is technical research, therefore one of the major limitations associated with the review is the time allocation. Since reviews differ from one to another, the researcher has no objective way of determining the amount of time that will be allocated for the studies. It can be noted that not all judicial decisions are published, therefore the researcher will have to cross-reference materials from multiple databases which are both time-consuming and ambiguous (Graham & Hoffman, 2022).

2. Scoping Review and Research

Artificial intelligence is widely implemented in different aspects of society today. Therefore, they are concerned about how automation adversely affects society and the legal ramifications of the actions of artificial intelligence. Various research has been conducted to understand the adverse impacts of artificial intelligence and the available laws protecting citizens and consumers against artificial intelligence. This chapter provides a literature review of artificial intelligence issues which are algorithmic transparency (credit scores programs, traffic lights algorithms, and Electronic health records algorithms.), vulnerabilities

in cyber security, data privacy, artificial intelligence bias, and the adverse effect of automation in the workplaces. It then focuses on provides on available literature on legislation enacted to combat these issues in various jurisdictions globally. This jurisdiction includes the federal government and local states government in the United States, the European Union, China, Brazil, and United Arabs Emirates. Due to the novelty of artificial intelligence, very few jurisdictions have effectively managed to enact legislation that governs the utilization of artificial intelligence. Most regulations are still in the proposal stage or are pending in congress. Therefore, the legal system heavily relies upon on-court officials to correctly interpret traditional laws in dealing with artificial intelligence and therefore develop precedents for future proceedings.

2.1 Algorithmic Transparency

An algorithm refers to the set of steps that programs in computers follow to complete commands imputed by the user. These algorithms are used for the processing of data, automated reasoning, and the calculation of best possible decisions and there has become a significant part of everyday lives. The various legal implications arising from this part of artificial intelligence are based on the question of whether artificial intelligence algorithms widely applied to the public should be made transparent. Artificial intelligence algorithms that are widely used today include credit scores programs and management of patient medical data. The major legal concern on artificial intelligence is the lack of precedents (which is the basis of any legal system) on cases involving new technologies. It is therefore dependent on new laws enacted or the new regulations put in place by various government agencies, such as the Food and Drug Administration agency of the United States of America.

Credit scores have become a significant determinant for the financial status of consumers worldwide although it is not accessible to every consumer. To ensure accessibility of credit to all consumers credit score algorithms have been applied to determine the creditworthiness of consumers with no credit history or who have a thin credit file (Chopra, 2020). The major legal concerns arising from credit scoring algorithms are the accuracy and transparency of the algorithms as a result of their secrecy, the legal protection, and the implementation of discriminatory and scoring actions that are biased for consumers with the use of non-traditional behavioral data (Chopra, 2020). There is a need for consumers to understand their credit scores and also be charged favorable interest rates despite their originality (Chopra, 2020). There is also need for a federal legislation that prohibits the use of non-traditional behavioral data which is obtained from social media networks that penalize customers based on their cultural and social interactions (Chopra, 2020).

According to the UK Consumer Credit Regulation, lenders are required to assess creditworthiness through the assessment of risk and the affordability of loans to the customer. Credit affordability assessment ensures that customers are

not heavily indebted, they can pay off loans easily (King et al., 2020). Despite the positive efficiency of artificial intelligence, lenders have the power to prohibit fairness by exploiting the behavioral and cognitive limitations of borrowers. This can be achieved by targeting a specific consumer or profile consumers and offering unfavorable credit terms to the borrower during extremely vulnerable moments. Borrowers in these cases are manipulated into signing unfair contracts since the need for immediate cash is higher than the need to review lending costs (King et al., 2020). Based on these concerns there is a need for regulatory authorities to put in place systems that supervise credit lending firms and also develop laws that protect both parties in every contract. The current traditional laws mainly protect credit lending firms and not consumers. The law provided by the United Kingdom Consumer Credit Regulation states that lenders must treat customers fairly, act with due care, skill, and, diligence and ensure that the marketing is clear, fair, and not misleading (King et al., 2020). This, therefore, provides a very wide legal ground for any cases arising from artificial intelligence algorithms considering the little to no precedents.

Electronic health records are one of the major forms of artificial intelligence implemented in the healthcare systems and therefore have a great impact on all stakeholders that are involved. Patients check on their medical records on a routine basis to access their diagnoses on the doctors' or hospital websites (Harman et al., 2012). Legally the patients' records are viewed as the hospital's or doctor's asset while the patient owns the information in the recorded in the systems (Harman et al., 2012). The National Coordinator for Health Information technology defines a health record as life as opposed to this record being regarded as merely data collected and guarded. (Harman et al., 2012). Data integrity is a major concern in electronic health records which in turn shifts focus to algorithmic transparency. Data collected between systems can be manipulated both intentionally and unintentionally and this leads to a risk of errors in the documentation that is harmful to patients (Harman et al., 2012). The major legal responsibilities arising from the use of Electronic Health Records are the extent to which medical professionals are liable to the negative risks of this artificial intelligence and the possible risks that may occur due to going against clinical decision support systems (Sittig & Singh, 2011). The 'hold harmless' clause on various Electronic Health contracts has restrictions on the extent to which health care professionals report the limitations of the system. Therefore, professionals risk facing incriminating themselves when reporting such cases. The National Strategy for Monitoring Medical Products Safety a part of the Food and Drug Administration agency has required organizations to be transparent on issues concerning the current and potential risks of their products. (Sittig & Singh, 2011).

2.2 Cyber security vulnerabilities

Artificial intelligence is controlled and managed by computers. Therefore, computers are used in the daily lives of many people around the world. One of the

major concerns about computers is cybercrime which is referred to as illegal activities conducted with the information accessed from computers through illegal access (Humayun et al., 2020). The global revolution which is an era of communication and information technologies has significantly increased the rate of cyber-crime. Cyber-crimes all over the world are made possible through the strength of internet security, organized criminals and hackers can bypass whatever form of security is implemented and easily access unauthorized information (Humayun et al., 2020). In the United States, the federal government has not instituted laws to manage vulnerabilities in cyber security but left the responsibility of different states who have cyber security and data breach notification laws. Entities that conduct operations nationwide and worldwide, therefore, do not have clear cover for cyber-crime attacks (Cybersecurity and privacy laws directory (n.d.). The US Consumer Privacy Protection Act of 2017 was structured to provide security to all-important individual information, avoid and manage cases of identity theft, notify relevant stakeholders on an occurrence of unauthorized information access and provide law enforcement entities with necessary assistance in combating cybercrime (Cybersecurity and privacy laws directory (n.d.).This provision applies to entities that manage information for ten thousand or more citizens of the United States for any 12month period of operation. These entities interact with personally identifiable information through collection, usage, access, transmission, storage, and disposal (Cybersecurity and privacy laws directory (n.d.). Penalties for breach of this act are fines not exceeding five million US dollars unless the violation is found to be willful or intentional in which additional five million US dollars is imposed (Cybersecurity and privacy laws directory (n.d.).

In China, the government has laid out various laws that protect the people against cyber-crime. In 2017, the People's Republic of China enacted cyber security law which governs several aspects of any network. To implement this law, various measures have been conducted measures for cybersecurity review and The National Emergency Response Plan for Cybersecurity Incidents (Wang et al., 2021). The Cybersecurity law recognizes the graded cybersecurity protection as the primary system of the law that ensures network security in China. In 2021 China enacted another law that ensures that data is collected, stored, processed, used, supplied. transacted and disclosed in the most secure way possible. This law is referred to as the Data Security Law (Qi et al., 2018). This law provides relevant authorities with autonomy to decide what is classified as important data within their areas of jurisdiction as well as enact necessary steps in security measures to ensure data security (Qi et al., 2018). Government agencies including the National Development and Reform Commission and the Cyberspace Administration of China enrolled out the Administrative Provisions on the Security of Automobile Data which provides the definitions of the primary concepts that are related to data processing of automobiles and the clarification of the legal responsibilities of data processors for automobiles in addition to the required standards of processing relevant data and sensitive significant information that is deemed personal. (Qi et al., 2018). The

People's Congress of Shenzhen Municipal released a local regulation referred to as the Regulation Shenzhen Special Economic Zone on Data which provides rules on how data is processed, shared, opened, and utilized. Another law enacted in China is the Personal Information Protection Law released in 2021 that provides guidelines on how personal information is to be handled by phone applications developers and operators.

The United Kingdom has instituted laws that protect its citizen from the activities of organized criminals and hackers. It should be noted that country does have a comprehensive legal system for cyber security but rather the laws are distributed across various legislations. The various laws enacted to deal with cyber security includes the Data Protection Act 2019 and the Network and Information Systems Regulations 2018. The Data Protection Act of 2019 works with the General Data Protection Regulation enacted by the European Union in 2018. This law provides guidelines for requirements concerning the protection of personal information for immigration and national security. The Network and Information Systems Regulations 2018 imposes responsibilities on the essential service operators and the providers of digital services (Baumer et al., 2004). Essential service providers are entities that provide the economy with significant services such as healthcare and digital infrastructure (Barrett et al., 2015). Digital service providers are entities that provide online marketplaces, cloud computing services, online search engines (Barrett et al., 2015). This law requires the above-mentioned parties to have installed high-end and strong security measures that will protect the data and information stored against any attacks and vulnerabilities. It also aims to ensure that the service provided by these parties is not harmful to consumers due to the usage of compromised data.

The United Arabs Emirates has also established several laws that aim to protect its citizens against cyber laws. The major law is Article 21 of the UAE cybercrime laws which relates to the violation of privacy. Violation of privacy refers to the illegal recording, intercept, listening, transfer, and transmittance of video, audio, and visual communications (Baker & Beeton, 2020). The law stipulates punishment for any person who uses computers and technology to manipulate and compromise records and important data will face a jail term of one year or a fine of two hundred and fifty thousand to five hundred thousand United Arab Emirates Dirham. The government has also instituted regulations concerning cyber-crimes in banks. Any individual that illegally accesses credit card information or bank account details will be punished through imprisonment or fines (Younies & Na, 2020). The government will issue punishments by fining the offender One Hundred Thousand to Three Hundred Thousand United Arab Emirates Dirham or a minimum jail term of six months. If the offender successfully managed to steal money from the accounts or credit cards, they will be charged a fine of Two Hundred Thousand to One Million United Arab Emirates Dirham or a minimum jail term of one year. To curtail terrorism through cyber-crime, the government has increased penalties for individuals who run websites or incite terrorist groups by charging a fine of Two

Million to Four Million United Arab Emirates Dirham or a serve a jail term of ten to twenty-five years (Younies & Na, 2020).

2.3 Infringement of Privacy

Since the inception of computers and the wide adoption of artificial intelligence, the privacy of information is a major concern for people worldwide. There are various ways in which privacy can be breached which include surveillance, informed consent, and the infringement of data protection rights such as illegal access to personal data (Di Minin et al., 2021). There is a need for the government to develop measures that protect the privacy of individuals without negatively impacting the development and applications of artificial intelligence. The operation of artificial intelligence is highly dependent on personal information whether it is developing this information or using the existing data for decision-making processes. This has led to increased concern among consumers about the information on their internet search histories, credit backgrounds, a location visited and their interest and the information collected is used. According to a survey conducted by Genpact (a multinational professional services firm) in the United States of America, United Kingdom, and Australia, seventy-one percent of the survey participants clearly expressed that they are against the application of artificial intelligence if it misuses their privacy despite the satisfaction in customer experience (Di Minin et al., 2021). Sixty-three percent of the survey respondents expressed their concern about artificial intelligence controlling their lives unintentionally without their knowledge (Di Minin et al., 2021).

In the United States, no singular federal law has been enacted to cover data privacy but rather, the protection of consumers is based on various laws and regulations enforced by various agencies. The Federal Trade Commission provides regulations on the use of personal data for commercial entities and enforces laws on privacy. The Children's Online Privacy Protection Act provides privacy for the information of minors (Solove & Schwartz, 2021). The Health Insurance Portability and Accounting Act provides guidelines on the handling of patient information and the protection of patients' privacy. The Fair Credit Reporting Act provides regulations on how credit information is collected and used Various states in the country have also taken measures to protect consumer data and ensure privacy. The states include California, Colorado, New York, and Virginia. The California Consumer Privacy Act requires organizations to receive consent from their consumers by informing subjects on when and how data will be collected and used. Consumers are then allowed to either store the information or delete it (Solove & Schwartz, 2021). Virginia's Consumer Data Protection Act which stipulates that companies that use consumer personal information for more than 100,000 people or earn more than 50% of revenue from the sale of personal data ensure that consumers expressly give consent before their data is processed and allowed to opt-out before the data is sold to third parties. The Colorado Privacy Act gives consumers rights to opt-out ads targeted to them, the right to gain access to

personal data from the company, the right to delete the data collected, and the right to move the data from one company to another (Solove & Schwartz, 2021). All these laws come with exemptions that also fairly protect businesses.

In Europe, the most singular data privacy law is provided in the General Data Protection Regulation. The regulation provides for consent where consumers are allowed to expressly give consent before any form of data is collected (Hoofnagle et al., 2019). It also states the rights that consumers have for their privacy including the right to be expressly informed about how their data will be collected and used. Consumers have the right to obtain a copy of their data from the company. Consumers have the right to do corrections to the data collected. Consumers have a right to install restrictions on how their data is processed. Consumers also have express rights to delete data collected from company records,. The European Union is working on various laws aiming to complement the existing one and also accommodate the dynamic digital era. These potential laws include the E-privacy regulations which will aim to provide regulations on electronic communications to safeguard consumer private information. Electronic communications include WhatsApp, Facebook Messenger, and Skype. The act will allow the user to choose how cookies track the browser activities and consumers can also withdraw consent that was granted on previous browser activities. The artificial intelligence act will be enacted to regulate how the technology affects the personal lives of users (Jiang, 2021). The act would also ban Artificial intelligence systems that can provide biometric data on a real-time remote basis in spaces that are publicly accessible (Hoofnagle et al., 2019).

In the United Arab Emirates, the Data Protection law was enacted and is to be enforced in 2022. The law sets consent as the primary legal basis where lack of consent will be considered a violation of the law leading to charges (Blanke, 2022). The legislation excludes the data used in the provision of healthcare, processing of credit and banking information (Baker, 2021). Entities operating in the Dubai International Finance Centre and the Abu Dhabi Global Market have excluded the law since they have predetermined laws that protect the privacy of data used. It also provides limited room for transparency on the information that is required to be provided the data processing begins. Individuals have the right to access their data, correctly recorded information, move data from one company to another, delete the data recorded in the system. The law also allows the movement of personal data from the UAE to countries that have been approved by the United Arab Emirates' data office. These countries have signed data protection contracts with UAE (Baker, 2021).

2.4 Artificial intelligence bias

Artificial intelligence bias occurs in a situation where results produced by algorithms cannot apply to every person in the general public. Bias is introduced in artificial intelligence algorithms during the development process before being tested and also through the data collecting process (Challen et al., 2019). Bias is

introduced in the algorithms by the engineering team, in that the more homogenous the team the more chances the algorithm results will be biased (Nelson, 2019). Artificial intelligence bias and discrimination impact consumers in various ways including, access to credit, the hiring process, and law enforcement. Artificial intelligence has been widely applied in the financial services sector to determine credit scores for consumers. Algorithms process large amounts of data to arrive at a certain decision making, therefore the probability of arriving at results that are aimed at people of a certain race or gender is high, based on the structure of the software and information available. In the recruitment sector, artificial intelligence is widely used to process large amounts of data and arrive at the best possible candidate without the issues of human bias. It can be noted that recruitment bias is still high despite the use of artificial intelligence. In 2018, Amazon identified an artificial intelligence recruitment algorithm that was biased against the female gender. The algorithm was designed to choose potential employees by processing patterns of resumes submitted in the company for 10 years, the results showed that male candidates were preferred (Parikh et al., 2019). Artificial intelligence in law enforcement is highly racist, where data inputted and results are biased against people from particular races (O'Donnell, 2019). The information processing is used in determining parole and developing legislation, such bias raises concern among many people (O'Donnell, 2019).

The Illinois state legislature enacted an Artificial Intelligence Video Review Act which requires the potential employer to expressly inform potential employer on the role of artificial intelligence in processing video interviews information to determine applicant fitness for the position (De Stefano, 2019). In New York, it will be a requirement for potential employers to inform applicants of the role of artificial intelligence algorithms in the recruitment process (Tambe et al., 2019). In the state of Colorado, the law prevents insurers from introducing the external data of customers or implementing artificial intelligence algorithms with data from outside sources to its business operations in a way that lead to unfair discrimination based on race, ethnicity, religion, sexual orientation, and color. China has not developed a singular law aiming to combat artificial intelligence bias and discrimination. However, state councils and specific legislation have addressed the issue of discrimination including the labor laws and education law (Latonero, 2018). The civil code instituted in 2020 provides regulations on the use of artificial intelligence decision-making that will have an impact on the lives of data subjects. It provides an avenue for people affected by artificial intelligence to voice out complaints and the entities are required by the law to efficiently conduct investigations on the complaints.

The European Union has also drafted proposed laws under the artificial intelligence act proposal that provides regulations on the uses of artificial intelligence and prohibits some of the artificial intelligence that has proven to be dangerous to consumers (Stix, 2021). The regulation bans various artificial intelligence algorithms that have been proven to be biased against the age, physical or mental disabilities of its citizen. It also prohibits the use of artificial intelligence

to provide discriminate against its citizens through social scoring basis by public agencies (Sacher, 2021). The regulations require artificial intelligence algorithms to be resilient and free from errors, inconsistencies, and faults that can occur in the system *(Sacher, 2021)*. The General Data Protection Rules prohibit the use of artificial intelligence in making decisions that will have legal repercussions or significant impacts on data subjects. The law is applied in the areas of online recruiting processes and the development of credit scores (Zuiderveen Borgesius, 2020)The law states that consumers have the right to decline participation on issues that base their decision on artificial intelligence results such as profiling that has the possibility of causing legal ramifications (Zuiderveen Borgesius, 2020).

2.5 Adverse effects of artificial intelligence on workers

Artificial intelligence has affected the job market both positively and negatively. Adverse impacts of artificial intelligence on employment come with legal ramifications. The era of automation comes with requirements for training and more education programs that the current workforce lack and therefore might lead to layoffs. Reports record the possibility of a loss of thousands of jobs as a result of automation and the application of artificial intelligence. The use of emerging technologies allows companies to save costs and time while increasing production efficiently a justification for the replacement of human capital by machines. According to reports from Bloomberg, an IBM survey conducted showed that more than one hundred and twenty million workers will need to undergo training to secure their jobs, (De Stefano, 2019). The report was based on research conducted by MIT-IBM Watson Lab which examined the one hundred and seventy million job posts online from the year 2010 to 2017. According to a Brookings institution publication, the most affected workers by artificial intelligence will be elite, highly paid employees whose job description is based on assessing data, developing plans, providing solutions, and predicting incoming trends. Artificial intelligence algorithms are designed to perform data processing of this nature (De Stefano, 2019).

The United States federal government and local states are in the process of enacting laws that be able to regulate the use of artificial intelligence in the workplace. The state of Illinois has enacted legislation that protects employees in the workplace by regulating the level of automation by companies (Holzinger et al., 2020). The state of Alabama enacted legislation that formed the Alabama Council on Advanced Technology and Artificial Intelligence whose main responsibility is to conduct reviews and diligently advise the local government and all stakeholders on the proper use and implementation of artificial intelligence. This agency has the power to protect the rights of employees from the negative impacts of automation in the workplace. The existing traditional laws do not have an allowance for matters related to artificial intelligence, therefore the power is left to courts to determine how the law will interpret issues concerning employee rights and artificial intelligence. Traditional employment laws include the Title VII of the Civil Rights Acts and the Age Discrimination in Employment Act.

In Europe, the European Union developed a proposal of various regulation that protects the interest of all stakeholders involved with artificial intelligence including employees. Under the artificial Intelligence Act proposal, any artificial intelligence algorithm is not operating alone but should be overseen by a human being. This ensures that humans work with artificial intelligence and are not completely deemed obsolete with automation. The proposal provides strict regulation for artificial intelligence to manage the level of automation in the workplace. The proposal also requires parties interested in using artificial intelligence to expressly by drawing a written European Union declaration of conformity which will ensure that parties within the confines of the law are punished if they go against the law. Employees will be given ample notice before termination and will be well compensated against any economic losses from termination (Howell & Pringle, 2019).

The United Arab Emirates is yet to improve legislation on the protection of workers from the impact of artificial intelligence. Courts are then required to use traditional labor laws in solving disputes that may arise due to automation in the marketplace. The labor laws are set under the Federal Decree-Law No.33 of 2021 which provides regulations of labor relations in the private sector. This law outlines the rights of employees on issues of termination or changes in contracts (Employment laws and regulations in the private sector, 2022). The United Arabs Emirates also introduced new labor laws in 2022 where The law also provides an avenue for grievances where employees can freely point out their dissatisfaction without fear of job losses Khalaf and Alkobaisi (1999) Employers are required to provide reasonable notice before termination of a contract and are required to provide reasonable compensation to the employee according to the years of service with the entity.

3. Methodology

The research will conduct a systematic review of all available information on the effectiveness of traditional legal systems on the legal ramifications of artificial intelligence. The systematic review will focus on identifying available studies that have been published on the topic of research and the corresponding results from the conducted studies. The findings of the review depend on the type of data that has been considered relevant in the studies. The systematic review requires collected data to be complete, accurate, and accessible for any updates available in the future. Methods used on determining the data to be used should be transparent, free from bias and human error.

3.1 Identifying Research Questions

There are various works of literature and reports that explore issues in artificial intelligence that have legal consequences in society. Therefore, this stage will assist the researcher in identifying the necessary research questions and

thereafter the type of data to be collected. The novelty of artificial intelligence has raised concerns on what it means for the legal systems since the law applies to natural persons and not technology. The issues that prompt legal response includes algorithmic transparency, infringement of data privacy, artificial intelligence bias, cyber security vulnerabilities, and the adverse impact of automation in the workplace. The available research on this particular topic has been independent studies conducted by experts in law and information technology to provide new information on artificial intelligence and the law. Therefore, the research gap exists where there is little understanding of the court's interpretation of traditional laws regarding the legal responsibility of artificial intelligence. This review aims to fill the gap by providing a conclusive finding on all available data regarding the research questions. The study will be able to provide a clear picture of the true legal ramification of artificial intelligence and how effective traditional law is in addressing the above-mentioned issues.

3.2 Identifying Relevant studies

Relevant studies on the key terms of this systematic review will be obtained from the published journal articles and available case law from judicial decisions.

Journal articles

Journal articles are the most common source of data for systematic review. The research will focus on peer-reviewed journals where all the articles have been reviewed by experts in the field. Before publication, experts ensure that the information presented is true and the methods or research are the right ones used to obtain the results. Journals articles contain first information on new research and are easily accessed through various databases (LibGuides: How to find scholarly, peer-reviewed journal articles n.d) Journal articles for this research will be retrieved from specialized databases that produce high relevance search results. These websites include Westlaw, Lexis Advance, and Google Scholar (Mart, n.d.). The research will use a research database list from both public and university libraries.

Table 1. Journal articles Inclusion and exclusion criteria summary

Inclusion criteria	Exclusion criteria
Must be written in a formal language	Articles from the non-healthcare industry
Must be peer-reviewed	Articles with no mention of artificial intelligence
Must be published in well-known journals or author affiliated with an organization	
Must be from a legal industry	
Must be in the artificial intelligence field	

Case law

Case law refers to the decision of the court usually on special cases that will future used to make decisions on similar cases (Law, 2022). Case laws vary according to different jurisdictions. The research will review case law reports on court decisions concerning grievances related to artificial intelligence especially cases of algorithmic transparency, data privacy, cybercrime, artificial intelligence bias, and adverse impacts of automation in the workplace. Judicial proceedings and decisions are often easily understood and therefore can be applied in any systematic review.. It can be noted that not all judicial decisions are published, therefore the study will obtain reports from the following avenues. Since the study conducts a review of case law on various jurisdictions, information will be obtained from various databases that publish legal material from the United States of America both the federal and local law, the People's Republic of China, the United Arabs Emirates, and the European Union.

Case law from the United States with be obtained from the LexisNexis and Westlaw databases. These databases allow a researcher to search cases by topic and jurisdiction. The cases are often stated in summary that allows any researcher to understand the context even with a background in law. The abstract information allows the researcher to easily determine the relevance of the material to their research and determine whether it will be used or not. Case laws from the European Union will be obtained from the case law database. The researcher will gain access to judicial decisions of the Court of Justice of the European Union and the European Court of Human Rights. The data on the database allows the research to access material on various cases under this jurisdiction. Case laws from China will be obtained from the LexisNexis database and Westlaw library. Case laws from the United Arabs Emirates will be obtained from lexis middle east and Westlaw middle east. The most significant limitations of using this form of the data source in its inaccessibility to the general public and time-consuming due to many publications that the researcher will have to go through. It is important to not all court decisions will be used as future precedents, it therefore important to ensure that results and findings from the case law databases will be compared to other sources of data to establish the accuracy of the data collected. In this research, case law reports will be influential in determining how traditional law is interpreted in this era of technology.

Table 2. Summary for Inclusion and exclusion criteria for case law publications

Inclusion criteria	**Exclusion criteria**
Must be from well-known databases that as LexisNexis, Westlaw, case law database (European union)	Studies from the internet with no backing from well-known legal databases or judiciary websites.
Must be informal English language	
Must be about artificial intelligence Must be about the law and technology	

Systematic review process

Preliminary research will be conducted to identify the key articles and case law publications from selected databases and journals that are most relevant to the study. This will ensure that the idea is valid and avoid the instance of data duplication. The following figure summarizes the systematic review process for both journal articles and clinical study reports.

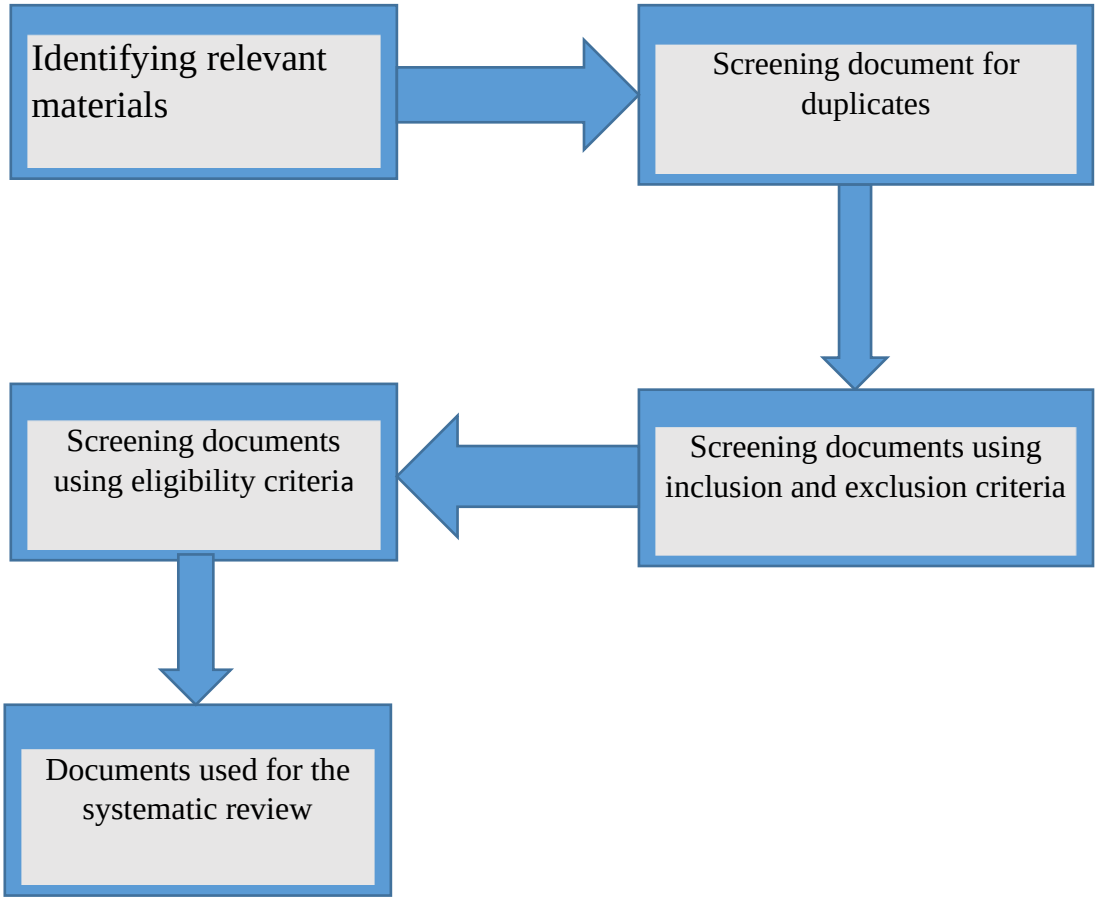

Figure 1: systematic review process

3.3 Study selection

Extensive research will be conducted on popular websites with key terms being artificial intelligence, algorithmic transparency, infringement of data privacy, artificial intelligence bias, cyber security vulnerabilities, and the adverse impact of automation in the workplace. The most used websites include Westlaw, lexis advance, and Google scholar (Mart, n.d.). The search will provide information on available studies on the topic to avoid duplication and any research gaps that need to be addressed. The figure below shows how websites will bring out relevant findings according to the keyed search topics. Therefore, the researcher should have been to check for the relevance of material before including it in the study (Mart, n.d.). Databases with a high percentage of relevance include Lexis Advance, Westlaw, and Google Scholar.

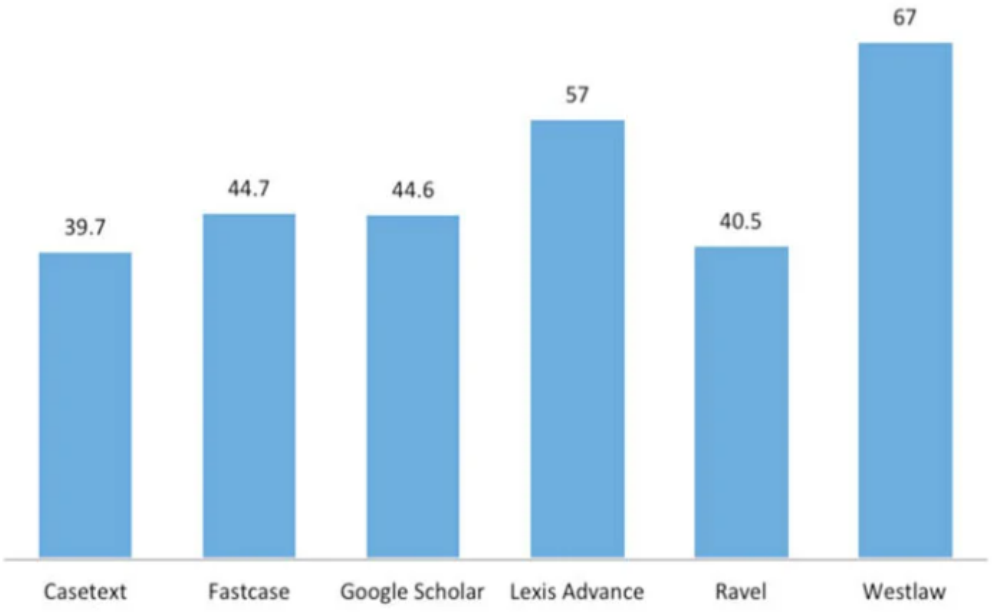

Figure 2. Percentage of results relevance per databases, (Mart, n.d.).

To access all relevant, the study will conduct unique searches on databases to get all available material**.** The search list will contain the following unique terms artificial intelligence\ artificial intelligence and law\algorithmic transparency and the law \the legal liabilities from infringement of data privacy \artificial intelligence bias and legal implications\ cybercrime and law\ adverse automation in the workplace and legal protection of workers. The search will cover materials from china, the United States of America, the United Arabs Emirates, and the European Union.

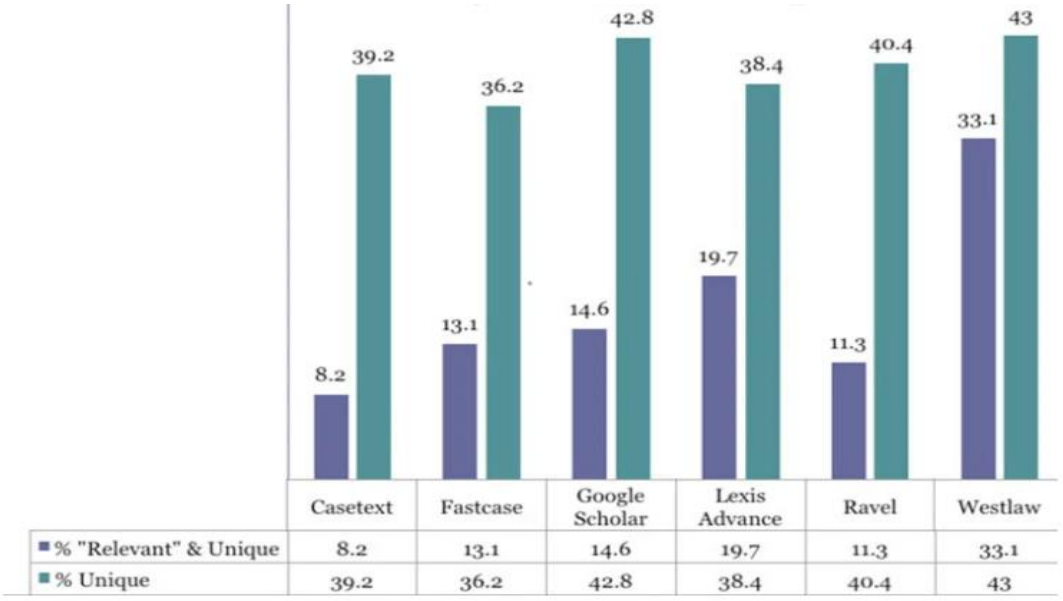

Figure 3. The percentage of relevant and unique search results on key websites (Mart, n.d.).

3.4 Charting the data

For a journal article or clinical study reports to be included in the research, they should pass both the inclusion and exclusion criteria (see table 1 and 2 above) as well as the eligibility criteria. The outcome of the journal articles or case law reports should be able to answer the research questions and provide adequate information. The research will aim to understand the effectiveness of the traditional law and legal responsibility of artificial intelligence in the following jurisdictions that is the Peoples Republic of China, the United States of America (both the federal and local state governments), the United Arabs Emirates, and the European Union.

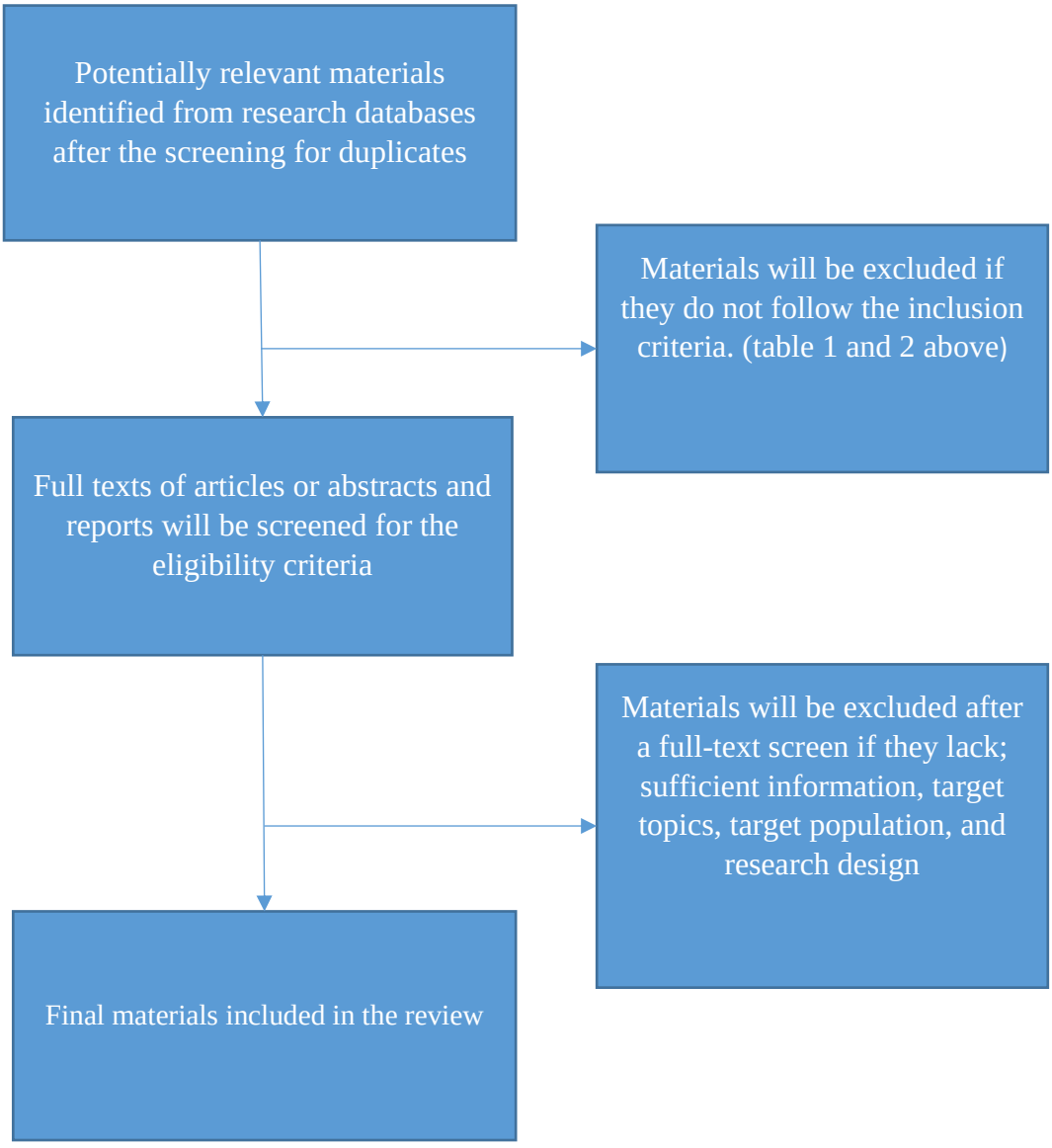

Figure 4. Eligibility criteria screening process

The relevant and unique outcomes of the search from selected databases and articles will be summarized in the table for easier understanding. The study will follow a diagramming approach similar to the account view (Tambe et al., 2019). The table to be filled is as follows.

Table 3: Proposed table for summarized information of reviewed studies or case law

No	Author\date\country jurisdiction	Title	Research problem\ legal complaint	Research model	Research method	Research Results\Judicial decisions
1	(Wilson-Aggarwal et al., 2019),United Kingdom	Law and Autonomous Systems Series: Algorithmic Credit Scoring and the Regulation of Consumer Credit Markets	Examining the rise of algorithmic credit scoring, and considers its implications for the regulation of consumer creditworthiness assessment and consumer credit markets more broadly.	Derived	Qualitative	Broad principles and conduct-based approach of UK consumer credit regulation provides the flexibility necessary for regulators and market participants to respond dynamically to these new technological risks.
2	(Zuiderveen Borgesius, 2020), Europe	Strengthening legal protection against discrimination by algorithms and artificial intelligence	Evaluating current legal protection in Europe against discriminatory algorithmic decisions	Experimental	Mixed	Non-discrimination law and data protection law are the most relevant legal instruments to fight illegal discrimination by algorithmic systems. If effectively enforced, both legal instruments can help to protect people.
3	(Chopra, 2020)/India	Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies	N/A	Derived	Qualitative	The current regulatory framework can better address discrimination by requiring lenders to disclose how they define "creditworthiness" so that consumers can gain a better understanding of the standards to which they are being held.
5	(Di Minin et al., 2021)UAE	The long-awaited Implementing Regulations to the New UAE Labour Law: 5 takeaways for UAE employers	Determining employment laws	N/A	N/A	N/A

6	(Challen et al., 2019), US	Legislation Related to Artificial Intelligence	Determining the impact of the use of AI or algorithms and the potential roles for policymakers.	Derived	N/A	N/A
7	(King et al., 2020), US	Electronic Health Records: Privacy, Confidentiality, and Security	Examining health information system in the past and present	N/A	N/A	N/A
8	(Humayun et al., 2020), US	Predictive policing algorithms are racist.	How predictive policing algorithms are biased and promoting racism	Derived	Mixed	The lack of transparency and biased predicting policing algorithms implies they are not fit for purpose. Thus, if they can't fix them, they should ditched.
9	(Howell & Pringle, 2019)	Shades of Authoritarianism and State–Labour Relations in China	Conceptualizing 'shades of authoritarianism' as a framework for better understanding the complexities and evolution of state–society relations in authoritarian states	Derived	Mixed	Authoritarianism in China tend towards a static focus on the state that is homogeneous across time.
10	(Baumer et al., 2004)	AI, machine learning and big data laws and regulations	How the Chinese government is actively embracing AI technology.	Observational	Qualitative	The Chinese recognize and acknowledge AI as key towards its future economic growth.
11	(Nelson, 2019)	Artificial Intelligence: Regulatory approaches in the UAE and abroad	Examining how UAE wants to regulate AI and the associated risks	Observational	Qualitative	There is the need to avoid blanket implementation of AI regulations due to its infancy and it's rapidly evolving nature.
12	(Chopra, 2020)	Credit denial in the age of AI	How AI alters the dynamics of credit denials and what policymakers and banking officials can do to safeguard consumer lending.	Derived	Qualitative	AI has the potential to alter credit practices in transformative ways and it is important to ensure that this happens in a safe and prudent manner

13	(Harman et al., 2012)	Use of AI in the Workplace Raises Legal Concerns	Examining the potential legal risks of using AI at workplace	Derived	Qualitative	If AI is not managed properly in organization, it may result in significant legal risks.
14	(Howell & Pringle, 2019)	UAE Publishes First Federal Data Protection Law	N/A	N/A	N/A	N/A
15	(Wilson-Aggarwal et al., 2019)	The role of bias in artificial intelligence	Reflecting on the algorithmic bias loopholes in the "so perfect" AI systems.	Derived	N/A	N/A
16	(Jiang, 2021)	Data privacy risks to consider when using AI	Examining the risks associated with new technology such as AI	Derived	N/A	New technology carries unexpected perils that corporate leaders should guard against to keep consumer, employee, and client data safe.
17	(Nelson, 2019)	Understanding Bias In AI-Enabled Hiring	Does AI really reduce hiring bias?	Experimental	Mixed	While in theory AI offers a more cost-effective, targeted and efficient hiring process by helping organizations sift through volumes of resumes, in reality, it may promote biased hiring because of its reliance on unconsciously prejudiced selection patterns like language and demography.
18	(Parikh et al., 2019)	Artificial Intelligence and Its Impact on Jobs	Examining the impact that AI has on jobs	Observational	Mixed	AI could lead to the loss of tens of millions of jobs
19	(Sittig & Singh, 2011)	Legal, ethical, and financial dilemmas in electronic health record adoption and use	Examining the unanswered legal, ethical, and financial questions threatening the widespread adoption and use of EHRs	Observational	Mixed	Identification of the problems and provision of solution helped in the effective and safe initiation of EHRs to assisting with transforming health care

20	(Younies & Na, 2020)	AI, machine learning and big data laws and regulations	Examining the potential legal implications that arise from use of AI in workplace and the legislative and regulatory response to the increased presence of AI in the workplace.	Derived	N/A	Employers need to be careful on their relationship with AI to ensure compliance with the existing body of employment laws that hinder the effective use of the technology.

3.5 Collating and Reporting

A comprehensive examination and evaluation of the articles and judicial decisions will be conducted to determine their relevance in the study. Thereafter relevant material incorporated in the study will be arranged in a table for easier access and explanation of findings. An extensive review of the materials will be done to combine and summarize the results included in the selected studies and journal articles. The researcher will then provide a conclusion on the research topic based on the evidence gained from the review.

4. Conclusion

The research will undertake a systematic review by using the published journal articles and clinical studies reports as the source of data. The key inclusion criteria for journal articles will be peer-reviewed articles and authors who are affiliated with the association. For the case studies, the key inclusion criteria are based on the legal proceedings that have been published on the case law database for European Union, LexisNexis database, and Westlaw. Data collection will be conducted by performing key search terms on Google Scholar, Lexis Advance, and Westlaw. Data analysis will be conducted by summarizing collected information on well-detailed tables and providing a conclusion based on the evidence from the review.

Reference

Anteby, R., Lillemoe, K. D., Fernández-Del Castillo, C., Ferrone, C. R., & Qadan, M. (2021). Analysis of in court malpractice litigation following pancreatic surgery. *Pancreatology, 21*(4), 819-823. https://doi.org/10.1016/j.pan.2021.02.017

Baker, L. (2021). Dubai International Financial Centre's Updated Data Protection Law, Part 2: Implementing a modern, global law in a UAE financial free zone. *Journal of Data Protection & Privacy, 4*(4), 362-371.

Baker, L., & Beeton, J. (2020). Dubai International Financial Centre's updated data protection law-Part 1: Developing a modern, global law in a UAE financial free zone. *Journal of Data Protection & Privacy, 3*(2), 161-171.

Barrett, M., Davidson, E., Prabhu, J., & Vargo, S. L. (2015). Service innovation in the digital age. *MIS quarterly, 39*(1), 135-154. https://doi.org/10.25300/MISQ/2015/39:1.03

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: a comparison between the United States and the European Union. *Computers & Security, 23*(5), 400-412. https://doi.org/10.1016/j.cose.2003.11.001

Blanke, G. (2022). The United Arab Emirates. *Yearbook of Islamic and Middle Eastern Law Online, 1*(aop), 1-24. https://doi.org/10.1163/22112987-12340015

Boronow, K. E., Perovich, L. J., Sweeney, L., Yoo, J. S., Rudel, R. A., Brown, P., & Brody, J. G. (2020). Privacy risks of sharing data from environmental health studies. *Environmental health perspectives, 128*(1), 017008. https://doi.org/10.1289/EHP4817

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., & Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias and clinical safety. *BMJ Quality & Safety, 28*(3), 231-237. https://doi.org/10.1136/bmjqs-2018-008370

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of information science, 44*(6), 752-767. https://doi.org/10.1177/0165551517748288

Chopra, S. (2020). Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies. *Vand. J. Ent. & Tech. L., 23*, 625.

De Stefano, V. (2019). 'Negotiating the algorithm': Automation, artificial intelligence and labour protection. *Artificial Intelligence and Labour Protection (May 16, 2018). Comparative Labor Law & Policy Journal, 41*(1).

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology, 35*(2), 437-446. https://doi.org/10.1111/cobi.13708

Graham, P., & Hoffman, J. (2022). *Introduction to political theory*. Routledge. https://doi.org/10.4324/9780429424106

Harman, L. B., Flite, C. A., & Bond, K. (2012). Electronic health records: privacy, confidentiality, and security. *AMA journal of ethics, 14*(9), 712-719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209

Holzinger, A., Goebel, R., Mengel, M., & Müller, H. (2020). *Artificial intelligence and machine learning for digital pathology: state-of-the-art and future challenges* (Vol. 12090). Springer Nature. https://doi.org/10.1007/978-3-030-50402-1

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law, 28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Howell, J., & Pringle, T. (2019). Shades of authoritarianism and state–labour relations in China. *British Journal of Industrial Relations, 57*(2), 223-246.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering, 45*(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2

Jiang, M. (2021). Cybersecurity policies in China. In *CyberBRICS* (pp. 183-226). Springer. https://doi.org/10.1186/s42400-021-00073-x

Khalaf, S., & Alkobaisi, S. (1999). Migrants' strategies of coping and patterns of accommodation in the oil-rich Gulf societies: evidence from the UAE. *British Journal of Middle Eastern Studies, 26*(2), 271-298. https://doi.org/10.1080/13530199908705686

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics, 26*(1), 89-120. https://doi.org/10.1007/s11948-018-00081-0

Latonero, M. (2018). Governing artificial intelligence: Upholding human rights & dignity. *Data & Society*, 1-37.

Law, H. (2022). Narrative coaching–Part 3: Approaches for groups, teams, organisations and community. *Coaching Practiced*, 397-413. https://doi.org/10.1002/9781119835714.ch42

Nelson, G. S. (2019). Bias in artificial intelligence. *North Carolina medical journal, 80*(4), 220-222. https://doi.org/10.18043/ncm.80.4.220

O'Donnell, R. M. (2019). Challenging racist predictive policing algorithms under the equal protection clause. *NYUL Rev., 94*, 544.

Parikh, R. B., Teeple, S., & Navathe, A. S. (2019). Addressing bias in artificial intelligence in health care. *Jama, 322*(24), 2377-2378. https://doi.org/10.1001/jama.2019.18058

Qi, A., Shao, G., & Zheng, W. (2018). Assessing China's cybersecurity law. *Computer law & security review, 34*(6), 1342-1354. https://doi.org/10.1016/j.clsr.2018.08.007

Sacher, M. (2021). Avoiding the inappropriate: The European Commission and sanctions under the stability and growth pact. *Politics and Governance, 9*(2), 163-172. https://doi.org/10.17645/pag.v9i2.3891

Sittig, D. F., & Singh, H. (2011). Legal, ethical, and financial dilemmas in electronic health record adoption and use. *Pediatrics, 127*(4), e1042-e1047. https://doi.org/10.1542/peds.2010-2184

Solove, D. J., & Schwartz, P. M. (2021). ALI data privacy: overview and black letter text. *UCLA L. Rev., 68*, 1252.

Stix, C. (2021). Actionable principles for artificial intelligence policy: three pathways. *Science and engineering ethics, 27*(1), 1-17. https://doi.org/10.1007/s11948-020-00277-3

Tambe, P., Cappelli, P., & Yakubovich, V. (2019). Artificial intelligence in human resources management: Challenges and a path forward. *California Management Review, 61*(4), 15-42. https://doi.org/10.1177/0008125619867910

Wang, D., Chen, K., & Wang, W. (2021). Demystifying the Vetting Process of Voice-controlled Skills on Markets. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 5*(3), 1-28. https://doi.org/10.1145/3478102

Wilson-Aggarwal, J. K., Ozella, L., Tizzoni, M., Cattuto, C., Swan, G. J. F., Moundai, T., . . . McDonald, R. A. (2019). High-resolution contact networks of free-ranging domestic dogs Canis familiaris and implications for transmission of infection. *PLoS neglected tropical diseases, 13*(7), e0007565. https://doi.org/10.1371/journal.pntd.0007565

Younies, H., & Na, T. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime, 27*(4), 1089-1105. https://doi.org/10.1108/JFC-04-2020-0055

Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights, 24*(10), 1572-1593. https://doi.org/10.1080/13642987.2020.1743976