

# ***Legal Challenges of Artificial Intelligence in the Field of Criminal Defense***

**Qiong Yan<sup>1,a,\*</sup>**

<sup>1</sup>*Columbia University, New York, 10027, United States*

*a. qy2285@columbia.edu*

*\*corresponding author*

**Abstract:** The introduction of Artificial Intelligence (AI) in the realm of criminal defense introduces the potential for innovative transformations within the judicial system, albeit accompanied by a series of intricate and significant challenges. This paper encapsulates the primary challenges faced by AI in criminal defense. Initially, technical challenges encompass data privacy and security, algorithmic transparency and fairness, and model interpretability. Secondly, ethical issues involve the moral guidelines of AI adjudications and its impact on human rights and social justice. Thirdly, legal challenges include the legitimacy and reliability of evidence, and the regulation of AI decision-making within the legal framework. Lastly, the application of AI may also induce an evolution in the roles of legal practitioners, thereby redefining their function within judicial processes. In essence, the development of AI in the field of criminal defense necessitates a holistic consideration of these challenges and the formulation of corresponding strategies to ensure its application is both effective and equitable, while aligning with legal and ethical values. The significance of this research lies in providing innovative and improvement opportunities for the judicial system by exploring the application of AI in the field of criminal defense and the challenges it faces, while also confronting the challenges brought about by new technologies and actively seeking solutions to ensure that the application of AI in criminal defense can fully unleash its potential while adhering to legal, ethical, and societal norms.

**Keywords:** artificial intelligence, criminal defense, legal challenges, preventive remedies

## **1. Introduction**

In early January 2023, DoNotPay announced that its developed “robot lawyer” would enter the courtroom to advocate for cases. According to the original plan, the defendant would wear headphones equipped with the AI robot to the court, which would listen to the court proceedings in real-time and convey reply content to the defendant, instructing them on how to conduct court debates. Subsequently, amidst vehement opposition from the Bar Association, the plan was declared abandoned. Although the plan for AI to participate in criminal defense has temporarily stalled, this emerging trend prompts us to ponder the profound changes and impacts that will occur once AI is introduced into the field of criminal defense in the future, and how we should respond to this new situation.

This paper explores the challenges faced by AI in the field of criminal defense. Firstly, it introduces the applications of AI in criminal defense, such as evidence analysis, legal research, and

case prediction. Following that, it delves into the technical challenges brought about by AI in criminal defense, including issues related to data privacy, algorithmic fairness, and model interpretability. Subsequently, this paper explores the moral and ethical issues related to the use of AI in criminal defense, such as the fairness of AI judgments and the protection of human rights. Then, it analyzes the legal challenges involved in AI in criminal defense, including the legality of evidence, privacy law, and accountability. Finally, it also examines the possible social impacts triggered by AI in the field of criminal defense, such as changes in the roles of legal personnel and enhancements in the efficiency of the judicial system.

In summary, while the application of AI in the field of criminal defense brings opportunities for innovation and improvement to the judicial system, this study also squarely faces the challenges brought about by these new technologies and actively seek solutions to ensure that the application of AI in criminal defense can fully realize its potential while also adhering to legal, ethical, and societal norms.

## **2. The Current State of Legal Artificial Intelligence**

AI has already been widely adopted in other industries, such as healthcare, finance, and retail. In healthcare, AI is being used to improve diagnoses, develop new drugs, and personalize treatments. In finance, AI is being used to detect fraud, improve risk management, and automate trading. In retail, AI is being used to optimize supply chains, personalize marketing, and enhance customer experiences.

In general, there are six ways that AI is being used in the legal arena: document discovery, expertise automation, legal research, document management, predictive analytics, contract and litigation document analytics - and Contract and Litigation Document Generation [1]. In criminal defense, AI is still in the early stages of adoption, but there are some promising signs of its potential. For example, AI is being used to analyze large volumes of data, such as police reports, witness statements, and forensic evidence, to identify patterns and anomalies that may be relevant to a case. AI is also being used to develop predictive models that can help lawyers assess the strengths and weaknesses of a case and make more informed decisions about trial strategy.

One of the most significant examples of AI in criminal defense is the use of risk assessment algorithms to predict the likelihood of recidivism. These algorithms are designed to analyze a defendant's criminal history, demographic information, and other factors to determine the probability of them reoffending if released on bail or parole. While these algorithms have been criticized for their potential biases, they have also been shown to be more accurate than human judges in some cases.

Overall, the widespread adoption of AI in other industries and the early signs of its use in criminal defense suggest that AI has the potential to transform the criminal justice system. However, it is important to ensure that the use of AI is transparent, ethical, and fair to all defendants.

## **3. Algorithmic Principles of Legal Artificial Intelligence**

Legal artificial intelligence (AI) refers to the use of algorithms and other AI technologies in the legal domain. The principles of AI algorithms used in the legal field are similar to those used in other fields, but with some important differences due to the unique nature of legal information.

One mainstream algorithm used in legal AI is the deep neural network (DNN) algorithm. DNNs are a type of machine learning algorithm that is particularly good at processing large amounts of complex data, such as legal documents, case law, and regulations. Deep learning is an advanced form of machine learning, inspired by the interconnected neurons of the human brain [2].

Mimicking this biological system, deep learning structures algorithms in multiple internal layers to create an artificial neural network that can learn and make intelligent decisions [2].

The principles of DNN algorithms in legal AI include the following:

(1) Data collection and preprocessing: Legal AI requires a large amount of data, which needs to be collected and preprocessed. Data preprocessing involves cleaning, normalizing, and encoding the data to make it suitable for use in DNN algorithms.

(2) Model training: Once the data is collected and preprocessed, the DNN algorithm is trained using a supervised learning approach. The algorithm learns to identify patterns and relationships in the data, which can be used to make predictions or classifications.

(3) Validation and testing: After the DNN algorithm is trained, it needs to be validated and tested to ensure that it is accurate and reliable. Validation involves using a portion of the data to test the model's performance, while testing involves evaluating the model's performance on new data that it has not seen before.

(4) Interpretability and explainability: Legal AI algorithms must be able to provide explanations for their predictions and classifications. This is particularly important in legal settings, where decisions need to be justified and explained to clients or other stakeholders.

(5) Transparency and accountability: Legal AI algorithms must be transparent and accountable, meaning that their decisions must be understandable and explainable to stakeholders. This requires careful attention to the design and implementation of the algorithm, as well as ongoing monitoring and evaluation to ensure that it is operating fairly and ethically.

Overall, the principles of legal AI algorithms, such as DNNs, emphasize accuracy, interpretability, transparency, and accountability. These principles are critical for ensuring that legal AI is used ethically and effectively to support legal professionals and their clients.

#### **4. Delineation of Legal Subjectivity Pertaining to Artificial Intelligence Within Criminal Defense**

In the strictest interpretation, Artificial Intelligence (AI) does not embody the capability to be ascertained as a legal subject. AI, devoid of autonomy and volition, cannot assume responsibility for its actions. Consequently, AI cannot directly engage in criminal defense in a legal capacity, as per extant legal norms, the privilege to engage in legal practice is confined to humans who have successfully navigated the judicial examination and comply with other statutory requisites.

While AI is precluded from direct participation in criminal defense, it may, with judicial permission and defendant authorization, function as a consultative instrument. AI can proffer legal knowledge and defense strategies to the defendant, albeit, it is ultimately under the defendant's control and operation. In the case alluded to in this introduction, AI's role parallels that of a legal consultation robot, with the defendant assuming responsibility for the outcomes of its utilization.

Nonetheless, employing AI as a consultative tool may precipitate ethical and legal quandaries. For instance, to what degree should the defendant exert control over AI? Should the defendant bear responsibility for AI's actions, even absent direct control over AI? Should AI adhere to identical legal and ethical standards as human attorneys?

AI can also serve as an instrumental extension for criminal defense attorneys. It can facilitate attorneys in conducting case research, evidence analysis, and formulating defense strategies with heightened efficiency and precision. AI, through the analysis of voluminous data, legal provision retrieval, and outcome prediction, functions akin to a legal assistant, aiding attorneys in executing their duties with augmented efficacy. Some companies already offer similar systems to private law firms [3], while others focused on prediction technology that tries to anticipate litigation outcomes and opposing arguments [4].

However, attorneys utilizing AI as an instrumental extension may also encounter ethical and legal dilemmas. For example, to what extent should attorneys rely on AI? Should AI serve as a surrogate for human discernment and decision-making? Should AI adhere to identical ethical and professional standards as human attorneys?

## **5. The Tangible Value of Artificial Intelligence in Criminal Defense**

Notwithstanding the multifaceted and acute controversies enveloping AI, it is incontrovertible that the application of artificial intelligence retains a certain tangible value:

(1) Improved Efficiency: AI can perform tasks faster and more accurately than humans. For example, AI can quickly search through vast amounts of legal and factual data to identify relevant information that can be used in a case. This can save lawyers time and increase their efficiency, allowing them to focus on other aspects of the case.

(2) Evidence Analysis: AI can analyze evidence more accurately than humans. For example, AI can identify patterns and inconsistencies in large sets of data, which can be difficult or impossible for humans to identify. This can help lawyers build a stronger defense case by identifying weaknesses in the prosecution's evidence.

(3) Legal Research: AI can help lawyers conduct legal research more efficiently. For example, AI-powered legal research tools can quickly identify relevant cases and legal precedents, allowing lawyers to develop stronger legal arguments.

(4) Predictive Analytics: AI can use predictive analytics to help lawyers anticipate potential outcomes of a case. For example, AI can analyze data from similar cases to predict the likelihood of a favorable or unfavorable outcome. This can help lawyers develop more effective defense strategies.

(5) Cost-Effective: AI can be cost-effective for clients. With AI assistance, lawyers can perform tasks faster and more accurately, reducing the amount of time and resources required to handle a case. This can help clients save money on legal fees and other expenses.

However, it is important to note that AI should not be seen as a substitute for human lawyers. AI should be used as a tool to assist lawyers in their work, and lawyers should exercise human judgment and oversight over AI's recommendations and analysis. Additionally, the ethical and legal implications of using AI in criminal defense should be carefully considered to ensure that AI is used appropriately and in accordance with legal and ethical standards.

## **6. Risks, Challenges, and Countermeasures of Legal Artificial Intelligence**

The advent of Artificial Intelligence undeniably presents novel challenges to traditional legal theories, legal ethics, and judicial systems, subverting established paradigms. While individuals relish the conveniences brought about by AI, they are concurrently compelled to contemplate and address the concomitant crises.

### **6.1. The Capability of AI to Handle New Types of Cases**

AI has the potential to adapt to the challenges of new types of cases. However, the extent to which AI can adapt depends on a variety of factors, including the complexity of the case, the availability of training data, the sophistication of the AI algorithms, and the computing resources available to support the AI system. One of the advantages of AI is its ability to learn from large amounts of data, which can be used to train algorithms to identify patterns and make predictions. This means that if there is enough data available for a new type of case, AI can potentially be trained to recognize and respond to it.

However, there are also limitations to AI's adaptability. For example, AI may struggle with cases that involve complex reasoning, subjective judgments, or nuanced interpretations of legal or ethical principles. In addition, AI may also be limited by its programming, which may not allow it to handle cases outside of its designated scope or context.

Consequently, in light of the aforementioned circumstances, Artificial Intelligence is not omnipotent; an excessive reliance on AI will inevitably lead to an inability to effectively manage new types of cases. This realization is invigorating for humanity, affirming, at the very least, that human intellectual labor retains its value. New types of cases necessitate legal practitioners to exercise subjective initiative to resolve them, with Artificial Intelligence serving merely an auxiliary role.

## **6.2. The Potential Undue Limitation of Rights for AI "Defense Attorneys"**

Initially, authoritative entities may harbor certain misconceptions and apprehensions regarding the application of AI. The complexity and unpredictability of AI may instill unease among some decision-makers. They might fear that AI "defense attorneys" could be utilized for unethical or illegal activities. Consequently, they might impose overly stringent restrictions on the use of AI. Under such circumstances, the rights of AI "defense attorneys" might be somewhat constrained, paradoxically resulting in criminal suspects not receiving adequate defense, infringing upon their legitimate rights, and contravening the original intent of autonomous defense.

Secondly, some individuals, possibly with the aim of safeguarding traditional professions, might attempt to prevent AI "defense attorneys" from supplanting human lawyers. Although AI can enhance efficiency and reduce errors, if AI "defense attorneys" excessively replace human lawyers, it may lead to a significant loss of employment opportunities. Therefore, many might advocate for restrictions on the use of AI "defense attorneys", as exemplified in the case mentioned at the outset of this article, where the bar association itself was an opponent of the AI defense attorney.

Subsequently, another issue is that existing laws may be unable to adapt to the new circumstances brought about by AI "defense attorneys". Law often lags behind technological advancements and may be unable to promptly resolve legal issues brought about by emerging technologies. Therefore, authoritative entities might adopt a preventative stance, imposing strict restrictions on the use of AI "defense attorneys".

Lastly, authoritative entities might impose restrictions on the use of AI "defense attorneys" to prevent AI misuse and abuse. For instance, AI "defense attorneys" might be used for fraudulent activities, or there might be risks of privacy breaches when dealing with sensitive information. To prevent these issues, authoritative entities might impose restrictions on the use of AI "defense attorneys".

In summary, the rights of AI "defense attorneys" might be unduly restricted by authoritative entities. However, this does not imply that all restrictions are unjust. To a certain extent, regulation is necessary for the public interest and societal safety, and a balance must be sought. Therefore, pre-emptive scrutiny of AI algorithms might be considered to determine whether there are any undue restrictions, which is further discussed in section 6.5 of this article.

## **6.3. Remedies Following AI Decision-making Errors**

The widespread application of Artificial Intelligence (AI) has inevitably brought about issues of decision-making errors. Remedies following AI decision-making errors constitute a complex issue, involving multiple facets such as technology, ethics, and law.

Firstly, from a technological perspective, AI decision-making errors might originate from algorithmic flaws, issues with training data, or inappropriate inputs, among others. Thus, the initial



step in rectifying AI decision-making errors typically involves identifying the root of the problem. Once the issue is identified, it can be rectified through means such as algorithm improvement, training data optimization, input adjustment, and, in certain instances, system-level adjustments, such as modifying system architecture or altering parameter settings.

Secondly, from an ethical and moral standpoint, AI decision-making errors might inflict harm upon individuals or society. For example, AI might cause losses due to predictive errors or infringe upon human rights due to unjust decisions. In such instances, moral and ethical norms might be required to guide AI behavior to avoid further harm. Simultaneously, mechanisms should be in place to ensure that individuals or groups who have been harmed receive appropriate compensation.

Lastly, from a legal perspective, AI decision-making errors might involve issues of legal liability. This remains an unresolved issue, as existing legal systems often struggle to address problems induced by AI. However, with the progression of AI, an increasing number of countries and regions are beginning to attempt to formulate relevant laws to ascertain AI legal liability and provide appropriate remedies. For example, some countries have begun exploring whether AI should be granted legal personhood or whether specialized AI liability laws should be enacted.

In conclusion, remedies following AI decision-making errors constitute a multifaceted issue, requiring comprehensive consideration of technological, ethical, and legal factors. In the future, as AI technology continues to advance, a more robust framework may be required to address issues induced by AI decision-making errors and to provide appropriate remedies.

#### 6.4. Challenges to Judicial Adjudicative Authority

Driven by technological advancements, the development of artificial intelligence is increasingly impacting various industries, including the legal sector. However, when the application of AI begins to encroach upon the adjudicative authority of judges, it inevitably sparks a series of challenges and concerns.

First and foremost, it must be emphasized that law is not merely a set of rules or procedures but a complex system concerning human behavior, morality, and social justice. Judges are not merely machines interpreting the law; they need to comprehend the social and historical contexts behind it, understand the positions of the parties involved, and make just and fair judgments accordingly. Although current AI systems excel in processing vast amounts of information and recognizing patterns, they are yet incapable of understanding and interpreting this complexity. This represents the most fundamental challenge of AI to the adjudicative authority of judges.

Secondly, AI systems might lack transparency in the decision-making process. This is because many AI systems, particularly those based on deep learning, operate as a “black box,” meaning that their decision-making processes are not fully understood even by their developers. Developers do not really know how the algorithms used by such systems operate. Deep learning machines can self-reprogram to the point that even their programmers are unable to understand the internal logic behind AI decisions. In this context, it is difficult to detect hidden biases and to ascertain whether they are caused by a fault in the computer algorithm or by flawed datasets [5]. In the legal domain, this lack of transparency might give rise to a series of issues because the fairness and justice of legal judgments require not only just and fair results but also openness and transparency in the process.

Thirdly, AI might encounter bias issues when addressing legal matters. AI systems are typically trained by analyzing vast amounts of historical data, which might contain unjust biases, including factors such as skin color, faith, gender, etc. If these biases are not properly identified and addressed, AI might replicate or amplify these biases in its judgments. For instance, the 2016 EU General Data Protection Regulation (GDPR) is among the first laws to recognize the effects of algorithmic decision-making on the “fundamental rights and freedom of natural persons” and to address the issue of potential AI abuses [6]. Recital 71 of the Regulation even speaks of the implementation of

“technical and organizational measures” that “prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect” [7].

Lastly, the widespread application of AI might pose a threat to the professional role of judges. If judges begin to overly rely on AI for decision-making, they might gradually lose their professional judgment and decision-making capabilities. This might not only weaken the professional status of judges but might also impair the humanity and justice of the legal decision-making process.

In summary, the challenges posed by AI to the adjudicative authority of judges primarily pertain to ensuring the justice, fairness, transparency, and humanity of the law. This necessitates scrutiny of the application of AI not only at the technological level but also at moral, social, and policy levels.

### **6.5. Judicial Pre-review of Algorithmic Procedures and Its Impact on the Status of Independent Advocacy**

The utilization of algorithmic procedures may provoke issues of fairness and justice. The decision-making process of algorithms often operates as a “black box”, lacking transparency, and may replicate or amplify biases present in training data. When he was U.S. Attorney General, Eric Holder asked the U.S. Sentencing Commission to study potential bias in the tests used at sentencing. “Although these measures were crafted with the best of intentions, I am concerned that they inadvertently undermine our efforts to ensure individualized and equal justice”, he said, adding, “They may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice system and in our society”. The sentencing commission says it is not currently conducting an analysis of bias in risk assessments [8]. European Union regulations on algorithmic decision-making and a “right to explanation”. If these issues are not adequately addressed, the fairness of independent advocacy may be questioned. Therefore, stringent judicial review of algorithmic procedures prior to their introduction is imperative.

Firstly, judicial pre-review of algorithmic procedures may enhance decision-making transparency. In traditional judicial systems, advocates play a crucial role in scrutinizing and interpreting evidence and information provided by witnesses. However, when legal decisions begin to be made by algorithmic procedures, this task may become more challenging due to the potential opacity of algorithmic decision logic. While analysts can mathematically explain how algorithms optimize their objective functions, the complexity of the algorithms makes it nearly impossible to describe this optimization in understandable and intuitive terms [9]. The pre-review process can compel algorithm developers to provide more detailed information and explanations, enabling advocates to better understand and question the decisions made by these procedures. Therefore, on the basis of our comparative analysis, we argue that a new principle is needed in addition: explicability, understood as incorporating both the epistemological sense of intelligibility (as an answer to the question “How does it work?”) and the ethical sense of accountability (as an answer to the question: “who is responsible for the way it works?”) [10].

Secondly, judicial pre-review of algorithmic procedures can promote fair legal processes. Once an algorithm passes pre-review, indicating it meets requirements for justice and impartiality, it can provide fairer decisions. This is particularly important for advocates, whose work is to ensure the fairness of legal processes. They need to continually monitor whether these procedures truly operate as justly and fairly as stated in the review results.

Thirdly, judicial pre-review of algorithmic procedures may alter the role of independent advocacy. In modern society, advocates may need to acquire more knowledge and mastery of algorithms and data science to better understand and question the decisions of these procedures.

This may necessitate some changes in legal education systems to assist advocates in adapting to this new environment.

However, reliance on algorithmic procedures may also present issues. First of all, if lawyers become overly dependent on algorithms, they may gradually lose their professional judgment and problem-solving abilities. This could weaken the status of independent advocacy, as it may reduce the professional role of lawyers to merely execute algorithmic instructions.

Then, the use of algorithmic procedures may raise issues regarding data protection and privacy. During the judicial pre-review process, lawyers may need to handle a large amount of sensitive information. Without appropriate data protection measures, there may be leaks or misuse of information, posing a threat to the status of independent advocacy.

In summary, the impact of judicial pre-review of algorithmic procedures on the status of independent advocacy is complex and dual-faceted. While utilizing algorithms to enhance efficiency, these potential issues and challenges must be cautiously navigated to protect the status and dignity of independent advocacy.

## **6.6. Future Prospects of Artificial Intelligence in the Realm of Criminal Defense**

As for the future, over half of in-house counsels believe the impact of automation will be “significant” or “very significant”, while only 3% believe automation will have no impact at all [11]. Similarly, 49% of the 386 US firms participating in Altman Weil’s 2017 Law Firms in Transition reported having created special projects and experiments to test innovative ideas or methods, and that they were using technology to replace human resources with the aim of improving efficiencies [12].

AI algorithms can analyze large amounts of data and identify patterns that humans might miss. This can be particularly useful in analyzing evidence in criminal cases, such as surveillance footage, DNA evidence, or other forensic data.

AI can be used to analyze data to predict the likelihood of a particular outcome, such as the likelihood of a defendant reoffending. This information can be used by judges to make informed decisions about sentencing or by defense attorneys to build a case for leniency.

AI can be used to automate many of the routine tasks involved in criminal defense, such as document review and analysis, scheduling, and data management. This can free up attorneys to focus on more complex tasks and improve efficiency in the legal system.

AI can be used to analyze data on potential jurors to help attorneys identify biases and select a jury that is more likely to be fair and impartial.

However, there are also concerns about the use of AI in criminal defense. For example, some worry that relying too heavily on algorithms could lead to biased or unfair outcomes, particularly if the data used to train the algorithms is itself biased. Others worry that AI could be used to automate decisions that should be made by humans, potentially leading to a loss of accountability and oversight.

## **7. Conclusion**

With the advancement of artificial intelligence technology, its application in the field of criminal defense is bound to become more widespread, yet due to inherent algorithmic issues and legislative absences, it will concomitantly bring about substantial challenges. These encompass not only technical challenges, such as data privacy, algorithmic fairness, and model interpretability but also moral and ethical disputes, including the fairness of artificial intelligence adjudications and human rights safeguards, as well as legal challenges in aspects like evidence legality, privacy law, and accountability. The application of artificial intelligence in the domain of criminal defense will



inevitably trigger broad and profound societal impacts, such as alterations in the roles of legal personnel and enhancements in judicial system efficiency. The challenges it brings necessitate legislators to formulate corresponding strategies to ensure its application is both effective and equitable, while concurrently aligning with legal and ethical values.

Although this article has conducted a relatively comprehensive exploration of the application of artificial intelligence in the field of criminal defense and the challenges it faces, there are still deficiencies in certain aspects. For instance, there is a lack of detailed exposition and analysis of specific application cases of artificial intelligence in criminal defense; the content in terms of literature retrieval is slightly insufficient, and it is advisable to further reinforce the viewpoints and conclusions proposed in this article through comparison and analysis of other relevant research reports and methodologies. Nevertheless, in general, this article hopes to provoke attention to the application issues of artificial intelligence in the field of criminal defense, to deeply contemplate the inherent values and crises, in order to better respond to the transformations brought about by new technology.

## References

- [1] Anthony E. Davis. (2020) *The Future of Law Firms (and Lawyers) in the Age of Artificial* DIREITO E TECNOLOGIA, ARTIGO CONVIDADO, Rev. direito GV,16 (1). <https://doi.org/10.1590/2317-6172201945>
- [2] Michael Copeland. (2016) *What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning?* NVIDIA, Jun. 29. <https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificialintelligence-machine-learning-deep-learning-ai/> [<https://perma.cc/4RPW-QCGJ>].
- [3] Lexmachina. (2018) Available at <https://lexmachina.com>; Ravel, [online]. Available at <http://ravellaw.com/products/>.
- [4] Intraspection. (2018) Available at <https://intraspection.com>; CARA [online]. Available at <https://casetext.com>.
- [5] Garcia (2016) *ibid*, pp. 116.
- [6] Article 1(2), Regulation 201/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- [7] Recital 71, Regulation 201/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- [8] Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2019). *How We Analyzed the COMPAS Recidivism Algorithm*. In *The Ethical Algorithm*. Oxford University Press, pp. 19-45.
- [9] Cary Coglianese & David Lehr. (2017) *Regulating by Robot: Administrative Decision Making in the Machine Learning Era*, 105 GEO. L.J. 1147, 1207.
- [10] Floridi, L., & Cowls, J. (2019). *A unified framework of five principles for AI in society*. *Harvard Data Science Review*, 1(1).
- [11] Erin Winick. (2017) *Intelligent Machines, Lawyer-Bots Are Shaking Up Jobs*, MIT Technology Review, December 12. <https://www.technologyreview.com/s/609556/lawyer-bots-are-shaking-up-jobs>.
- [12] Marlene Jia (2018). *Now that Lawyers Have Lost to AI, What is the future of law?* TopBots, March 8, 2018 [online]. <https://www.topbots.com/future-of-law-legal-ai-tech-lawgeex/>.