NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3079-0603 PRINT ISSN: 3079-059X
Utu Journal (Utu J.)
Utu Journal of Legal Studies

Utu Journal *Original Article*

Artificial Intelligence and the Law: Legal Frameworks for Regulating AI and Ensuring Accountability

Jaafar Abd Al Hussain Kahdhim Al- Kemawee [1*]

[1] College of Art, Mansoura University, Mansoura, Egypt

***** Corresponding Author: Jaafar Abd Al Hussain Kahdhim Al- Kemawee, Email: jaafarabd19951995@gmail.com.

***Abstract*:** This essay explored the key opportunities, challenges, and ongoing responses to AI regulation, with a specific focus on the implications of AI for the law. AI relies on high volumes of data and large-scale computation to make decisions or predictions that would otherwise require human intelligence. The opportunities afforded by AI touch every sector, including law, where it can streamline tedious administrative tasks acting at scale to help prioritize cases, retrieve data, etc. in just seconds. In this context, the European Parliament is looking to prevent the emergence of a Wild West environment and is striving to ensure that AI use is ethical, protects fundamental rights, and respects the rule of law. However, existing laws have proven insufficient in effectively addressing the challenges posed by such technologies. The opportunities AI provides should be maximized whilst ensuring accountability and civil liability when AI systems cause damage. Thus, a two-pronged response is needed:

1. legal frameworks for the regulation of AI systems in the interest of fairness, safety, privacy, anti-discrimination, etc.; and
2. mechanisms to ensure that when AI systems cause damage, adequate civil liability systems are in place to redress victims.

The discussion was underpinned by empirical evidence from the literature that outlines and explains the problems posed by AI for the legal sector and the implications of the proposals advanced by the European Parliament. The extent to which empirical evidence goes beyond the legal sector was also examined.

Access this article online

***Keywords*:**
Artificial Intelligence, Explainability, GDPR, Transparency

1. Introduction to Artificial Intelligence and its Impact on Society

The term Artificial Intelligence (AI) is most commonly used to refer to computer systems that can perform tasks that are otherwise difficult for computers, or their programs, to undertake. Although AI systems undertake numerous tasks of great complexity and importance, the ways they function are poorly understood outside the domains in which they operate. Owing to the opaque and uninspected nature of the data-driven models that underpin these systems, the process by which these systems transform inputs into outputs - and hence their decisions - can be difficult to explain. These AI systems may also be viewed as "responsible" in that they have authority or accountability tied to their outputs (Belle, 2019). The scope of legal and ethical frameworks to shape AI implicates questions concerning the abilities, actions, and consequences of these systems and their social context. In this context, this report considers a characterization of AI

Received February 02, 2024; Revised March 01, 2024; Accepted March 10, 2024; Published June 30, 2024
https://doi.org/10.57238/ujls.s90hsa43

systems that is comprehensive enough to provide a foundation for understanding them. It explores AI and their repercussions for society broadly and the legal sector specifically, revealing an overwhelming commercial incentive to profit from their use.

Several different regulators, parliaments, committees, and other bodies are currently examining the possible dangers posed by AI systems. Emerging legislation and guidelines generally focus on wise planning, fairness, transparency, justness, and prudence in the pursuit of the AI technologies in question (Surden, 2019). In the absence of a proper understanding of the kind of systems involved, the kind of behaviors they exhibit or the choice of measures to adopt, there is concern over the viability of "regulation," either on an industry or political level. Given the inherent complexity and unpredictability of AI systems, it is surely naive to imagine that any set of operational or legal principles or guidelines will guarantee safety.

1.1 Definition and Scope of Artificial Intelligence

Artificial Intelligence and Law: An Overview Artificial Intelligence (AI) is a subset of computer science that focuses on creating systems that can perform tasks that would normally require human intelligence. Some common applications of AI include image and speech recognition, natural language understanding, robotics, and expert systems, which emulate the judgment and decision-making ability of a human expert. In the legal domain, there have been promising commercial efforts to apply AI to tasks such as e-discovery, legal research, document drafting, contract analysis, and even litigation strategy (Surden, 2019).

Most of today's AI technologies use one of a few approaches, such as "big data" statistical approaches (including "machine learning"), rules-based systems, or using AI to create AI. Many current AI approaches require problem areas that have underlying patterns or structures. These technologies often just give a first rough pass at many lawyerly tasks, providing, for example, a template document for an attorney. Humans are still squarely in the loop for complex, sophisticated legal tasks. AI is best understood as a family of technologies rather than as a single technology. Because there are many aspects to AI and many ways that AI can be deployed in society, it is important to develop a well-defined scope and terminology for understanding AI. This section develops definitional territory related to AI.

Responsible Artificial Intelligence: A Structured Literature Review AI will have an ever-increasing impact on our daily lives 3. AI should be viewed as a tool, not a system that has infinite control over everything. There needs to be a system that we can truly call 'responsible' AI. The elements of ethics, privacy, security and explainability are the true pillars of responsible AI, which should lead to a basis of trust. Responsible AI is an interdisciplinary and dynamic process: it goes beyond technology (procurement, development, operation, lifecycle management), but also includes laws with standards such as quality management systems, professional standards, ethics guidelines and the Sustainable Development Goals. If the technical and ethical side is satisfied the user trust is maintained.

1.2 Historical Development of AI

Artificial intelligence (AI) systems are increasingly leveraged to assist in the administration of law and decision-making activities where enforceable legal rules are applied. Such law-related AI systems raise a number of questions related to accountability: Who can be held accountable for the decision or recommendation made by the system? How can the system itself be rendered accountable? Such questions become crucial when the law-related AI system was developed or is operated using opaque machine-learning techniques (Belle, 2019).

The development of AI can be divided into three phases: the first period of early enthusiasm, which ran from 1945 to 1970 and is often called "The Golden Age"; the second period of disappointment, which ran from 1970 to 1987; and a third period of success, which began around 1988 and is ongoing (Surden, 2019). It is useful to trace the path AI has taken in order to see the current state of AI, and its potential opportunities and challenges in regard to the law. One technology enabler is the availability of powerful computers. Computers have become far more powerful, cheaper to buy and have shrunk so that today they are part of everyday life. Computer power also increased exponentially. This law-plus-AI combination has the potential to greatly improve the quality and efficiency of work in the legal field.

2. Challenges and Opportunities of AI in the Legal Sector

Lawyers spend too much time on document review, legal research, e-discovery, and other tasks that give low rates of return. It is low-hanging fruit for AI companies wanting to automate tedious work and displace lawyers. On the other hand, lawyers worry that AI systems in these realms still need more transparency/interpretability. They either ignore the AI's decision-making process or make it ultra-complex to achieve fairness and prevent discrimination. As a result, the crux of the advice seems to be this Hypertrophied Solomon, always enigmatic and wishing to navigate a legal minefield. What is the legal framework around the human-centric project mentioned above? At least in the UK, there are four different categories of tax and regulatory requirements for AI companies: protecting the algorithm, AI-related exemptions, AI-related surveys, and bias-identifying algorithms. General principles governing the protection of personal data and privacy:

1. the EU's General Data Protection Regulation.
2. The UK's Data Protection Act.

These latter provisions establish a principle-based legal framework that works universally and variably across jurisdictions, and harmonization within the EU. Various initiatives are underway to create sectoral rules and applications for AI systems. Such systems have a limited

dataset in legal research and require dozens if not hundreds of thousands of texts to train them.

AI can enhance legal research and analysis in multiple ways. Firstly, AI-powered tools can streamline online searches for case law and legal commentary, making information retrieval more efficient and effective. AI systems can analyze legal databases, extract relevant information, and present it in an accessible format for lawyers and paralegals (Dwivedi et al., 2021). Secondly, AI can support the drafting of legal documents by suggesting language, checking for compliance with regulations, and analyzing previous drafts' acceptability based on case law. Thirdly, AI can assist judges in searching for applicable norms within legal texts and determining a case's acceptance probability based on judges' previous decisions (Cai et al., 2018).

2.1 Automating Contract Review and Management

AI tools such LegalSifter, DoNotPay, and Evisort have been developed to automate the process of contract review, redline generation, and identification of key clauses. These tools can enhance the efficiency and accuracy of review/management by highlighting discrepancies with benchmark contracts, suggesting amendments, and flagging missing provisions. AI-assisted tools can also help corporations classify agreements and extract metadata, providing insights into company liabilities and obligations. Several major corporations use these AI tools to review/redline contracts and identify legal issues. However, these early adopters are often large companies with extensive legal departments and manpower to combat AI ineffectiveness (Trunk et al., 2020).

While AI tools offer considerable efficiencies and greater accuracy, there is still uncertainty and concern surrounding their use. Blind adoption of AI tools may result in regulatory questions and liability for errors (Messias et al., 2022). All accepted agreements must still be reviewed by a qualified lawyer, which will require envisioning a new work division between seasoned lawyers and AI tools. On the other hand, small corporations may find it difficult or impossible to turn a profit from such tools if they are not completely free to use. The wide-spread adoption of AI tools may inevitably become a necessity of practice with its inherent risks and considerations. In light of all these opportunities/challenges, the legal field is ideal for discussing issues concerning the regulation of AI.

3. Ethical and Social Implications of AI in the Legal Field

The legal field is not exempt from the rapid advancements in artificial intelligence (AI). Various stakeholders are incorporating AI systems into their daily activities, interested in their efficiency and cost-effectiveness. Law firms use AI for marketing and billing, as well as tools among their legal teams to automate the drafting of pleadings, contracts, and discovery requests. Courts use AI tools for decision making and, in some countries, as support in the sentencing phase. Public bodies use AI to undertake monitoring of all sorts of public interest and enforce compliance with laws, regulations rules (Smyrnova, 2021). All these uses of AI have potential social and ethical implications that have raised concerns, such as algorithmic discrimination related to the results produced by AI systems that can impact the fundamental rights of individuals.

Recently, various stakeholders proposed different regulatory initiatives to understand how AI systems are created, trained, and operated and on what bases their results are computed. The concern is about the impacts of such underlying factors on the results produced by AI systems, including fairness (such as non-discrimination) and the human context (such as interpretation of results). It also includes awareness of the level of granularity of the legal frameworks and any prohibitions establishing certain AI systems that should simply not exist due to their complex and risky nature. In this context of growing awareness about social risks and wrongs potentially related to the scaling up of AI, various stakeholders proposed different laws and regulations (Larsson, 2019). Current regulations rely on principles and keywords such as transparency or accountability but lack more specificity, such as the conditions under which an AI system is considered black box and subject to a certain level of scrutiny.

3.1 Bias and Discrimination in AI Algorithms

The increased utilization of Artificial Intelligence (AI) has a corresponding rise in ethical complexities, many of which are tied to existing and emerging legalities. The philosophical basis for AI regulations pursuant to legal frameworks can be approached through ethical dimensions concerning such complexities, with a specific investigation into anticipated hurdles and barriers to the implementation of regulations. Addressing pertinent ethical considerations of AI enables scrutiny of elements such as bias and discrimination, transparency, financial and economic conditions, privacy and civil liberties as shown in Fig. 1, comparability to human-made decisions, safety and security considerations, and others. Thereupon, proposed regulations are examined to observe how well the entities controlling AI address the challenges therein (Ferrer et al., 2021).

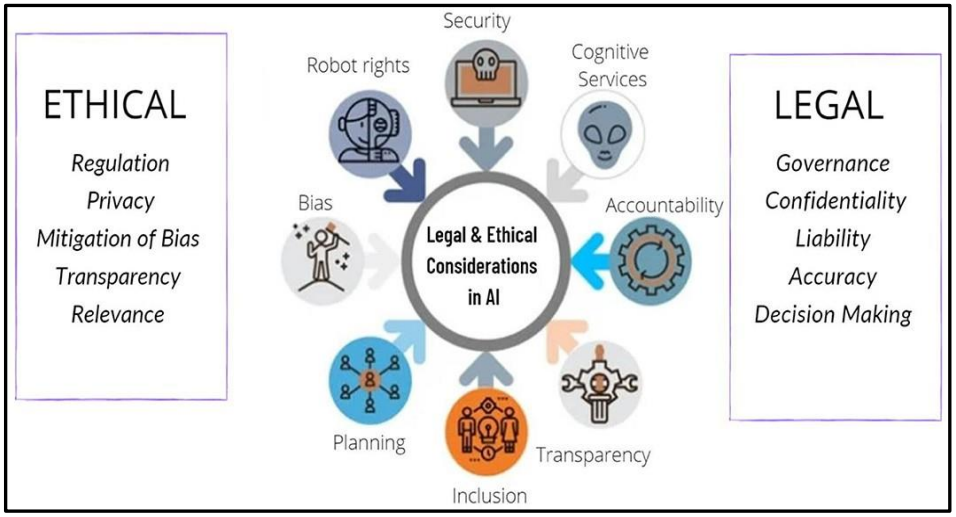

Figure 1. Legal and ethical consideration in AI

The complexities of AI algorithms stem from the nature of AI and the various ways of deploying AI outputs. AI algorithms are complex mathematical formulas and sequences constructed to fulfill distinct tasks pertinent to the processing and examination of data. At a basic level, a dataset is ingested by the algorithm, processed according to the mathematical sum operation, and an output is generated. This implies that several factors, such as the data inputted and the nature of the algorithm itself, directly impact the nature of the algorithm output (Wang et al., 2024). For instance, take a simple algorithm designed to analyze images and determining whether an image represents a pineapple or not.

Two dataset example outputs are most readily conceivable. In the first instance, the algorithm's dataset is filled with images of pineapples, other images depict sausages or plums, and in the end, the algorithm determines that what represents a pineapple does not exist in the image dataset. Now, if the dataset were far more inclusive, then perhaps the algorithm output would be interpreting at least some of the images of pineapples as images representing pineapples.

3.2 Privacy Concerns and Data Protection

The advancements of Artificial Intelligence (AI) technologies engender substantial implications across various sectors, including the legal field. This concurs with increasing concerns regarding the accessibility, transparency, bias, accountability, and ethical considerations of AI systems. Thus, balancing AI systems' opportunities and threats becomes fundamental. Though many critical implications of AI in the legal field arise, only a limited number are selected for further discussion. McCormick (2019), in his foundational work on AI and the law, engages with several implications, such as the expansion of the analytical capabilities of AI within legal theory and practice, limiting human discretion via law and AI, and the impact of AI systems and technologies on the legal environment. Nevertheless, from a legal perspective, additional and more contemporary implications emerge.

These implications coincide with and build on legal regulations to confront the challenges posed by digital technologies, including AI systems with legal information and systems (Radanliev et al., 2024). Therefore, with the advancements of AI systems, surrounding data privacy and protection becomes increasingly relevant. AI systems usually rely on personal data containing sensitive information; thus, individuals' privacy concerns solidify. Moreover, as AI systems often incorporate automated decisions, individuals would also like to monitor these algorithmic operations.

The legal framing of AI systems' implications concerns not only pure law regulations but also overlaps legal regulations and ethical ones. AI systems are designed to replicate human behavior, especially human judgment, such as reasoning. Therefore, AI systems could impact fairness notions; ensuring categories are reasonably captured, widely considered, and lawfully applied towards individuals. Attempting to restore fairness within human and societal operation is a crucial, though difficult, task of regulation.

4. Existing Legal Frameworks for AI Regulation

An overview of the current legal frameworks for regulating artificial intelligence (AI) is provided in this section. It highlights laws and treaties at the international level as well as relevant national legislation. Laws aiming to regulate AI on the basis of its potential risks are of particular interest. This overview serves as a foundation for understanding the legislation that is currently in place for regulating AI. AI regulating laws that are coherent and effective to protect the interests of humanity are desired. An understanding of the legal frameworks for regulating AI helps to develop such laws (Van Vliet et al., 2015).

At the level of international laws and treaties, AI is not specifically or directly regulated. Laws that could apply to AI are however in place, but primarily with other goals than regulating AI. At the national level, legislation that could regulate AI either directly or indirectly exists in multiple countries. For general risk-based regulation of emerging technologies, such as biotechnology and nanotechnology, laws have been adopted in the European Union (EU) and France. These laws could apply to block the future deployment of a high-risk AI technology as demonstrated here (Gervais, 2023).

4.1. National Legislation on AI

In early 2023, following a long period of debate, the European Commission published the Artificial Intelligence Act, which provides a comprehensive framework for regulating the technology regarding civil liability 14. The proposed approach is threefold. On the one hand, many would consider AI-generated decision making—such as surveillance, risk assessment, and recruiting—or court AI systems that inform judges about the probable outcomes of the case, inadmissible in court by analogy to the EU General Data Protection Regulation (GDPR) concerning taking automated decisions. On the other, AI systems that fall short of the Risk-by-Degree requirements should incur strict product liability. If regulation over strict product liability is unsuccessful, Member States should be encouraged by EU directives to foresee liability based on fault in the civil codes. AI risk-in-degrees evaluations determine the appropriate regulatory approach. High-risk systems should be regulated through steps, such as public scrutiny. AI machines operated via public decision-making or affecting fundamental rights on a significant scale should be under a procedure of prior approval (Díaz-Rodríguez et al., 2023).

Several countries are working on national legislation regarding AI. Facial recognition systems by the police under urban law should be prohibited. The four Guiding Principles for Civic Activism are that public debate guided by the principles of transparency, empathy, and patience, such as using historical examples of negative consequences where real threats to democracy ensued, should be promoted.

A broad coalition of social, civil, and expert stakeholders should be established to speak as one regarding the dangers of AI. Actively, the governments of Germany and the Netherlands participated in investments in AI research; continue investment in an adequate workforce (scientists) and education to sustainably build a responsible, ethical, and secure AI environment; establish boundaries for governmental AI use by prohibiting profiling without prior approval; and presume that AI systems impact fundamental rights or freedoms as default within the government context.

5. Key Principles for AI Regulation

Implementing AI systems raises challenges about transparency and accountability, as algorithms' "decisions" increasingly affect people without their knowledge. While "decision trees," "if–then" rules, and linear regression models are highly interpretable, employing complex models, such as neural networks, makes these decisions opaque. Explainability is understood as a broader umbrella term covering both transparency and interpretability concepts. Furthermore, several terminology discrepancies are present across disciplines, which need harmonization so that the discussion better converges (Larsson, 2019). AI has been increasingly embedded in decision-support systems; there are concerns about allocating responsibility and liability in the context of emerging AI capabilities. Without national and international agreements, there is a high risk of having the benefits of these technologies disproportionally accumulated by individuals and few countries. The objective is to ensure that the use of AI will not entail a concentration of power in the hands of a few, prolonging inequities and poverty.

The goal is also to ensure that using powerful algorithms will not become a "wild-wild-west," and that the regular legislation will be compatible with AI and not waver. Further, responsibility is one of the key conditions for promoting ethical execution (Doshi-Velez et al., 2017).

5.1. Transparency and Explainability

A number of institutions have produced AI guidelines that notably contain a call for transparency and explanation. Transparency is commonly understood as making the operation of AI systems public and interpretable. Transparency is intimately connected to accountability, as it is very difficult to hold actors or systems accountable for their actions if these actions are unknown and not public. Addressing the black-box problem in AI and Big data systems – ensuring that they behave in a predictable manner – is therefore a necessary precondition for assuring the fair and controllable use of these technologies, both by humans and machines.

Applied to distinguish between different forms or degrees of understanding regarding an AI model (Budhwar et al., 2023). Transparency refers to the degree to which an AI system can be inspected and understood. Higher transparency (to a human interrogator) implies that a model is more easily understood, or is clearer in revealing its structure, operations, and motivations. Common approaches to produce transparency are, for example, producing human-readable surrogate models for given black-box models, exposing formal mathematical properties of models, and exhibiting both the training dataset of a model and the training procedure itself as shown in Fig. 2.

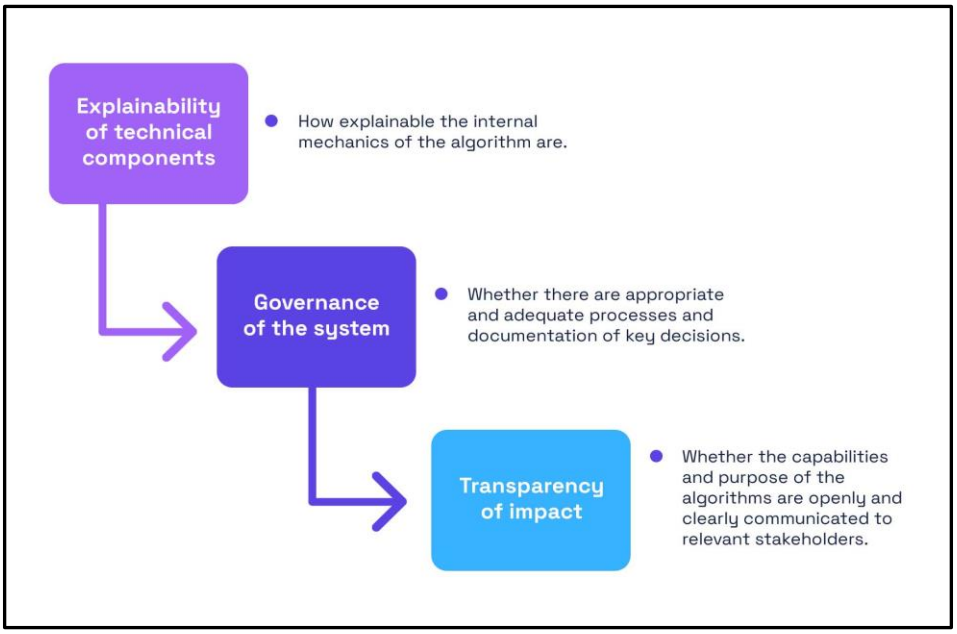

Figure 2. The relationship between transparency and explainability

Usually, the principle of transparency states something to the effect that AI systems should be developed in a way that makes them sufficiently understandable and interpretable. At the same time, AI systems are understood as massive and complex systems built from large collections of component algorithms or mechanisms, so that some AI systems can be considered to lack transparency at any reasonable definition of the concept. There is a pressing need to provide clear guidelines that can assist in ensuring transparency of algorithmic decision-making, epidemiological modelling, dynamic financial modelling, and the design and deployment of other AI systems.

Transparency and explainability have to be understood as relative concepts. There are many possible human interrogators, each coming with a different background in moral philosophy, economics, political theory, legal science, etc., and AI can deal with each background differently. This raises questions of the trained human interrogators. Misinterpretation of those questions can lead subsequently to uninterpretable answers and, ultimately, unfair accountability of the AI system. Regarding this issue, a number of institutions have produced AI guidelines that contain principles and recommendations explicitly addressing the black-box problem in AI systems and codifying what is known today regarding transparency and explainability in AI systems. It is clear that no AI system is fully transparent and explainable.

5.2 Accountability and Responsibility

Accountability and responsibility are key legal principles that should be applied to the law governing Artificial Intelligence (AI). To encourage the responsible design, development, and deployment of AI systems, there exists a critical need for well-defined lines of accountability and responsibility. The law governing each AI system should employ a clear definition of responsibility and establish an allocation of liability across all relevant actors. Responsibility refers to the act of being liable, answerable, or accountable for something within one's power, control, or management. Six principles have been identified, of which two are vital for the legal framework concerning AI: the assignment of responsibility and liability to stakeholders involved in the development and deployment of AI systems, and the mandate for the ongoing assessment of that responsibility and liability by all stakeholders post-deployment (Van Vliet et al., 2015).

The legal framework should cover both civil and criminal matters. A complementary legal regime covering civil responsibility, claim regulation, burden of proof adjustment, and punitive damages could bolster the legal framework. Responsibility in the civil dimension can only be effective if sanctions are defined and enacted. The cloned framework allows more agile application and adaptation of the legal regimes, which is especially important for fast-paced technological sectors such as AI. There should also be coordination between concerned regulatory institutions to ensure the integrity and effectiveness of the legal framework with regards to AI systems (Budhwar et al., 2023). Concerns regarding the impact of AI on human and environmental safety, privacy rights, civil rights, labor and employment rights, and monopolization should be addressed and factored into what AI systems are permitted.

6. Enforcement Mechanisms for AI Regulations

A concern for the next phase of this regulatory approach is how it is going to be enforced. This concern hinges on two successive questions that arise in the context of AI code

regulation. The first is what institutions/actors will be responsible for the primary enforcement of these AI Code rules? The second question is about the prior question's substantive aspect. If rules are enforced, what mechanisms will be available for compliance monitoring and reporting? Will there be penalties and sanctions for non-compliance? (Veale & Zuiderveen Borgesius, 2021). these two questions exploring the foundations for the implementation of the proposed regulatory approach will be elaborated upon and answered here.

With a view toward embodying accountability in MIL's discourse about AI regulation, the first necessary step is to consider how this regulatory approach could actually be implemented at the socio-technical level—that is, how human beings and organizations involved with AI machines would comply with it and how compliance would be monitored and enforced. The legality of those steps is a prerequisite before regulation and compliance go hand-in-hand. To this end, compliance with the law is transposed into different institutional processes or private governance mechanisms. For example, this transposition takes the form of corporate duties or contracts in the case of private actors. Such contracts include Terms of Use, which stipulate the engagement of the contracting party concerned to respect the law (Hacker, 2023).

6.1 Compliance Monitoring and Reporting

Focusing on compliance monitoring and reporting, this subsection examines how AI can be guaranteed to comply with requirements through mechanisms for overseeing adherence to AI regulatory requirements. It informs how AI regulations and their compliance monitoring can be practically operationalized in the legal domain and, hence, makes the full regulatory picture possible. Compliance monitoring addresses a central aspect of the functioning of regulations: The ability to check, and influence if needed, whether subjects of regulation related to AI comply with requirements. Compliance monitoring can be broadly defined as the performance of certain actions to ascertain or guarantee compliance (Hacker, 2023). Compliance monitoring generally relates to regulations, and statutory compliance monitoring usually relates to legal regulations. In the context of AI, compliance monitoring comes into play when there are requirements on AI systems or their development that are subject to monitoring to ensure adherence 8. Compliance monitoring is distinguishable from auditing, with compliance monitoring being broader than auditing. Compliance monitoring refers to mechanisms that can perform certain functions, while auditing is one of the potential means to perform compliance monitoring. Other means similarly include inspections, performance evaluations, and controls. Compliance monitoring is further distinguished from technical compliance, the latter term referring to the fit of an AI system with certain standards.

The concept of compliance monitoring is generally easy to grasp and does not require an exhaustive definition. Instead, it is accompanied by categories to assist in understanding. These categories are specified based on prior studies into (legal) compliance monitoring, conceptualization of regulatory approaches, and studies of monitoring techniques in diverse regulatory areas. Further, compliance reporting is part of compliance monitoring and is discussed in its relation to monitoring. It involves reporting on compliance in some way, generally on the behalf of the subject of the regulation. Compliance reporting can come in several forms depending on how reports are provided. According to its categories, the compliance monitoring of AI regulatory requirements can be structured into three components, each with its own subcategories and examples:

1. Coverage, such as oversight body types and compliance targets;
2. Means, such as monitoring techniques and digital tools; and
3. Independent expert involvement, such as the role of experts and resource aspects.

AI regulatory compliance monitoring needs to be designed on a certain level, for instance at an EU level. Key challenges are identified that are deemed to be particularly relevant and have potentially major influences on the prospects of compliance monitoring specifically in the AI context: The audience aspect of compliance monitoring, compliance monitoring of model-disseminating AI systems and indirect compliance monitoring through third parties, and the challenges of monitoring rapidly changing AI systems and organizational settings.

6.2 Penalties and Sanctions for Non-Compliance

Outside the scope of the application of the directive, a number of penalties and sanctions are envisioned in case of non-compliance, and possible appeals for recourse against these sanctions are described. Sanctions can be both administrative fines and corrective measures. In case corrective measures are not executed by the liable party within the agreed timeline, administrative fines may apply (Meszaros et al., 2022). Compliance is guaranteed by the involvement of market authorities, which have the obligation to ensure that these rules are complied with both in the EU and extra-EU cases or else a case can be brought up by the Commission. Personal liability of the natural persons who led the breach of obligations may also apply in certain cases.

Individual member states remain free to enforce additional provisions in their own legal systems. Current deterrent sanctions are a minimum sanction of 4% of the yearly global turnover for serious breaches, and a minimum violation of 2% of the yearly global turnover for less serious breaches. It is worth noting that with the definitions of AI system and operator, these penalties are additional compliance/defensing costs, unaffected by the number of claims or the damages done by the civilly liable party. This logic may not be suitable in case of errors that are unforeseeable by design choices made in good faith, or seem excessive in comparison to the punishment regime for

similar determinations (data losses, medication errors, etc.) Penalties are didactical and have an effect of deterrence on AI operators, whose market success and even operation can be threatened by a non-negligible sanction. However, AI operation is made by a combined effort of multiple actors, and there might be less consideration for the civilly liable party outside the tort system already matching these criteria.

7. Case Studies of AI Regulation in Practice

Real-world cases of AI regulation in practice are presented by looking at the General Data Protection Regulation (GDPR) adopted on April 14, 2016, by the European Union (EU) and the California Consumer Privacy Act (CCPA) signed into law on June 28, 2018. These regulations have introduced a number of new legal obligations for businesses powered by AI and automated decision-making systems. There has been a variety of interdisciplinary work from the fields of law, ethics, and computer science on addressing or assessing the implications of these regulations in the context of AI and automated decision-making systems. However, there has been limited work that integrates these research streams. Such integration is needed to help develop a comprehensive understanding of the regulations' implications on AI as well as to ensure compliant development of AI systems. The GDPR has many implications for AI and many of its provisions resonate with AI ethics proposals, especially the fairness, transparency, and accountability principles (Messias et al., 2022). The GDPR is the most comprehensive regulation that attempts to balance data subject protections and interests when personal data is processed by organizations and AI businesses (Goldman & Hudson, 2000). The CCPA is a state-level consumer privacy law in the US and is one of the first of such legislations in North America, adopted in part, in response to the Cambridge Analytical scandal involving incorrectly gained personal data of Facebook users employed to target voters in the US presidential election.

7.1 EU's General Data Protection Regulation (GDPR)

A prominent case study of AI regulation in the legal sphere is the General Data Protection Regulation (GDPR). Adopted in May 2016 (Regulation 679/2016), the GDPR established a unified approach to people's data privacy in the European Union (EU) and European Economic Area (EEA). The goal of the GDPR is "to protect natural persons with regard to the processing of personal data and on the free movement of such data" (Regulation 679/2016). In "AI Regulation: Lessons Learned from the GDPR" (2023), the effectiveness of the GDPR as an attempt to tackle the challenge of emerging technologies is unpacked. Particular emphasis is placed on its strengths and challenges. Conclusions provide insights that are valuable in thinking about how AI will be regulated in the future.

The adoption of the GDPR stands out as one of the most consequential responses to the rapid rise of new technologies. Such technologies fundamentally transformed the relationship between individuals and organizations concerning personal data. By standardizing and strengthening protections of individuals' privacy throughout the EU and shedding light on the responsibilities of organizations using personal data, the GDPR represents an evolution of privacy protection, moving from a rights-based to a fundamentality-based approach . From an engineering perspective, addressing compliance with the GDPR is a challenging task. Compliance requires understanding and conforming to intricate legal requirements. Such requirements result in the need for significant organizational changes and the evolution of complex systems that store and process statutory personal data. AI models training and functioning also rely on complex data-driven processes. Consequently, the legal approach of mitigating biases introduced by data-based technologies can be illuminating.

7.2. California Consumer Privacy Act (CCPA)

As a case study of the larger topic, the California Consumer Privacy Act (CCPA) was examined because it is the only AI-specific law currently in place that is not currently being challenged. The CCPA was passed in 2018, and it took effect on January 1, 2020. Companies had until July 1, 2020 to bring their policies into compliance. The impetus behind the CCPA was a concern from California legislators that companies weren't being transparent about the data they were collecting on their customers and how it was being used. In 2019, European Union's General Data Protection Regulation (GDPR) took effect, and it was viewed as overly restrictive to businesses. However, the CCPA contains some of the same provisions as the GDPR, such as requiring companies to disclose what data about a consumer they have collected and prohibiting the sale of the data to a third party unless the consumer is made aware and agrees to it. The act differs from the GDPR in that the burden of litigation mainly lies with the government instead of consumers (Samarin et al., 2023).

The CCPA applies to for profit entities that

1. Collect personal information from California residents when at least $25 million in gross annual revenue;
2. Buy, sell, or receive personal information about at least 50,000 California consumers or their households for commercial purposes; or
3. Derive more than 50 percent of its annual revenue from the sale of personal information.

For the purposes of this act, "personal information" is defined broadly as information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, to a particular consumer or household (Dwivedi et al., 2021).

8. Future Trends in AI Regulation

The rapid development of emerging technologies, such as generative AI and deepfake proliferation, creates new challenges for companies and governments in terms of creating robust legal frameworks for regulation. Technological advancement will always outpace the laws and regulations governing the abuse of that technology. The market can cope temporarily with a vacuum of laws or interpretative rules but the liberal use of such technology has the ability to curtail democratic freedoms, insult cultural sensitivities, produce emotionally simplistic and ideologically simplistic information, and create social hardship.

In view of past failures, legislators should investigate greater involvement of a broader array of stakeholders in the legislative processes and greater reliance on network or platform governance models. Legislative responses to the rise of radio and television broadcasters wanting to turn human audiences into objects to be monitored and influenced were too late. Efforts at self-regulation were ignored as the entrenched interests of well-monies elites and high-margin industries swept aside civil interests. The same might be expected again with the rise of large tech platforms wanting to turn all humans into monitored objects using high-capacity surveillance, data-mining and automation processes. Technologists and technical experts alone cannot be relied upon to design laws which will guard against risks to society arising from their own developments. Regardless of the strength of the laws and rules, AI will operate independently from any human supervision. Errors or malfunctions will occur and may cause catastrophic results. Where laws provide safety nets operators may directly or indirectly invoke exemption clauses away from liability. Therefore, there is a clear need to examine corporate and government organizational accountability for risks.

8.1 Emerging Technologies and Regulatory Challenges

The advent of emerging technologies poses challenges to pre-existing relations within the legal framework organized in anticipation of past paradigmatic technologies. The persistence of a linear evolution, applied to the existing legal framework, may result in gaps of law and regulation that permit the abuse of new technology, as well as its prudent and ethical utilizations being exploited 23. As continues to evolve, allowing for new functions and possibilities, its governance and the regulation of its societal, ethical, and legal impacts are sought after. Law has a dynamic nature, and new events permeating its rules and norms do happen, as underlined by the construction of new legal qualifications, new institutions and regulatory agencies, or the adjustment of sanctions in light of new facts (Veale & Zuiderveen Borgesius, 2021).

In other words, event-driven construction takes place as new circumstances and facts take place. Nonetheless, it follows a difficult path, laden with negotiations and conflicts stemming from vested interests and power able to counter the change of present status quo. This has been the case with such technologies as the telephone, the internet, television, factory automation, and so forth. This historic pattern need to ask about the implications of the current emergence of Artificial Intelligence (AI), and about its social interaction with the (under-construction) rules, laws, norms, and institutions intending to shape its development and use. Rapidly addressing the four set of questions mentioned above; this gives account of the technical and social unfolding of AI and of its legal governance and regulation, exploring this dyadic interaction (Dwivedi et al., 2021).

8.2 Global Cooperation and Harmonization Efforts

Examining global cooperation and harmonization efforts in AI regulation, this subsection navigates the international dimension of AI governance, highlighting the significance of collaborative approaches across borders. This includes challenges regarding cross-border data flows, technology transfer, and multinational AI systems impacting multiple jurisdictions. In this context, efforts by international organizations and attempts to facilitate collaboration among diverse stakeholders are examined.

Concerns surrounding the regulation of AI systems often extend beyond domestic jurisdictions, requiring international consideration. AI systems are trained on vast and diverse datasets, many of which contain personal data. National data privacy frameworks typically include provisions governing the transfer of personal data outside their borders. The AI systems that analyze these datasets typically require other necessary considerations, such as specific computing facilities and sufficient AI literacy. Similarly, aside from data privacy concerns, national security laws may impose restrictions on the transfer to another country of highly sensitive AI systems (Stix, 2022). To establish a level playing field across nations, policy responses are vital at the international level.

International norms, standards, and principles provide blueprints to govern the domestic use of AI systems (Stix, 2022). Concerns regarding the transnational use of AI systems, either directly or indirectly often consist of loosely structured normative “soft law” efforts. Nevertheless, the international nature of AI raises challenges regarding the enforcement of various international non-binding recommendations. In such a fast-moving sector, efforts remain to proactively manage the risks associated with AI systems before the global application of these technologies occurs. To bolster understanding, transparency, and knowledge sharing among regulators, there is a need to facilitate international cooperation in AI governance, including the establishment of coordination mechanisms and pathways for cross-border investigations, risk assessments, and other regulatory measures.

Within this context, bilateral initiatives and the desire to establish AI “trust zones” are discussed. To ensure ongoing cohesion and an avoidance of fragmentation of AI industrial policy choices, AI governance is examined within a broader

international context that calls for an inclusive and globally sensitive approach to technology transfer. This is achieved by minimizing industrial policy competition that favors any one economic bloc. Ultimately, the efforts showcased in this section represent a growing recognition of the significance of the international dimension of AI governance, with welcoming acknowledgement that the desirable goal of globally cohesive and harmonized regulatory mechanisms is vital in rendering techno nationalism and splinter net concerns inevitable.

9. Conclusion and Recommendations

This essay has examined the legal frameworks for regulating artificial intelligence (AI) and ensuring accountability for its use. Key insights include the need for regulation that strikes a balance between fostering AI innovation and protecting individuals and society from AI-related harms, the importance of transparency and explainability in AI decision-making processes, and the challenges of assigning responsibility for harm caused by autonomous AI systems. The complexity and diversity of AI systems make it difficult to determine causation, foreseeability, and intent, complicating the question of liability allocation 19. Reasoning by analogy to human behavior is often inadequate: in the case of self-driving cars, a lack of manual intervention from the driver does not entail a lack of responsibility for the manufacturer. The essay also highlights the gap between the promise of AI and its economic, ethical, and societal problems. The range of approaches and instruments taken by the EU member states is very broad, pointing to the necessity of a sophisticated and coordinated risk-based approach including legal standards, standards, and best practices in every relevant field.

To translate the key insights into actionable recommendations, it is suggested that policymakers engage in ongoing discussion with a diverse group of stakeholders, including the technology sector, civil society, academia, and concerned citizens. Policymakers should consider the appropriate degree of intervention, not limiting options to hands-off regulation, strict liability, or blanket criminalization of AI practices. Instead, respondents should be free to choose the safest AI practices. Policymakers should provide a minimum degree of assurance of compliance with the standards. They should solicit and consider public input on the level of acceptable AI risk. Policymakers should be mindful that regulation means intervention in a system, which can drive behavior underground. Lastly, when considering regulatory standards, policymakers must first clarify their objectives.

9.1. Policy Recommendations for Effective AI Regulation

Policy recommendations for effective AI regulation are proposed. Policymakers, legal professionals, and other stakeholders are provided with actionable insights. The aim is to present practical guidelines and strategic recommendations to navigate the complex AI governance landscape within the legal domain. The proposed recommendations find their origin in publicly available documents, including the European Commission's White Paper on AI and the AI Act Proposal, as well as the author's research.

Firstly, it is recommended that regulators deepen their technical understanding of AI systems. AI tools are often marketed to decision-makers in the form of automated applications that obfuscate AI systems' real risk and magnify their apparent benevolence. Regulators and decision-makers should be aware of the AI systems' contextual use, expert opinion, and calibration to make informed judgments about their safety and fairness. The AI systems dispute resolution mechanisms, or Auditability-from-the-Outside provisions, should further ensure that AI systems' safety, performance, and fairness are independently verified and audited (Meszaros et al., 2022).

Furthermore, regulators are encouraged to monitor any changes made to the AI systems which are high-risk by nature or impact to the decision-makers. Internal decision-making processes for AI systems should be accurate and accessible to regulatory scrutiny. In this vein, IA systems operate more like moving targets than static algorithms, and decision-makers should keep track of any updates or modifications made to the model particularly when updates are applied automatically and unilaterally, as is often the case with commercial partnerships.

References

Belle, V. (2019). The quest for interpretable and responsible artificial intelligence. *The Biochemist*, *41*(5), 16-19. https://doi.org/https://doi.org/10.1042/BIO04105016

Budhwar, P., Chowdhury, S., Wood, G., Aguinis, H., Bamber, G. J., Beltran, J. R., Boselie, P., Lee Cooke, F., Decker, S., & DeNisi, A. (2023). Human resource management in the age of generative artificial intelligence: Perspectives and research directions on ChatGPT. *Human Resource Management Journal*, *33*(3), 606-659. https://doi.org/https://doi.org/10.1111/1748-8583.12524

Cai, W., Chen, W., Fang, J., & Holm, S. (2018). A survey on fractional derivative modeling of power-law frequency-dependent viscous dissipative and scattering attenuation in acoustic wave propagation. *Applied Mechanics Reviews*, *70*(3), 030802. https://doi.org/https://doi.org/10.1115/1.4040402

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896.

https://doi.org/https://doi.org/10.1016/j.inffus.2023.101896

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., Scott, K., Schieber, S., Waldo, J., & Weinberger, D. (2017). Accountability of AI under the law: The role of explanation. *Artificial Intelligence*, 21. https://doi.org/https://doi.org/10.48550/arXiv.1711.01134

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., & Eirug, A. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management*, *57*, 101994. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Ferrer, X., Van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: a cross-disciplinary perspective. *IEEE Technology and Society Magazine*, *40*(2), 72-80. https://doi.org/https://doi.org/10.1109/MTS.2021.3056293

Gervais, D. J. (2023). Towards an effective transnational regulation of AI. *AI & society*, *38*(1), 391-410. https://doi.org/https://doi.org/10.1007/s00146-021-01310-0

Goldman, J., & Hudson, Z. (2000). Perspective: Virtually Exposed: Privacy And E-Health: Privacy concerns are keeping consumers from reaping the full benefit of online health information. *Health Affairs*, *19*(6), 140-148. https://doi.org/https://doi.org/10.1377/hlthaff.19.6.140

Hacker, P. (2023). The European AI liability directives–Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, 105871. https://doi.org/https://doi.org/10.1016/j.clsr.2023.105871

Larsson, S. (2019). The socio-legal relevance of artificial intelligence. *Droit et société*, *103*(3), 573-593.

Messias, I. d. A., Nascimento, A., & Rocha, R. (2022). Job rotation as a legal requirement: analysis of the participatory approach in acceptance and workers' perception at a meatpacking plant. *Gestão & Produção*, *29*, e10522. https://doi.org/https://doi.org/10.1590/1806-9649-2022v29e10522

Meszaros, J., Minari, J., & Huys, I. (2022). The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union. *Frontiers in Genetics*, *13*, 927721. https://doi.org/https://doi.org/10.3389/fgene.2022.927721

Radanliev, P., Santos, O., Brandon-Jones, A., & Joinson, A. (2024). Ethics and responsible AI deployment. *Frontiers in Artificial Intelligence*, *7*, 1377011. https://doi.org/https://doi.org/10.3389/frai.2024.1377011

Samarin, N., Kothari, S., Siyed, Z., Bjorkman, O., Yuan, R., Wijesekera, P., Alomar, N., Fischer, J., Hoofnagle, C., & Egelman, S. (2023). Lessons in VCR repair: Compliance of android app developers with the california consumer privacy act (CCPA). *Cryptography and Security*, 19. https://doi.org/https://doi.org/10.48550/arXiv.2304.00944

Smyrnova, K. (2021). Europeanization of Competition Law: Principles and Values of Fair Competition in Free Market Economy in the EU and Association Agreements with Ukraine, Moldova, and Georgia. In *EU External Relations Law* (pp. 163-176). Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-030-62859-8_10

Stix, C. (2022). Foundations for the future: institution building for the purpose of artificial intelligence governance. *AI and Ethics*, *2*, 463-476. https://doi.org/https://doi.org/10.1007/s43681-021-00093-w

Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, *35*, 1305.

Trunk, A., Birkel, H., & Hartmann, E. (2020). On the current state of combining human and artificial intelligence for strategic organizational decision making. *Business Research*, *13*, 875-919. https://doi.org/https://doi.org/10.1007/s40685-020-00133-x

Van Vliet, N., Gomez, J., Quiceno-Mesa, M., Escobar, J., Andrade, G., Vanegas, L., & Nasi, R. (2015). Sustainable wildlife management and legal commercial use of bushmeat in Colombia: The resource remains at the cross-road. *International Forestry Review*, *17*(4), 438-447. https://doi.org/https://doi.org/10.1505/146554815817476521

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97-112. https://doi.org/https://doi.org/10.9785/cri-2021-220402

Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. *Frontiers in Artificial Intelligence*, *7*, 1320277. https://doi.org/https://doi.org/10.3389/frai.2024.1320277

How to cite this article

Kahidhim, A. J. A. A. (2024). Artificial Intelligence and the Law: Legal Frameworks for Regulating AI and Ensuring Accountability. *Utu J.*, *1*(1), 18-29. doi: 10.57238/ujls.s90hsa43

Access this article online