

Crimebots and Lawbots: Cyberwarfare Powered by Generative Artificial Intelligence

Peter E. Murray

Oak Brook College of Law, Fresno, California, United States

ABSTRACT

Crimebots are fueling the cybercrime pandemic by exploiting artificial intelligence (AI) to facilitate crimes such as fraud, misrepresentation, extortion, blackmail, identity theft, and security breaches. These AI-driven criminal activities pose a significant threat to individuals, businesses, online transactions, and even the integrity of the legal system. Crimebots enable unjust exonerations and wrongful convictions by fabricating evidence, creating deepfake alibis, and generating misleading crime reconstructions. In response, lawbots have emerged as a counterforce, designed to uphold justice. Legal professionals use lawbots to collect and analyze evidence, streamline legal processes, and enhance the administration of justice. To mitigate the risks posed by both crimebots and lawbots, many jurisdictions have established ethical guidelines promoting the responsible use of AI by lawyers and clients. Approximately 1.34% of lawyers have been involved in AI-related legal disputes, often revolving around issues such as fees, conflicts of interest, negligence, ethical violations, evidence tampering, and discrimination. Additional concerns include fraud, confidentiality breaches, harassment, and the misuse of AI for criminal purposes. For lawbots to succeed in the ongoing battle against crimebots, strict adherence to complex AI regulations is essential. Ensuring compliance with these guidelines minimizes malpractice risks, prevents professional sanctions, preserves client trust, and upholds the ethical and legal professional standards of excellence.

Keywords: Cybercrime Law, Lawyers Justice, Criminals Malpractice, Rules of Professional Conduct

INTRODUCTION

Artificial intelligence (AI) automation is transforming the legal profession [1]. Terms like 'lawbot,' 'robot lawyer,' 'lawyer-bot,' and 'legal chat-bot' [2] along with debates over their capabilities and regulation, have sparked significant controversy [3]. At its core, a lawbot is an AI application designed to perform legal research tasks traditionally handled by paralegals or junior associates at law firms [4]. The use of lawbots powered by generative AI by legal professionals has surged from 19% to 79% over the past year [5]. Lawbots provides lawyers with powerful AI capabilities to analyze cases, interpret laws, evaluate evidence and optimize legal processes and strategies. Crimebots are the sinister counterpart of lawbots [6]. Crimebots maliciously repurpose AI technologies to enable criminal activities [7] and are poised to drive an impending wave of cybercrime [8]. To avert this crisis, swift and decisive action is essential. By harnessing the capabilities of lawbots and deploying them as policebots [9], we can effectively combat the emerging cybercrime pandemic [7]. Critics argue that crimebots, and lawbot AI misuse, could jeopardize protections for the innocent, facilitate the exoneration of

guilty criminals, compromise fairness and equity within the justice system [10], and intensify the harshness of criminal justice outcomes [11]. These risks arise from AI's potential for misuse, including fabricating evidence, generating deepfake alibis, and producing misleading crime reconstructions. Such abuses threaten to erode the very foundations of justice [12]. These dangers underscore the urgency for legal professionals, clients and society to grasp the beneficial and destructive implications of rules for lawbot AI taking control over the legal and justice systems.

The use of lawbot AI by U.S. legal profession is regulated by the American Bar Association's (ABA) Model Rules of Professional Conduct (MRPC) [13], the ABA formal opinion 512 governing the use of generative intelligence tools (AI Formal Opinion) [14], the State Bar of California's Practical Guidance for Artificial Intelligence (CPG) [15], and other state and national laws. While AI developers aim to elevate human capabilities through technology [16], cybercriminals increasingly exploit AI for fraudulent purposes, often operating from jurisdictions beyond legal reach [17]. For lawyers and programmers, understanding the good, bad, and destructive aspects of AI rules, can mitigate malpractice risks, avoid professional sanctions, prevent client dissatisfaction, foster ethical integrity, and promote professional excellence in an increasingly AI-driven legal landscape

LAWYERS USE OF ARTIFICIAL INTELLIGENCE

The legal profession is at a transformative crossroads, with advancements in generative AI revolutionizing the way lawyers work [18]. Similar to lawbots, AI's everyday influence is evident in tools like virtual personal assistants such as Siri and Alexa, which recognize speech and execute commands [19]. These technologies allow lawyers to issue verbal instructions rather than typing, streamlining routine tasks and reshaping their interaction with technology in practice. As AI continues to evolve, it has the potential to significantly reduce human involvement in tasks like preparing evidence and drafting legal documents [20]. This shift carries profound implications for the future of legal practice, redefining how lawyers serve their clients in an increasingly technology-driven world. AI's transformative impact on the justice system is also demonstrated by advanced platforms like LexisNexis and Casetext [21]. These tools leverage AI to generate detailed headnotes for cases, helping users to quickly grasp key legal principles and identify similar cases. AI also empowers lawyers to conduct Shepard's analyses of citations, pinpoint weaknesses in opposing counsel's arguments, and uncover opportunities to strengthen their legal strategies [22]. The widespread adoption of virtual court appearances on platforms like Zoom during the COVID-19 pandemic underscores the rapid acceptance and integration of technology into legal practice. Virtual hearings, depositions, arraignments, settlement conferences, and even trials [23] have become standard, showcasing how technology is reshaping the legal landscape. The American judiciary and legal system is widely viewed as being in a state of crisis, plagued by excessive costs, long delays, and inconsistency leading to a growing lack of public confidence [24]. One reason for this is the vast amount of information that must be collected and integrated for the legal system to function properly. Lawbot AI offers unparalleled opportunities to enhance the speed, efficiency, and accuracy of every digital task in a law practice, from managing communications, such as answering calls, emails, and messages, to scheduling meetings, depositions, hearings, and trials [25]. Lawbot AI can perform complex legal research by identifying relevant laws, statutes, and

case law to draft complaints and motions [26]. Additionally, lawbot AI can analyze court decisions, predict damages [27], and assist in developing effective case management strategies, all of which can empower lawyers to serve their clients more effectively [28]. Remarkably, lawbot AI is already capable of analyzing trends in court decisions and predicting the outcomes of class action damages cases with 79% accuracy [29]. This capability underscores lawbot AI's potential to transform the legal profession, possibly even replacing certain functions traditionally performed by judges and lawyers [30]. The exploration of the legal practice applications of Lawbots powered by generative AI is illustrated in Figure 1.

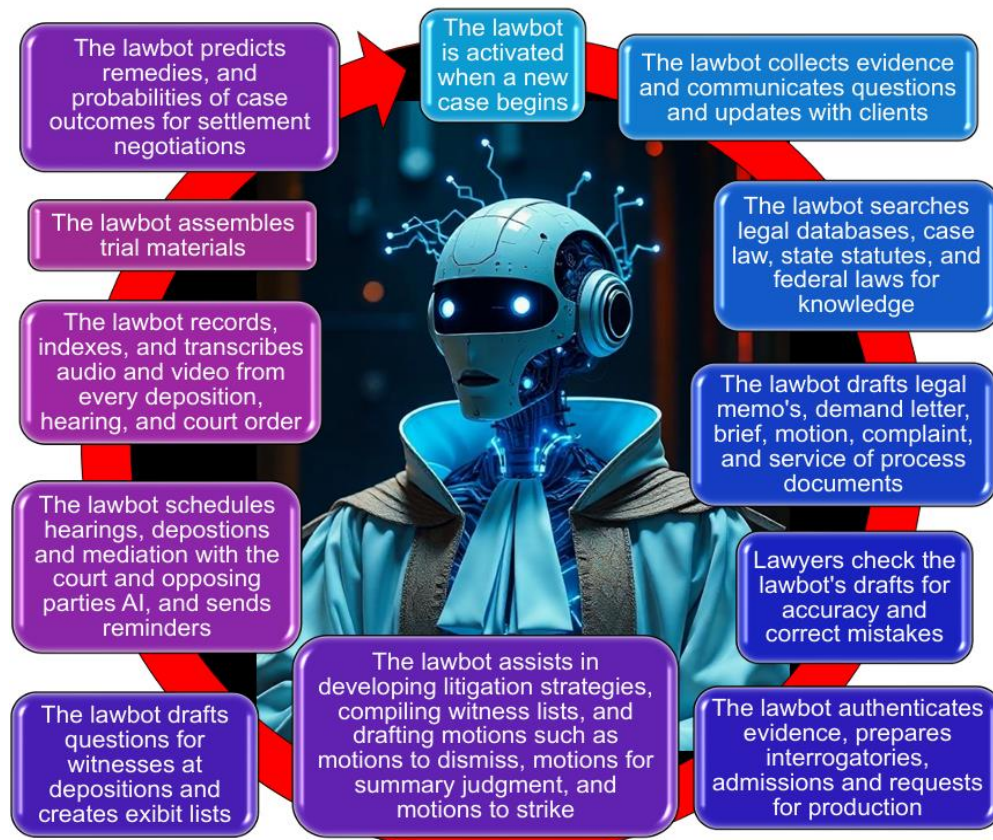


Figure 1: Lawbots legal practice applications.

Ultimately, the limits of which lawyers will use lawbot AI within their legal practice will rely on the implementation and enforcement of robust MRPC [13], AI Formal Opinion [14], CPG [15], laws, rules, and other guidelines designed to prevent misuse and safeguard ethical standards [31]. AI was created to operate with minimal human ethical oversight and is being developed and provided by major technology companies, including Google, Amazon, Apple, Microsoft, OpenAI, and others. The reliance of legal AI systems on external providers underscores the urgent need for clear ethical frameworks to guide its responsible use within the legal profession [32]. The dictionary [33] defines “artificial intelligence” as “the capability of a machine to imitate intelligent human behavior”. Unlike traditional programming, AI relies on “machine learning,” a process where machines learn autonomously and make decisions without being explicitly programmed for each specific task [34]. Machine learning or data mining is a branch

of AI to “extract knowledge from large amounts of data” [35]. This allows AI to distinguish itself from traditional software through its ability to teach itself, improve performance based on experience, and analyze large datasets [36]. AI's self-learning and autonomous decision-making capabilities have sparked considerable ethical concerns [37]. Pope Francis and others have warned about the potential risks of machines operating independently of human oversight and deciding matters as critical as war and peace [38]. Pope Francis emphasized that “No machine should ever choose to take the life of a human being,” [39] echoing the principles of Asimov's First Law of Robotics: “A robot may not injure a human being or, through inaction, allow a human being to come to harm.” [40] These concerns highlight the pressing need for stringent controls over AI, particularly in areas like the legal and justice systems, where its influence could become pervasive and unchecked.

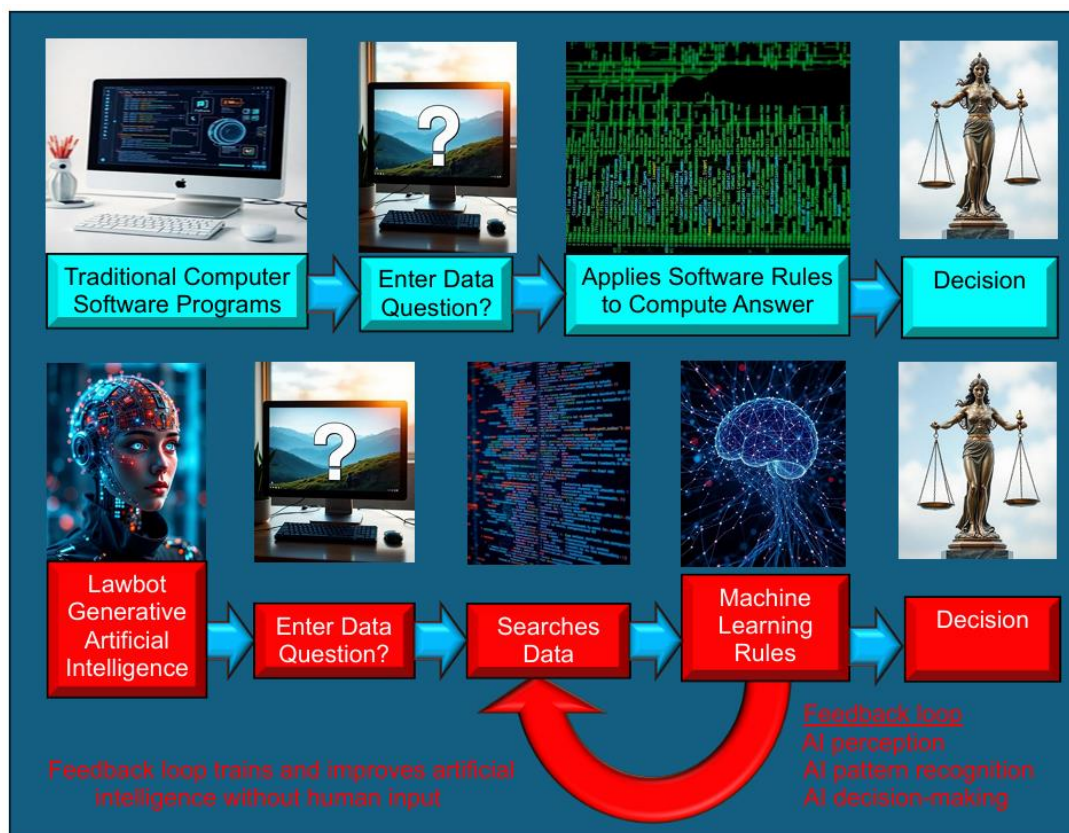


Figure 2: Lawbot generative artificial intelligence and its comparison with traditional computer software programs.

AI's machine learning capabilities, operating independently of human intervention, offer virtually limitless potential [41]. At its core, AI is powered by machine learning algorithms that are trained, rather than explicitly programmed, enabling it to perform tasks traditionally requiring human intelligence, such as perception, pattern recognition, and decision-making [42]. This fundamental difference between AI and traditional computer software programs [43] is illustrated in Figure 2, emphasizing the transformative nature of AI and the challenges it poses to ethical governance.

ARTIFICIAL INTELLIGENCE DANGERS AND RISKS

AI has the capacity to produce seemingly authentic yet entirely fraudulent documents [44], posing a serious threat to the integrity of legal proceedings. The Federal Trade Commission holds authority to prosecute fraudulent and deceptive practices involving AI, including crimebots, and chatbots disseminating false legal advice [45]. Lawyers also face significant risks when over-relying on AI-generated content, as demonstrated by a recent case where a lawyer submitted a legal brief written with ChatGPT, only for the court to discover that the AI had fabricated and falsified citations [46]. Crimebots powered by AI can create highly convincing “deep fake” images, videos, and documents, which can facilitate the rapid spread of fake news misinformation online [47]. The fake evidence is often weaponized to manipulate public opinion, promote antisocial narratives, or incite harmful behaviors [48].



Figure 3: Crimebot misuses by criminals.

The misuse of crimebot AI by criminals significantly heightens the risks of identity fraud, cybercrimes, data breaches, and cybertheft [49], threats that jeopardize both lawyers and their clients. These vulnerabilities demand vigilant security measures within the legal profession [50]. The scale of these threats is staggering, with banks reportedly fending off 45 billion cyberattacks daily [51]. A summary of how criminals exploit crimebot AI for malicious purposes is presented in Figure 3.

LAWBOT AND CRIMEBOTS ARTIFICIAL INTELLIGENCE SAFEGUARDS

In response to the risks of AI misleading users, the European Union and various governments have enacted legislation requiring AI developers to safeguard consumers from discrimination [52] and to prevent the unauthorized use of individuals' likenesses [53]. However, lawbot AI safeguards specific to the legal profession were inadequate, as the American Bar Association's (ABA) Model Rules of Professional Conduct (MRPC 2011) [12] did not yet incorporate provisions addressing the unique challenges posed by lawbot AI in legal practice. To address some of these AI shortcomings, the ABA issued its AI Formal Opinion) [14] governing the use of generative intelligence tools [lawbots], the State Bar of California introduced its Practical Guidance for Artificial Intelligence (CPG) [15], and other states are promulgating similar guidance, as an initial step toward mitigating the AI ethical gaps in the MRPC and promoting responsible use of lawbot AI within the legal field [54].

LAWYERS' VIOLATIONS OF THE RULES OF PROFESSIONAL CONDUCT

Good laws make good people [55]. But many argue that America has too many laws [56]. The nation is weighed down by an overwhelming volume of legal provisions, with the U.S. Congress producing an average of 2–3 million words of new federal legislation annually [55]. This legislative abundance is mirrored in the staggering number of regulations and statutes: over 300,000 federal regulations [57], more than 5,000 federal statutes, and over 156,000 individual sections in California's State Codes alone [58]. Compounding this complexity are innumerable state laws and local ordinances, the full extent of which remains unknown, creating a labyrinthine legal system that challenges accessibility and clarity.

Lawyers are obligated to comply with all laws and adhere to the 58 professional conduct rules outlined in the MRPC [13] that are enacted within their jurisdiction. AI's potential for enabling fraud, misuse, abuse, and breaches of confidentiality is both significant and rapidly increasing [59], driven in part by the growing use of AI by lawyers. However, the precise misuses of AI by lawyers has not been previously analyzed.

ARTIFICIAL INTELLIGENCE ABUSES AND MISUSES IN LEGAL PRACTICE

There are an estimated 1.33 million lawyers practicing in the U.S. and the total numbers of "artificial intelligence" cases in Google Scholar according to the ethical violations (keywords, to screen out non-relevant cases), were 17,884, which is 1 in 74, or 1.34%. The analysis of the proportions of "artificial intelligence" cases alleged in the Google Scholar case law revealed that its use poses serious legal risks, because AI has the potential to create disputes over charges (17%), conflict of interest (9%), responsibilities (8%), illegal (8%), diligence (8%), negligence (6%), competence (5%), evidence (5%), other jurisdictions (4%), harassment (4%), candor (3%), justice (3%), retaliation (3%), money (2%), fraud (2%), employment (2%), communication (2%), crime (1%), and others (<1%); conviction, discrimination, confidentiality, supervision, abuse of process, ethics, injustice, fabrication, dishonest and falsification. However, a statistical analysis found no significant differences (Kruskal-Wallis $X^2 = 27$, $df = 27$, $P > 0.05$) (JMP Statistical Discovery, Cary, NC, USA) shown in Figure 4. Indicating that AI can be used for many types of abuses and misuses, in addition to falsifying case law, generate flawed motions and briefs, misapply or miscite laws, and ultimately lead to injustice and unprofessional conduct [60]. These AI abuses and misuse results highlights the evolving

challenges lawyers, clients and society faces, particularly as AI introduces new complexities to the professional landscape. The numerous risks associated with using AI in legal practice underscore the urgent need for robust ethical guidelines and oversight to prevent its unethical applications.

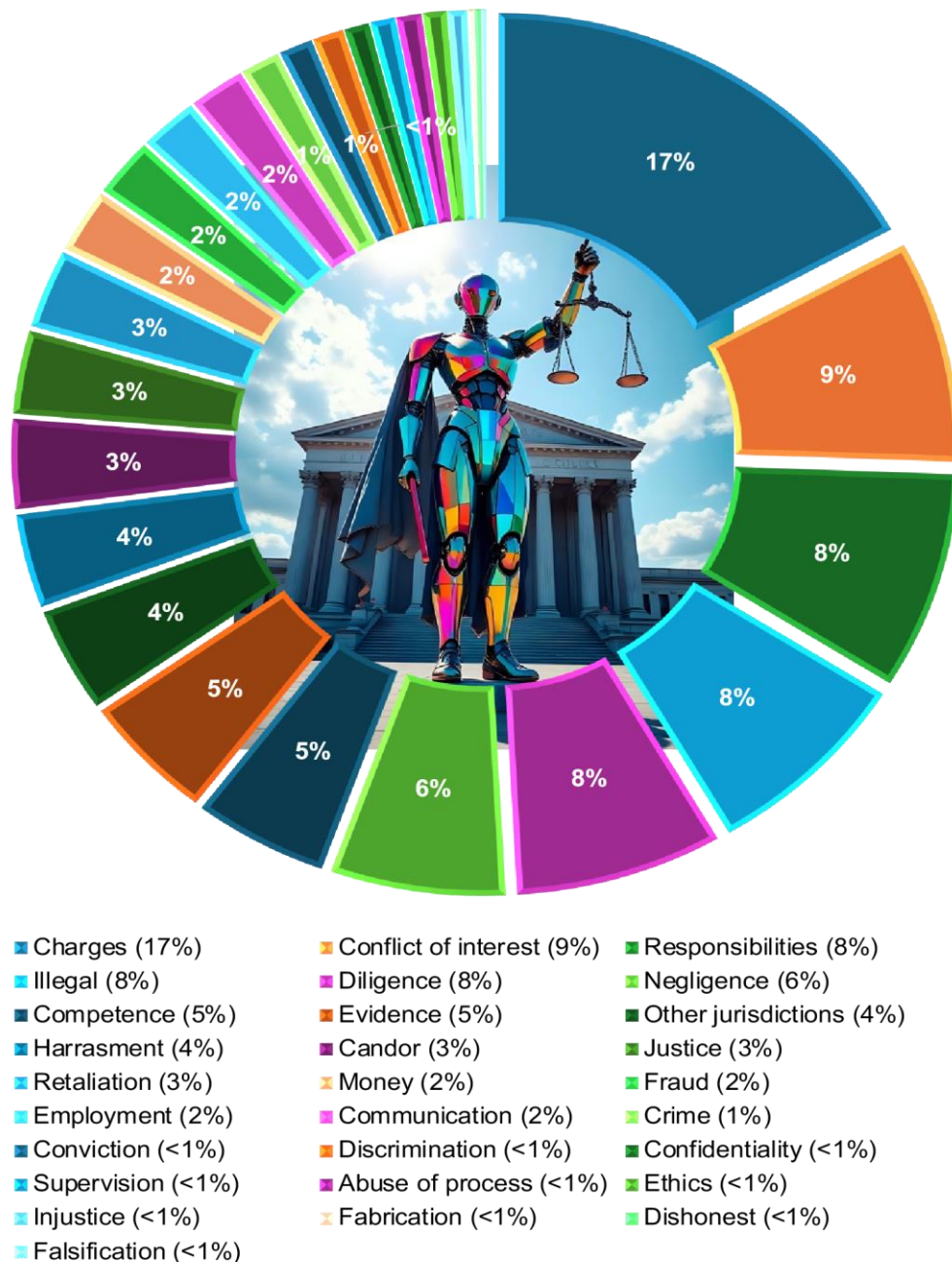


Figure 4: Pie chart of the artificial intelligence allegations in legal cases.
(This is a chart of the percentage of legal case citations from a search of these terms in Google Scholar on 01/20/25.)

A prominent example is the Cambridge Analytica scandal, where Facebook allowed unauthorized access to sensitive user data from 87 million users. Cambridge Analytica leveraged AI algorithms to micro-target political advertisements during the 2016 U.S. elections [61], raising profound concerns about data privacy and the misuse of AI for manipulative purposes.

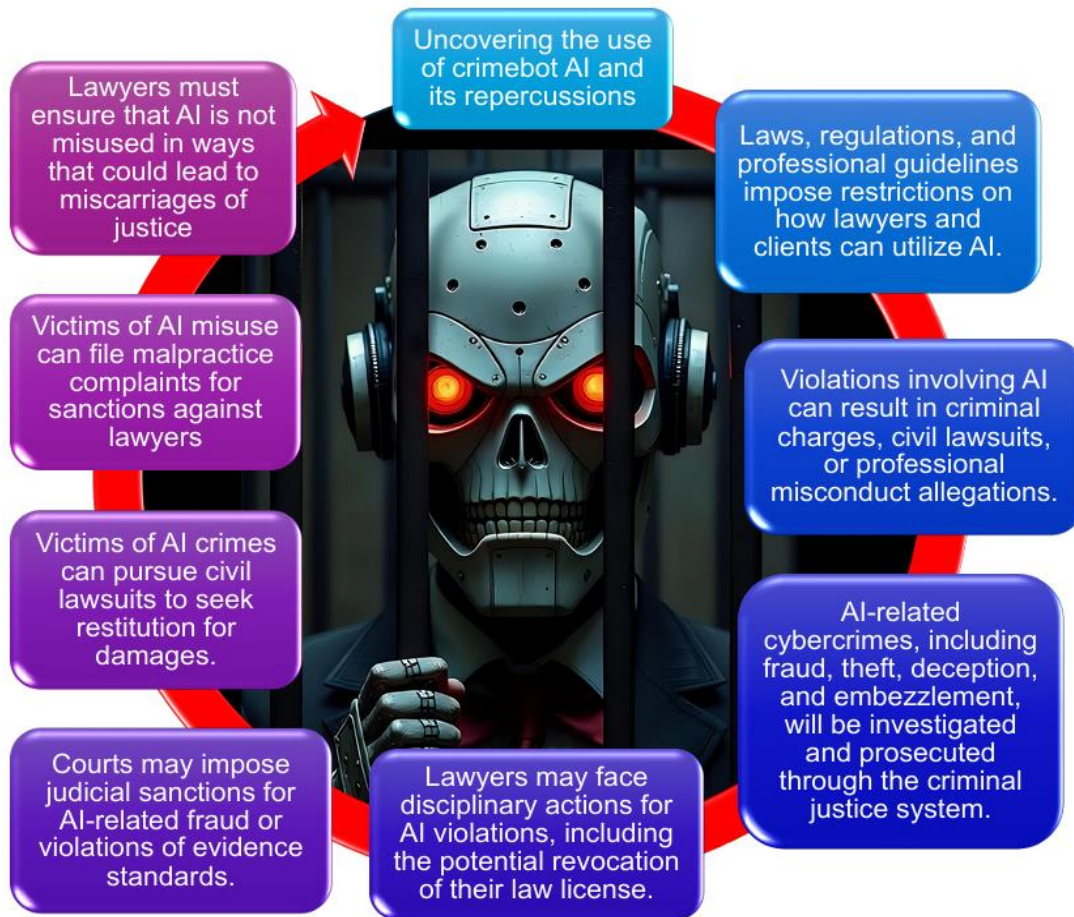


Figure 5: Crimebot misuse and its consequences

Past scandals involving major technology companies highlight the consequences of AI misuse, and the need to deter lawyers from misusing AI. This requires lawyers to have a knowledge of legal principles, adhere to their own ethics and morals, be aware of the types of inaccurate legal research due to AI reliance that can arise, detect the fabrication and falsification of evidence, understand the consequences of inaccurate AI uses, know the deterrents for AI misuses, and be aware that they may be disciplined if AI misuses are discovered, as shown in Figure 5.

LEGAL PRINCIPLES FOR USING LAWBOTS

Lawyers can apply core legal oversight principles, such as due diligence, confidentiality, competence, and accountability, to integrate AI into their practice responsibly. Legal professionals are expected to conduct thorough accurate work (MRPC Rule 1.1) [13], to successfully advocate for their clients [62]. Lawyers can apply this principle to AI by applying

the quality assurance principles of rigorously validating AI outputs, understanding the technology's limitations, and only relying on AI after verifying its accuracy, recommendations or results [63]. AI oversight helps prevent errors in case law analysis, document drafting, and legal research. Legal educators and lawyers, as stewards of justice, have both a professional and ethical responsibility to ensure that AI promotes fairness and equity in legal outcomes in a sustainable and responsible manner [64]. This requires selecting AI tools that enhance access to justice rather than creating new barriers, while leveraging technology to improve the legal system's efficiency and accessibility, particularly for underserved populations. By adhering to these principles, lawyers can use AI ethically and responsibly, ensuring that it strengthens, rather than undermines, their professional duties and client advocacy. In doing so, lawyers can uphold ethical integrity, foster trust, and advance professional excellence.

INACCURATE LEGAL RESEARCH DUE TO ARTIFICIAL INTELLIGENCE OVER RELIANCE

AI, unlike human lawyers, lacks the nuanced understanding of legal standards necessary for revising and editing legal documents. As a result, initial AI-generated drafts often require substantial human review, including thorough editing and verification of cited case law, to ensure accuracy and compliance with legal requirements. AI systems rely on the quality and comprehensiveness of the data they are trained on [65]. If the training data is outdated, incomplete, or biased, the AI may produce unreliable results, missing crucial precedents or relevant statutes. The consequences of inaccurate legal writing generated by AI can be significant, because they may lead to misrepresentations in legal proceedings, potentially resulting in unfavorable outcomes for clients, ethical violations for lawyers, or even malpractice claims [66]. As a result, it's essential for legal professionals to exercise caution and diligence when using AI tools for legal writing, ensuring thorough review and validation of all AI-generated content.

FABRICATION AND FALSIFICATION OF EVIDENCE

There have been over three-thousand wrongful convictions by the U.S. criminal justice system [67]. The conviction of a person for a crime that they did not commit, is one of the greatest travesties of the U.S. criminal justice system [68]. AI holds the potential to detect and prevent wrongful many convictions, because improved forensic technology, testimony standards, or practice standards may have prevented a wrongful conviction at the time of trial [69]. AI can be misused to generate fraudulent but authentic-looking evidence, even fabricating fake case reports and scientific medical articles; Pandora's box has been opened [44]. Legal reliance on falsified evidence can lead to serious miscarriages of justice. AI misuse can put innocent people at risk of being wrongly convicted, and incarcerated, for crimes they did not commit [70]. The increasing use of facial recognition technology creates the risk of misidentifying innocent people [71]. The consequences of wrongful convictions are damaged reputations and the loss of public trust in the legal system.

BIAS AND DISCRIMINATION BY ARTIFICIAL INTELLIGENCE

Lawyers are bound by ethical rules to ensure fairness and equal treatment for all clients [72]. If the AI tools, they use in case analysis, client selection, or sentencing recommendations introduce bias, such as favoring or disadvantaging certain racial, gender, or socio-economic groups, lawyers could face charges for ethical violations [73]. Practicing due diligence when

evaluating AI helps to prevent injustices that can arise from biased algorithms or skewed data [74]. Lawyers and firms should engage in training to better understand AI bias, equipping themselves to recognize and mitigate potential discriminatory outcomes [75]. Ensuring fairness in AI applications not only protects clients and upholds ethical standards but also preserves public trust in the legal profession.

MISAPPLICATION OF ARTIFICIAL INTELLIGENCE OUTPUTS

Lawbots do not undergo disciplinary hearings, unlike human lawyers who are subject to professional accountability and regulatory oversight [76] which underlies the ethical risks in over-relying on AI guidance. A misapplication of AI outputs in legal practice occurs when lawyers misuse or misinterpret the information or recommendations generated by AI tools [77]. This can lead to flawed case strategies, poor client advice, ethical violations, and even adverse legal outcomes. Some lawyers may rely too heavily on AI tools without applying their own professional judgment, treating AI outputs as accurate or complete without further analysis [78]. For instance, an AI system might recommend a legal precedent that appears relevant but fails to account for subtle jurisdictional nuances, rendering it less applicable to the case at hand. Training and continuing education can equip lawyers with a better understanding of AI technologies, including how to responsibly interpret and apply AI-generated data [79]. The misapplication of AI outputs highlights the need for a balanced approach in using AI within legal practice. By understanding AI's limitations and maintaining professional oversight, lawyers can enhance their practice without compromising accuracy, ethics, or the quality of client representation.

LEGAL PROFESSIONAL RESPONSIBILITY RULES

The MRPC and CPG and impose duties of confidentiality, competence and diligence, comply with the law, supervise lawyers and others, communication, charging for AI work, candor to the tribunal and meritorious claims, prohibition on discrimination, harassment and retaliation, professional responsibilities owed to other jurisdictions, which are shown in Figure 6.

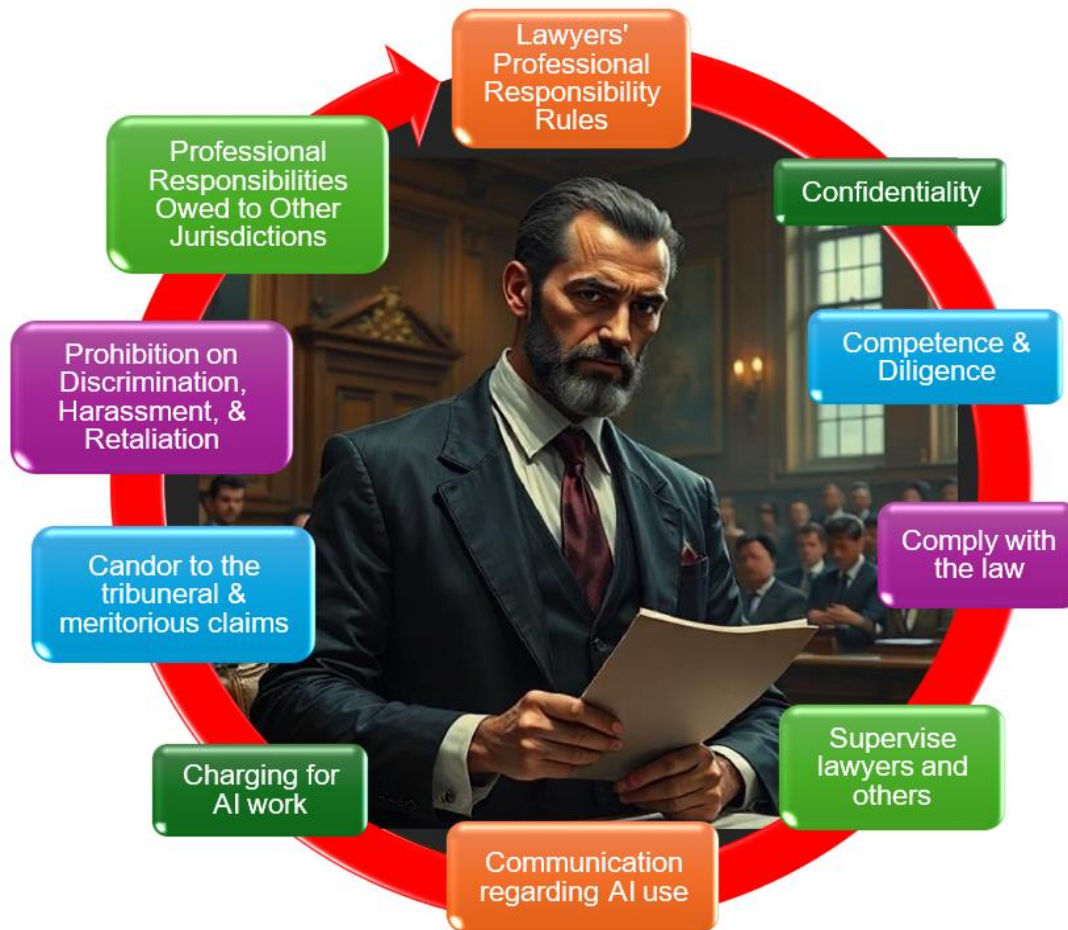


Figure 6: Lawyers' professional responsibility rules for using lawbot artificial intelligence.

GOOD ARTIFICIAL INTELLIGENCE RULES

The professional AI rules for lawyers, particularly those outlined in the MRPC [13], CPG [15], and AI Formal Opinion [14] serve as a framework for ethical practice in the legal profession. The key aspects that can be considered "good" because they are beneficial and helpful, are Client Confidentiality, Competence & Diligence, Conflict of Interest Guidelines, Honesty & Integrity, Communication Obligations, Respect for Legal System, Professional Development, Accountability & Ethical Oversight, Promotion of Justice, and Focus on Client Welfare, for the following reasons:

DUTY OF CLIENT CONFIDENTIALITY

The duty of confidentiality is fundamental to the attorney-client relationship and ensures that sensitive information is protected [80]. A lawyers breaches of confidentiality accounts for <1% of all alleged malpractice cases in Figure 4. The MRPC Rules 1.6, 1.9(c) and 18(b) [13] requires lawyers to maintain current, past and future client confidentiality that can foster trust and encourage open communication between clients and their lawyers. The AI Formal Opinion [14] states that "Lawyers also must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." The CPG [15] states that "A lawyer must not input any confidential

information of the client into any generative AI solution that lacks adequate confidentiality and security protections. A lawyer must anonymize client information and avoid entering details that can be used to identify the client.” These AI rules are necessary because lawyers are entrusted with confidential information and have a duty to protect it with the utmost care. Practicing AI stewardship involves using secure systems for data storage [81], sharing information only when legally required, deidentifying and encrypting personal data, and protecting every piece of confidential information from disclosure.

DUTIES OF DILIGENCE, COMPETENCE, AND ETHICS

Even in normal times, the legal profession is challenging, and lawyers must be especially mindful of their ethical duty to acquire competence in novel or unfamiliar areas [82] such as their use of AI. A lawyers alleged lack of diligence, competence, negligence, and breaches of ethics, comprised for 8%, 5% and >1% of all alleged malpractice cases in Figure 4. The MRPC Rules 1.1 and 1.3 [13] and the AI Formal Opinion [14] emphasizes the duties of competence and diligence to ensure that lawyers exercise the “legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation,” as well as to understand “the benefits and risks associated” with the technologies used to deliver legal services to clients.” The CPG states that “A lawyer must ensure competent use of the technology, including the associated benefits and risks, and apply diligence and prudence with respect to facts and law,” and “A lawyer’s professional judgment cannot be delegated to generative AI and remains the lawyer’s responsibility at all times.” Therefore, lawyers must gain AI skills, stay informed about AI, seek assistance from experts when necessary, and cannot delegate or avoid their AI duties of competence and diligence [83].

DUTY TO COMPLY WITH THE LAW

Clients seek guidance from lawyers to understand what the law requires, prohibits, or permits. However, the boundaries of the law are often unclear, requiring lawyers to exercise professional judgment in determining how to interpret and explain legal matters to their clients. While each lawyer-client consultation may impact only one individual, legal ethicists argue that the collective outcomes of these consultations shape the broader landscape of law in society [84]. A lawyers alleged illegal activity, fraud, conviction and injustice accounted for 8%, 2%, <1% of all the AI legal malpractice cases in Figure 4. The MRPC Rules 8.4. and 1.2.1 [13] requires lawyers to comply with the law. The CPG states that a “A lawyer must comply with the law and cannot counsel a client to engage or assist a client in conduct that the lawyer knows is a violation of any law, rule, or ruling of a tribunal when using generative AI tools.” Therefore, lawyers play a crucial role in preventing the unethical use of AI in society's everyday life.

DUTY TO SUPERVISE LAWYERS AND OTHERS

AI automation has the potential to outperform human lawyers, paralegals, and legal support staff in various tasks, with the possibility of replacing them entirely in some areas [85]. To prevent such outcomes, it is crucial to establish safeguards that ensure AI is utilized to enhance , rather than replace humans in the practice of law. By automating repetitive and tedious tasks, AI can enable legal professionals to concentrate on more complex, intellectually stimulating aspects of their work [84]. A lawyers lack of supervision accounted for only <1% of alleged malpractice cases in Figure 4. The MRPC Rules 5.1, 5.2 and 5.3 [13] impose a professional duty

on lawyers to supervise the work of lawyers and others. The AI Formal Opinion [14] states that “Managerial lawyers must establish clear policies regarding the law firm’s permissible use of [AI]... Supervisory obligations also include ensuring that subordinate lawyers and nonlawyers are trained, including in the ethical and practical use of the GAI tools relevant to their work as well as on risks associated with relevant GAI use.” The CRG [15] states “Managerial and supervisory lawyers should establish clear policies regarding the permissible uses of generative AI... providing training on the ethical and practical aspects, and pitfalls, of any generative AI use.” Accordingly, lawyers cannot abdicate their responsibility to supervise the use of AI in their legal practice. This duty is critical to ensuring that AI is employed ethically and in compliance with MPRC, CPG and other professional standards, ultimately benefiting clients while minimizing the risk of unintended consequences or violations.

DUTY TO COMMUNICATE REGARDING ARTIFICIAL INTELLIGENCE USE

Chatbots and robocalls have become prevalent in customer service communications, but ineffective interactions with these technologies can lead to client frustration, anxiety, confusion, and dissatisfaction [86]. Similarly, poor communications is a key reason that up to half of all clients hate their lawyers and is a key reason for ending client-lawyer relationships [87]. Communicating with clients can be an overwhelming task for lawyers and most of the legal malpractice claims stem from poor communication, which could have been avoided using better communication skills [86]. Although the results found only 2% of legal malpractice cases involved communication in Figure 4. The MRPC Rules 1.4 and 1.2 [13] impose a professional duty on lawyers to effectively communicate with clients. The AI Formal Opinion [14] states that “Client consultation about the use of an [AI] tool is also necessary when its output will influence a significant decision in the representation, such as when a lawyer relies on [AI] technology to evaluate potential litigation outcomes or jury selection...” but “It is not possible to catalogue every situation in which lawyers must inform clients about their use of [AI]. The CRG states: “The lawyer should consider disclosure to their client that they intend to use generative AI in the representation, including how the technology will be used, and the benefits and risks of such use.” Communication, transparency and accountability are widely recognized as essential principles for responsible AI development and deployment [88]. Transparency enables individuals to understand how AI systems make decisions that affect their lives, while accountability ensures that there are clear mechanisms for assigning responsibility and providing redress when these systems cause harm [89].

DUTY TO CHARGE FOR ARTIFICIAL INTELLIGENCE WORK

The cost of AI equipment and software typically ranges from \$20,000 to \$500,000 [90]. Legal overheads generally account for 35% to 50% of the legal fees charged [91], while the U.S. median lawyer hourly rate is \$249 [92]. As a result, it may take law firms several years to recover the cost of their AI investments. Charging clients and handling their money handling account for approximately 17% and 2% of alleged AI malpractice claims against lawyers in Figure 4. Under MRPC Rule 1.5 [13], lawyers are permitted to use generative AI to create work products more efficiently, and the costs associated with AI use may be passed on to clients, provided they comply with applicable law. The AI Formal Opinion [14] states that “The firm may agree in advance with the client about the specific rates to be charged for using a GAI tool, just as it would agree in advance on its legal fees... Absent an agreement, the firm may charge

the client no more than the direct cost associated with the [AI] tool (if any) plus a reasonable allocation of expenses directly associated with providing the [AI] tool.” The CPG further confirms that “a lawyer may use generative AI to more efficiently create work product and may... charge clients in compliance with applicable law.” Furthermore, “a fee agreement should explain the basis for all fees and costs, including those associated with the use of generative AI.” While AI offers substantial benefits by streamlining tasks like evidence analysis and case law searches, it requires significant investment. As a result, law firm overheads and costs are unlikely to decrease significantly despite the integration of AI. While some experts suggest that AI-driven digitization could commoditize legal advice, reducing reliance on human lawyers and making it more accessible and affordable for consumers [93], this outcome may only fully materialize in the long term if lawyers fail to maintain control over how AI is utilized within the legal profession. It will be disastrous for humans, if the entire legal, justice, and police systems becomes replaced by a network of AI Chatbots, Robocops and virtual judges

DUTY OF CANDOR AND HONESTY TO THE TRIBUNAL AND MERITORIOUS CLAIMS

Laws prohibiting fraud, perjury, and defamation are intended to both punish and prevent deceptive practices [94]. Spreading false information alone does not qualify for First Amendment freedom of speech protection [95]. Lawyers must never advocate for, nor tolerate, a client's false testimony. This principle aligns with the long-standing expectation that trial conduct should reflect “a search for truth” [96]. A failure of a lawyers duty of candor and being dishonest accounted for 3% and <1% of alleged legal AI malpractice claims against lawyers in Figure 4. Furthermore, some other alleged AI violations concerned justice (3%), abuse of process (<1%), and injustice (<1%) in Figure 4.

Accordingly, MRPC Rules 3.1 and 3.3 [13] impose a duty of candor to the tribunal, requiring lawyers to pursue only meritorious claims. The Formal Opinion [14] states that “output from an [AI] tool must be carefully reviewed to ensure that the assertions made to the court are not false... correct errors, including misstatements of law and fact, [correct] a failure to include controlling legal authority, and [prevent making] misleading arguments.” The CPG [15] extends these rules to the use of AI, stating, “A lawyer must review all generative AI outputs, including, but not limited to, analysis and citations to authority, for accuracy before submission to the court, and correct any errors or misleading statements made to the court.” Furthermore, a lawyer follow all rules which require the “disclosure of the use of generative AI.” Therefore, lawyers and their clients must never be permitted to use AI to fabricate or falsify evidence in any way that undermines the pursuit of justice. Furthermore, a lawyer must thoroughly review all generative AI outputs, including, but not limited to, analyses and citations to authority, for accuracy before submitting them to the court and promptly correct any errors or misleading statements.

DUTY OF PROHIBITION ON DISCRIMINATION, HARASSMENT, AND RETALIATION

Discrimination and retaliation based on race, color, sex, religion, national origin, age, disability, and genetic information is prohibited by the Civil Rights Act of 1964 [97] and other federal and state laws. However, ensuring fairness in AI systems remains a complex challenge, as antidiscrimination laws are inherently dynamic and context-specific, making them incompatible with static or standardized testing methods in AI frameworks [98], because

nearly all algorithmic inputs are correlated with race [98]. Alleged harassment, retaliation and discrimination claims account for 4%, 3% and <1% of cases in Figure 4. The MRPC Rule 8.4.1 [13] prohibits lawyers from discrimination, harassment, & retaliation. The CPG [15] extends these rules to the use of AI, stating, "Some generative AI is trained on biased information, and a lawyer should be aware of possible biases and the risks they may create when using generative AI (e.g., to screen potential clients or employees). Firms should establish policies and mechanisms to identify, report, and address potential AI biases." Consequently, lawyers cannot delegate their anti-discrimination responsibilities to AI, or operate AI without antidiscrimination policies, as everyone is entitled to equal protection under the law, fairness, and unbiased outcomes in legal proceedings. Without the intervention of human lawyers, AI lacks the capacity to uphold democratic principles and cannot adequately safeguard the legal rights of marginalized, vulnerable, disabled, disadvantaged, and minority populations.

DUTY OF PROFESSIONAL RESPONSIBILITIES AND RESPONSIBILITIES OWED TO OTHER JURISDICTIONS

AI is a global technology that transcends jurisdictional boundaries. As legal practices become increasingly multijurisdictional, lawyers must navigate the complexities of applying AI rules across diverse legal jurisdictions [99]. When laws conflict, lawyers must determine which laws take precedence, such as federal laws over state laws, and typically apply the most stringent laws to minimize the risk of legal malpractice claims. Alleged responsibilities failures, and duties owed to other jurisdictions accounted for 8% and 4% of legal malpractice cases (Figure 4). The MRPC Rule 8.5 [13] imposes a professional responsibility on lawyers to comply with the laws of all jurisdictions in which they operate. The CPG [15] further mandates that "a lawyer must analyze the relevant laws and regulations of each jurisdiction in which they are licensed to ensure compliance with such rules." The legal use of AI presents challenges for lawyers when there are no established rules for its novel applications, becomes more manageable as some rules are now in place, and is increasingly problematic due to the existence of multiple, often conflicting jurisdictional rules. Nevertheless, lawyers have a professional duty to adhere to all applicable AI rules, even when they conflict.

CONFLICT OF INTEREST GUIDELINES

Conflicts of interest remain a significant source of legal malpractice claims, ethics complaints, and law firm disqualifications, despite the widespread adoption of practices and procedures designed to mitigate them [100]. Which notes, "There are bigger merger deals, bigger transactions going on, and if you make one conflict mistake, boom, there you have it: a huge claim" [100]. Conflict of interest claims are the second leading cause of alleged legal cases, accounting for 9% of such claims, as illustrated in Figure 4. MRPC Rules 1.7 through 1.12 [13], which govern conflicts of interest, aim to protect clients by requiring lawyers to avoid circumstances where their loyalty to one client might compromise their representation of another. Common conflicts of interest that lawyers must avoid are: Personal conflicts arising from familial or personal relationships with a party to the litigation; Simultaneously representing clients with opposing interests; Breaching former client confidentiality; Engaging in pecuniary interests related to the matter of litigation; and Failing to withdraw from representation when a conflict arises. By adhering to the MRPC Rules, lawyers uphold their ethical duties and protect the integrity of client representation.

HONESTY AND INTEGRITY

Lawyers have a professional duty to uphold honesty, which requires refraining from making false statements [94]. The misuse of AI for fraud, fabricating fake evidence, creating deepfake alibis, generating misleading crime reconstructions, and engaging in the cybercrimes illustrated in Figure 3 constitutes clear dishonesty and is expressly prohibited under MRPC Rule 8.4 [13]. This rule underscores the essential role of integrity in legal practice. Notably, illegal activity, fraud and dishonesty accounted for 8%, 2%, and <1% of alleged legal cases respectively, as shown in Figure 4. By ensuring that lawyers use AI ethically and responsibly, the MRPC rules play a pivotal role in preserving public trust and confidence in the legal system.

RESPECT FOR THE LEGAL SYSTEM

AI chatbots, robocalls, robocops, messaging apps, and virtual judges lack an inherent understanding of or respect for the principles and values that underpin the legal and criminal justice systems [101]. Consequently, their use should be limited to non-legal advisory roles as communication tool, with strict oversight by lawyers to ensure ethical and professional compliance [102]. Notably, responsibilities, negligence, and abuse of process of the legal system, accounted for 8%, 6%, and <1% of alleged legal cases, respectively, as shown in Figure 4. The MRPC Rule 3.1 [13] which underscores respect for the law and the judicial system, promotes the ethical conduct of lawyers. By fostering this respect, the rule helps uphold the rule of law and ensures fairness and justice in legal proceedings.

PROFESSIONAL DEVELOPMENT

Lawyers have a professional obligation to understand AI technology before incorporating it into their practice [17], as part of their duty to provide competent representation under MRPC Rule 1.1 [13]. To integrate AI responsibly and effectively, lawyers must commit to continuous professional development. Gaining expertise in AI not only enhances their knowledge but also adds value to their services and has the potential to transform their careers [18]. AI-related issues and failures in fulfilling professional responsibilities each accounted for 8% of legal malpractice claims, as shown in Figure 4. Several jurisdictions have explicitly included a duty of "technological competence" in their ethical rules for lawyers, which encompasses the use of generative AI [31].

ACCOUNTABILITY AND ETHICAL OVERSIGHT

"AI in the legal field has evolved from science fiction to a niche subject, and now to mainstream interest... We now possess a toolset capable of transforming the legal industry for the better. It is a lawyers responsibility to use it properly" [103]. But alleged cases of negligence and lack of supervision of others, accounted for 6% and <1% of cases in Figure 4. A lawyer's duty of AI accountability and oversight means that when utilizing AI tools in their practice, they must actively ensure the accuracy, reliability, and ethical integrity of the AI's output. This includes verifying information, addressing potential biases, and taking full responsibility for any legal decisions based on AI-generated content. Lawyers must act as the ultimate decision-makers and not blindly rely on AI results [104]. The MRPC and CPG disciplinary rules are in place to help ensure accountability, providing an oversight mechanism that upholds ethical standards and addresses misconduct within the profession.

PROMOTION OF JUSTICE

Rapid advancements in AI technologies have created new opportunities for human-machine collaboration in legal practice, enhancing the capabilities of lawyers [105]. However, justice and injustice accounted for 3% and <1% of cases in Figure 4. Legal AI holds the potential to serve the public good by scaling solutions that address economic and justice disparity gaps. It can significantly improve the efficiency of legal aid lawyers, helping them streamline administrative tasks and serve more clients effectively. This aligns with many of the MRPC and other professional rules which emphasize a lawyer's duty to promote justice and serve the public interest, encouraging pro bono work and community service. This broader perspective empowers lawyers to contribute to the greater good, advancing a more equitable and accessible legal system.

FOCUS ON CLIENT WELFARE

The primary objective of the MRPC [13], AI Formal Opinion [14], CPG [15], and other professional rules is to protect clients and ensure their best interests are upheld. By prioritizing client welfare, lawyers are guided to act with ethics, fairness, and justice. These foundational principles are crucial in shaping a legal profession that is accountable, ethical, and dedicated to upholding justice.



Figure 7: Good lawbot AI rule consequences for lawyers and clients.

By adhering to these standards, lawyers can foster strong client relationships, enhance the integrity of the legal system, and make a significant positive impact on society. These "good" AI rules for lawyers provides vital guardrails for navigating the complexities of AI use, mitigating malpractice risks, avoiding professional sanctions, preventing client dissatisfaction, fostering ethical integrity, and promoting professional AI work standards of excellence. The key beneficial or "good" AI rules are summarized in Figure 7.

BAD ARTIFICIAL INTELLIGENCE RULE CONSEQUENCES

The professional AI rules for lawyers within the MRPC [13], CPG [15], the AI Formal Opinion [14], and other AI laws, rules and guidelines have consequences that can be seen as "bad" in practice. The bad consequences for lawyers are likely the inadequate guidance on AI legal technology uses, rigid AI rules – strict liability for violations, multiple layers of complicated AI rules, lack of support for solo and small firm practitioners, lack of comprehensive AI ethics training, lawyers liable for AI ethics violations - but not AI agents, and AI squeezing revenue away from lawyers, for the following reasons:

INADEQUATE GUIDANCE ON ARTIFICIAL INTELLIGENCE LEGAL TECHNOLOGY USES

While ignorance of the AI rules is likely an inadequate defense, a philosophical argument may be made that rules too vague to be enforced, can lack legitimacy [106]. The AI rules outlined in the MRPC [13] and CPG [15] provide limited and insufficient guidance on the use of AI technology. The AI Formal Opinion [14] recognizes this limitation by stating that "AI is a rapidly moving target, in the sense that its features and utility for legal practice are evolving quickly and will continue to change in ways that may be difficult or impossible to anticipate... It is not feasible to catalog every situation in which lawyers must inform clients about their use of AI." As legal practice continues to evolve alongside technological advancements, current professional rules may fail to adequately address issues related to AI, data privacy, and cybersecurity. These gaps in AI guidance expose both lawyers and clients to significant risks and liabilities, stemming from uncertainties about the boundaries between acceptable AI usage and professional misconduct. Without clearer regulations, legal professionals face challenges in navigating ethical obligations and ensuring that AI technologies are employed responsibly and effectively within the practice of law.

RIGID ARTIFICIAL INTELLIGENCE RULES AND STRICT LIABILITY FOR VIOLATIONS

The phrase "Rules are mostly made to be broken..." suggests that, in certain situations, disobeying rules may be justifiable if doing so leads to a better outcome [107]. Moreover, research indicates that overly rigid rules can backfire by fostering more rule violations. When rules are inflexible, individuals who break one rule may experience reduced cognitive conflict and are more likely to continue breaking additional rules, often resulting in serial rule-breaking behavior [108]. The AI rules outlined in the MRPC [13], CPG [15], and the AI Formal Opinion [14] require that "lawyers must be vigilant in complying with the Rules of Professional Conduct to ensure that lawyers are adhering to their ethical responsibilities and that clients are protected." The rigid structure of AI-related rules suggests that lawyers may face strict liability for violations, regardless of any defenses they might present. Moreover, this inflexibility poses significant challenges, hindering lawyers' ability to adapt to the unique needs of individual

clients. Such rigidity can restrict the development of tailored legal solutions, often prioritizing procedural compliance over the fundamental goal of serving clients' best interests.

MULTIPLE LAYERS OF COMPLICATED ARTIFICIAL INTELLIGENCE RULES

Complex rules are broken more often than simple ones [109]. Moreover, the likelihood of a rule being broken increases with its complexity, and such rules are often violated repeatedly [110]. Instead of a uniform set of AI regulations for lawyers, there exists a mosaic of overlapping and layered rules, including the MRPC [13], the CPG [15], and various state and jurisdiction-specific regulations, all demanding compliance. Adding to this complexity, there are no plans to streamline or simplify these legal AI rules. The AI Formal Opinion [14] acknowledges that "it is anticipated that this Committee and state and local bar association ethics committees will likely offer updated guidance on professional conduct issues relevant to specific GAI tools as they develop." Consequently, the landscape of AI rulemaking is still in its infancy. As new and increasingly complex rules emerge, the risk of violations by lawyers will inevitably grow, and such violations are likely to occur repeatedly.

LACK OF SUPPORT FOR SOLO AND SMALL FIRM PRACTITIONERS

The majority of all practicing U.S. lawyers work in solo or small firms [111]. Whereas, in California, nearly one in three (39.2%) attorneys work as solo practitioners, or in small law firms of between one and five attorneys [112]. Solo and small firm lawyers are disadvantaged by burdensome regulations, as shown by their disproportionately high risk of suffering disciplinary sanctions [113]. The new AI rules outlined in the CPG [15], the AI Formal Opinion [14], and similar other state rules, were imposed upon lawyers and their staff within the past few months, without adequate warning, and with no probationary AI rule learning period to adapt to these requirements. This creates a steep-learning curve for law firms every time new rules are imposed upon them. Moreover, it is unclear whether lawyers can be held liable for AI rule violations, that occurred before these regulations were introduced, despite the prohibition of *ex post facto* laws under the United States Constitution [114]. Complying with these new AI rules demands significant time, training, and financial investment. This burden disproportionately affects solo practitioners and small firms, which often lack the resources to navigate new complex AI compliance requirements. As a result, some lawyers may withdraw from representing clients in technology cases, to avoid the increased risk of AI rule violations and sanctions, potentially undermining their ability to serve clients effectively and jeopardizing equitable access to legal services for clients facing AI-related issues.

LACK OF COMPREHENSIVE ARTIFICIAL INTELLIGENCE ETHICS TRAINING

Ethical training is widely regarded as a crucial factor in effective decision-making, as it helps clarify and resolve ethical dilemmas before they escalate into violations [115]. But the new AI rules outlined in the CPG [15], the AI Formal Opinion [14], and similar state regulations were introduced without providing any comprehensive AI ethics training criteria for lawyers. Expecting lawyers to self-educate on AI ethics, does not ensure that the training they pursue will be unbiased, comprehensive or reliable, particularly in the absence of proper supervision, support and encouragement [116]. Compounding this issue, many law schools offer none or minimal AI ethics instruction, leaving new lawyers ill-equipped to navigate the AI ethical

challenges they may encounter in practice. This lack of comprehensive AI ethics training likely significantly increases the risk that lawyers will unintentionally violate the AI rules.

LAWYERS ARE LIABLE FOR ARTIFICIAL INTELLIGENCE ETHICS VIOLATIONS, BUT NOT THE AGENTS

Ethics regulators disproportionately blame and punish attorneys for AI abuses, leaving AI agents, providers, or programmers largely unaccountable [117]. Sophisticated AI agents have preemptively shifted the blame for rule violations onto lawyers, exploiting the opacity of AI systems that often harm those unable to comprehend their inner workings. If the legal profession fails to reform AI ethics rules with the creativity and flexibility this critical juncture demands, a generation of Americans harmed by AI may be denied justice from its providers [118]. AI tools—including chatbots, predictive policing systems, legal analysis software, motion drafting assistants, and even virtual jurors and judges—cannot be subjected to legal disciplinary sanctions for misconduct. Instead, the onus of responsibility falls on attorneys, who are required to maintain supervisory authority and bear full accountability for any violations [118]. This framework, codified in the CPG [15], the AI Formal Opinion [14], and comparable state regulations, is rooted in MRPC Rule 5.3(b) [13]. The rule obligates lawyers with direct supervisory authority over nonlawyers to make "reasonable efforts to ensure that the nonlawyer's conduct conforms to the professional obligations of the lawyer." These principles have been extended to encompass AI tools and providers. However, most attorneys lack the technical expertise of computer programmers, and the intricate nature of AI systems, particularly machine learning algorithms, renders it nearly impossible for lawyers to fully understand, predict, or control the behavior of their AI tools. This disconnect creates profound legal challenges, testing the limits of causality and accountability [119]. Assigning sole liability to lawyers for the autonomous or unforeseen actions of AI tools raises serious questions about fairness and practicality. The broader issue of accountability remains unresolved. AI agents' unpredictable behavior, combined with the impracticality of continuous lawyer supervision, exacerbates the problem. The current disparity in accountability—where lawyers are held liable while AI developers, providers, and programmers face no comparable consequences—risks eroding public trust in the legal profession's use of AI. This imbalance not only undermines confidence in the justice system but also fails to incentivize AI developers to prioritize the interests of lawyers and their clients. Without meaningful liability or accountability for AI providers, the potential for harm remains significant and unaddressed.

ARTIFICIAL INTELLIGENCE SIPHONING REVENUE AWAY FROM LAWYERS

Law clients frequently voice concerns about the high costs of litigation [24]. Lawyers typically utilize three primary fee structures: (i) flat fees for straightforward tasks, such as managing traffic tickets; (ii) contingency fees, ranging from 25% to 40%, often used in personal injury cases; and (iii) billable hour pricing, predominantly employed in business law [120]. The rise of AI presents a significant challenge to the traditional billable hour model. AI tools can perform tasks in seconds that previously required hours or even days, creating a dilemma for law firms. They must choose between clinging to the billable hour model—despite drastically reduced hours—or transitioning to alternative billing structures that emphasize value over time spent [121]. This shift is inevitable as AI's efficiency enhances client outcomes while law firms face shrinking revenues from fewer billable hours [122]. The legal industry is increasingly adopting

hybrid pricing models, signaling a decline in hourly billing in favor of value-based pricing. These new models better align with AI's capabilities and the tangible benefits it provides to clients [123]. However, AI is unlikely to ease the mounting pressure on lawyers to meet billable hour and profitability targets. Instead, it is more likely to squeeze revenue away from lawyers, potentially leading to unethical practices such as overbilling or rushing through cases, to maintain profitability. These "bad" aspects of the AI rules for lawyers underscore the complexities and farreaching consequences the profession will face in the years to come. Lawyers need to take a proactive approach to mitigate the "bad" aspects of the AI rules, so, they can help create a more supportive, equitable, and effective legal system—one that upholds the rule of law and serves the broader interests of justice. The bad or unhelpful and problematic, AI rule consequences are summarized in Figure 8.



Figure 8: Bad lawbot artificial intelligence regulation consequences for lawyers and clients.

DESTRUCTIVE ARTIFICIAL INTELLIGENCE RULE CONSEQUENCES

The professional AI rules for lawyers within the MRPC [13], CPG [15], AI Formal Opinion [14], and other AI laws, rules and guidelines have consequences that can be seen as unduly burdensome, or "destructive" in practice. The destructive consequences for lawyers are likely the legal workforce reductions, excessive focus on AI rule adherence - rather than deterrence

or rehabilitation and remediation, Quickly Changing AI Rules - Conflicts and Ambiguities, burdensome bureaucracy of IA rule compliance, competitive pressure to implement AI tools, insufficient support for addressing the misuse of AI by whistleblowers and malicious actors, AI cyberspace justice and technology challenges, for the following reasons:

LEGAL WORKFORCE REDUCTIONS

While AI is expected to serve as a supplementary tool in most professions, its potential impact on the legal industry may be far more disruptive. A significant number of legal roles are at risk of automation [124]. Research indicates that AI could reduce or redefine up to 80% of jobs in the legal sector, with nearly half (44%) of paralegals and secretarial staff potentially being replaced [124]. At the same time, AI tools are poised to dramatically boost the productivity of senior attorneys, law clerks, and judges, enabling them to handle complex legal tasks with greater speed and efficiency [125]. To safeguard their careers, new lawyers are advised to future-proof their skillsets by embracing lifelong learning and maintaining adaptability to evolving technologies. By staying ahead of technological advancements, they can ensure their legal expertise remains relevant and resilient in an AI-driven future.

EXCESSIVE FOCUS ON ARTIFICIAL INTELLIGENCE RULE ADHERENCE, RATHER THAN DETERRENCE OR REHABILITATION AND REMEDIATION

The mere threat of punishment is insufficient to prevent rule violations, address the root causes of misconduct, or reduce recidivism [126]. In recent years, the criminal justice system has shifted its focus from purely punitive measures to strategies emphasizing deterrence and social rehabilitation. These approaches aim to address the underlying causes of criminal behavior and reintegrate offenders into society through initiatives such as education, vocational training, and mental health treatment [127]. Given this progressive shift, it seems counterproductive for AI-related legal guidelines, such as those in the MRPC [13], CPG [15], the AI Formal Opinion [14], and other frameworks, to focus excessively on strict rule adherence without providing mechanisms for deterrence, rehabilitation, and remediation. Prioritizing deterrence in these rules would align with the broader goal of achieving compliance, ideally preventing violations altogether. Moreover, there is a notable lack of evidence regarding the nature and enforcement of punishments for AI rule violations—especially in cases where there are no human victims or measurable damages. Addressing these gaps would strengthen the ethical and practical foundation of AI legal regulations.

QUICKLY CHANGING ARTIFICIAL INTELLIGENCE RULES CREATES CONFLICTS AND AMBIGUITIES

“Today, the pace of change is not only faster but also more complex, turbulent, and unpredictable. This era of transformation is unlike any experienced before” [128]. The rapidly evolving landscape of AI regulations exemplifies this phenomenon, creating temporal anomalies where what was permissible yesterday may now be considered misconduct [129]. In just the past five years, 17 states have enacted 29 bills regulating AI. At the federal level, the White House issued an Executive Order titled Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Additionally, the White House Office of Science and Technology Policy has outlined five principles for an AI Bill of Rights, which emphasize safe and effective systems, protections against algorithmic discrimination, data privacy, transparency, and

human alternatives with fallback options [130]. Lawyers now face the challenge of navigating an ever-expanding patchwork of AI-related rules, including the MRPC [13], the CPG [15], and the AI Formal Opinion [14]. The rapid pace of regulatory changes increases the risk of rule conflicts and ambiguities, making it difficult for legal professionals to stay current. This dynamically changing AI environment not only heightens the risk of unintentional rule violations but may also paralyze legal decision-making, undermining lawyers' ability to provide effective representation.

BURDENSOME BUREAUCRACY OF ARTIFICIAL INTELLIGENCE RULE COMPLIANCE

With each new layer of AI regulations, the administrative burden on lawyers becomes increasingly complex, akin to "untangling a bowl of conceptual spaghetti" [131]. This complexity arises from the overlapping and often inconsistent nature of these rules, creating significant bureaucratic challenges. Compliance with state bar MRPC standards and AI-specific professional guidance requires substantial investments of time, effort, resources, training and costs, expenses that cannot be directly recovered through client billing. The growing bureaucracy of AI regulations imposes inefficiencies, displaces original goals, stifles innovation, fosters blind spots, dehumanizes processes, coerces compliance, and creates rigidity through risk aversion [132]. This raises critical questions about the true efficacy and value of introducing more AI rules in advancing the legal profession or protecting client interests. Moreover, there remains a notable lack of empirical evidence demonstrating that the proliferation of AI regulations and their associated bureaucratic obligations are either necessary or beneficial to legal professionals or their clients.

COMPETITIVE PRESSURE TO IMPLEMENT LAWBOOTS

The adoption of AI lawbots by legal professionals has skyrocketed over the past year, increasing from 19% to 79% [5]. This rapid growth is driven by increasing pressure on lawyers to integrate and upgrade AI technologies in response to evolving client demands for faster, more efficient legal services, intensified competition within the legal market, and the cost-saving potential of automating routine tasks. These factors compel law firms to innovate and remain competitive to stay relevant [133]. However, early adoption of AI comes with substantial risks. Failures in AI tools, such as data security breaches or operational errors, could have widespread consequences, impacting not just a single client but an entire firm's clientele, with the potential to severely damage the firm's reputation and client trust. Particularly troubling are instances of AI "hallucinations," where models generate false or fabricated information that is not grounded in real data or events [134]. Such inaccuracies are intolerable in the legal profession, where accuracy and factual reliability are paramount. Moreover, many legal professionals lack the skills and expertise necessary to mitigate or rectify AI failures, compounding the risks associated with early adoption. Given these challenges, the decision to adopt AI prematurely poses significant threats to both lawyers and their clients, making cautious and informed implementation critical.

INSUFFICIENT SUPPORT FOR ADDRESSING THE MISUSE OF ARTIFICIAL INTELLIGENCE BY WHISTLEBLOWERS AND MALICIOUS ACTORS

AI tools have made it significantly easier to create deepfake evidence, enabling tampering, fabrication, and falsification of documents, records, videos, and photographs. These deepfakes

are often so realistic that they may be admitted in court, posing serious challenges to the authentication process [135]. AI technology can be easily misused by whistleblowers or malicious actors to fabricate evidence that wrongfully implicates innocent individuals, leading to unjust convictions. Similarly, criminals can exploit AI tools to generate deepfake alibis or misleading crime reconstructions, thereby evading accountability and achieving wrongful exonerations. Lawyers often lack the specialized skills and technological resources required to detect falsified or fabricated evidence, making it increasingly difficult to challenge tainted evidence. As a result, the integrity of all evidence comes into question in the age of AI, as tampering becomes harder to detect. Innocent lawyers and clients are particularly vulnerable, as there is a widespread presumption that realistic videos, recordings, and documents are inherently truthful and reliable, an assumption that deepfake technology can exploit to devastating effect.

CYBERSPACE JUSTICE AND TECHNOLOGY CHALLENGES

Too few cybercriminals are held accountable due to inadequate policing of the internet [136]. It is unacceptable to expect lawyers to act as vigilantes in the fight against cybercrime and to deliver justice to victims [137].



Figure 9: Destructive lawbot artificial intelligence rule consequences.

The problem largely stems from law enforcement and political leaders treating cybercrime as a low priority, providing minimal resources for combating these offenses [138]. Cybercriminals are increasingly exploiting AI technology and digital platforms to perpetrate crimes against individuals and organizations, as shown in Figure 3. These criminals often conceal their identities and operate across international borders, making apprehension and prosecution especially difficult. Consequently, while cybercrime rates continue to rise, conviction rates remain stagnant [138]. This gap in justice can be attributed to multiple factors: the difficulty of identifying cybercriminals, the complexity of tracing electronic crimes, challenges in recovering stolen funds, insufficient forensic support for legal professionals, and a host of legal and technological obstacles [139]. To effectively combat cybercrime, lawyers need clearer regulations, improved law enforcement assistance, and enhanced cross-jurisdictional collaboration, such as the use of cyber-defensive models [140]. Given these challenges, very few lawyers will have the necessary skills and resources to secure restitution for the victims of cybercrimes. The AI regulations imposed on lawyers by the MRPC [13], the CPG [15], the AI Formal Opinion [14], and various state laws provide no assistance in helping lawyers identify or apprehend cybercriminals. In fact, these rules may hinder lawyers' ability to secure justice for the victims of cybercrimes. The "[cyber]road to hell is paved with good intentions [AI regulations]" [141], and while the legislators and regulators imposing multiple layers of AI rules on lawyers likely intend to benefit society, these regulations also carry significant and burdensome "destructive" consequences for the legal profession. The destructive consequences of these AI rules on lawyers are illustrated in Figure 9.

CONCLUSION

Crimebots undermine justice by committing crimes such as fraud, misrepresentation, extortion, blackmail, and identity theft, often facilitated through security breaches. Crimebots can also manipulate the legal system by fabricating evidence, creating deepfake alibis, and generating misleading crime reconstructions. These actions pose a grave threat to the integrity of the justice system, enabling wrongful convictions and unjust exonerations. To address these risks, many jurisdictions have established ethical guidelines to promote the responsible use of AI by lawyers and clients. While the growing layers of lawbot AI regulations imposed by state and national laws have the potential to produce good outcomes for lawyers, clients, and society, they also carry bad and destructive consequences. Over-regulation risks stifling innovation, threatening the legal profession's future viability, and hindering its ability to combat the cybercrime pandemic fueled by crimebots. For lawbots to succeed in the ongoing cyberwarfare battle against crimebots, strict adherence to complex AI rules and guidelines is essential. These regulations are vital for minimizing malpractice risks, avoiding professional sanctions, preserving client trust, and upholding the ethical and professional standards that underpin the legal system's integrity and excellence.

References

- [1]. Choi JH, et al., Lawyering in the age of artificial intelligence. *Minn. L. Rev.* 2024;109:147.
- [2]. Srivastav E, et al., LAWBOT: A Smart User Indian Legal Chatbot using Machine Learning Framework. In 2024 IEEE 9th International Conference for Convergence in Technology (I2CT) 2024 Apr 5 (pp. 1-7). IEEE.

-
- [3]. Arai, K. ed., *Intelligent Systems and Applications: Proceedings of the 2023 Intelligent Systems Conference (IntelliSys)*. Springer Nature; 2024.
- [4]. Debnath S, et al. LawBot: a multiagent assistant for legal research. *IEEE Internet Computing*. 2000;4(6):32-7.
- [5]. Ambrogi B. AI Adoption By Legal Professionals Jumps from 19% to 79% In One Year, Clio Study Finds. LawSites. Oct 7 2024. <https://www.lawnext.com/2024/10/ai-adoption-by-legalprofessionals-jumps-from-19-to-79-in-one-year-clio-study-finds.html#:~:text=Clients%20are%20increasingly%20supportive%20of,toward%20firms%20that%20use%20AI>.
- [6]. Pastrana, S, et al. "Crimebb: Enabling cybercrime research on underground forums at scale." *Proceedings of the 2018 World Wide Web Conference*. 2018. pp. 1845-1854.
- [7]. King, TC, et al., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*. Sci Eng Ethics. 2020;26:89–120.
- [8]. Sharkey N, et al., *The coming robot crime wave*. Computer. 2010;43(8):115-6.
- [9]. Khatri M, et al., *PoliceBOT-An Informative RASA Powered Chatbot based Crime Registration and Crime Awareness System*. Int Res J Engin Techn. 2021;8(06):1408-15.
- [10]. Solow-Niederman A. *Developing artificially intelligent justice*. Stan Tech L Rev. 2019;22:242.
- [11]. Alexander M. *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*, New Press, New York, NY, US. 2010, pp 7–8.
- [12]. Broinowski A, and F.R. Martin,. *Beyond the deepfake problem: Benefits, risks and regulation of generative AI screen technologies*. Media Int Australia. 2024:1329878X241288034.
- [13]. American Bar Association's Model Rules of Professional Conduct. 2021. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/
- [14]. American Bar Association's Formal Opinion 512. *Generative Artificial Intelligence Tools*. July 29 2024. https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethicsopinions/aba-formal-opinion-512.pdf
- [15]. State Bar of California Practical Guidance, 2024. <https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf>
- [16]. Markauskaite L, et al., *Rethinking the entwinement between artificial intelligence and human learning: What capabilities do learners need for a world with AI?* Comput Educ Artif Intell. 2022;3:100056.
- [17]. Rasyid MFF, et al., *Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime*. Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan 2024;11(1):49-63.
- [18]. Waisberg N, Hudek A., *AI for lawyers: how artificial intelligence is adding value, amplifying expertise, and transforming careers*. John Wiley & Sons; Feb 2 2021.
- [19]. Singh PN, M. Navaneetha, and P.V. Tijare, *Operating system command execution using voice command*. In 2023 3rd Asian Conference on Innovation in Technology (ASIANCON) IEEE. 2023.
-

- [20]. Frolova EE, E.P. Ermakova, *Utilizing artificial intelligence in legal practice*. In Smart Technologies for the Digitisation of industry: Entrepreneurial environment. Springer Singapore, Singapore. Oct 2 2021 pp. 17-27.
- [21]. Pike, G.H. *AI in legal research: Casetext and LexisNexis battle it out*. Info Today. 2018;35(9):167.
- [22]. Ashley, K.D. *Automatically extracting meaning from legal texts: opportunities and challenges*. Ga St UL Rev. 2018;35:1117.
- [23]. Bannon, A.L. and D. Keith, *Remote court: principles for virtual proceedings during the COVID19 pandemic and beyond*. Nw UL Rev. 2020;115:1875.
- [24]. Patterson S, et al., *The Withering of Public Confidence in the Courts*. Judicature 2024;108:1.
- [25]. Rodriguez X. *Artificial Intelligence (AI) and the Practice of Law*. In SEDONA CONF J Sep. 2023;24:783.
- [26]. Surden H. *Artificial intelligence and law: An overview*. Geo St U Law Rev. 2019;35(4).
- [27]. Giaoui FS. *From Causal Inferences to Predictive Analytics: Using AI to Settle on Damages*. J Manage Policy Pract. 2024;25(1).
- [28]. Alarie B, et al. *How artificial intelligence will affect the practice of law*. U Toronto Law J. 2018;68:supplement 1:106-124.
- [29]. Daniel B. Garrie DB, Michael M. *Using AI to Predict Outcomes in Class Action Litigation*. Law.com, May 3 2024. <https://www.law.com/2024/05/03/using-ai-to-predict-outcomes-in-classaction-litigation/>
- [30]. Bell F, et al. *AI decision-making and the courts: a guide for judges, tribunal members and court administrators*. Australasian Instit Judicial Admin. 2023.
- [31]. Shope ML. *Lawyer and judicial competency in the era of artificial intelligence: Ethical requirements for documenting datasets and machine learning models*. Geo J Legal Ethics. 2021;34:191.
- [32]. Pierce NA, Goutos SL. *Why lawyers must responsibly embrace generative AI*. Berkeley Bus LJ. 2024;21:469.
- [33]. Merriam-Webster s.v. "Artificial Intelligence," <https://www.merriamwebster.com/dictionary/artificial%20intelligence>
- [34]. Taye MM. *Understanding of machine learning with deep learning: architectures, workflow, applications and future directions*. Computers. 2023;12:91.
- [35]. Han J, Micheline K. *Data mining: concepts and techniques*. 2nd ed. Elsevier; San Francisco, CA, USA. 2006.
- [36]. Morgan L. *4 Types of machine intelligence you should know*. Information Week, November 27 2024, <https://www.informationweek.com/big-data/ai-machine-learning/4-types-of-machineintelligence-you-should-know/a/d-id/1331480>.
- [37]. Marques M, et al., *The Medicine Revolution Through Artificial Intelligence: Ethical Challenges of Machine Learning Algorithms in Decision-Making*. Cureus. 2024;16(9):e69405.
- [38]. Humble K. *Artificial intelligence, international law and the race for killer robots in modern warfare*. In Artificial intelligence, social harms and human rights. Cham: Springer International Publishing. Jan 13 2023, pp. 57-76.

-
- [39]. Pope Francis. *Pope Francis tells AI leaders: No machine should ever choose to take human life*. Catholic News Agency. July 10 2024. <https://www.catholicnewsagency.com/news/258241/popefrancis-tells-ai-leaders-no-machine-should-ever-choose-to-take-human-life>
- [40]. Asimov I. "Runaround". I, Robot (The Isaac Asimov Collection ed.). Doubleday, New York City, NY, USA. ISBN 978-0-385-42304-5. 1950, p40.
- [41]. Wach K, et al., *The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT*. Entrep Bus Econ Rev. 2023;11(2):7-30.
- [42]. Miller S. *Artificial Intelligence – What Every Legal Department Really Needs To Know, Ten Things You Need to Know as In-House Counsel*. Aug. 15 2017. <https://hilgersgraben.com/blogs/blogs-hidden.html/article/2017/08/15/ten-things-artificialintelligence-what-every-legal-department-really-needs-to-know>
- [43]. Batarseh FA, et al., *The application of artificial intelligence in software engineering: a review challenging conventional wisdom*. Data democracy. 2020:179-232.
- [44]. Májovský M, et al., *Artificial intelligence can generate fraudulent but authentic-looking scientific medical articles: Pandora's box has been opened*. J Med Internet Res. 2023;25:e46924.
- [45]. Weaver JF. *Helping AI to Comply with the Federal Trade Commission Act*. J Robotics Artif Intel Law. 2019;24:291-9.
- [46]. Neal J. *The legal profession in 2024: AI*. Harvard Law Today. Feb 14 2024.
- [47]. Zhang X, Ghorbani AA. *An overview of online fake news: Characterization, detection, and discussion*. Information Processing & Management 2020;57(2):102025.
- [48]. Hohenstein J, et al. *Artificial intelligence in communication impacts language and social relationships*. Sci Rep 2023; 13:5487.
- [49]. Desamsetti H. *Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenges*. Am J Trade Policy 2021;8(3):239-46.
- [50]. Allan K. *Cybercriminals are creating a darker side to AI*. Cyber Magazine, October 24 2023.
- [51]. Vigliarolo B. *JPMorgan exec claims bank repels '45 billion' cyberattack attempts per day*. The Register, 18 January. 2024
- [52]. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
- [53]. State of Tennessee. *The Ensuring Likeness, Voice, and Image Security (ELVIS) Act*, July 1 2024.
- [54]. Gonzalez K, Friedman M. *State Bar of California*. Cal Reg L Rep. 2024;29(2):14.
- [55]. Stout L. *Cultivating Conscience: How Good Laws Make Good People*. Princeton University Press. Princeton NJ, USA. 2010.
-

- [56]. Gorsuch N, Nitze J. *America Has Too Many Laws*. The Atlantic. August 5 2024. <https://www.theatlantic.com/ideas/archive/2024/08/america-has-too-many-laws-neilgorsuch/679237/>
- [57]. Best K. *300,000 Ways to Do Time with a Federal Crime*. UConn Today, Oct 22 2019. <https://today.uconn.edu/2019/10/threre-300000-ways-time-federal-crime/#>
- [58]. Micheli C. *How Many Sections Are in California's Codes (Statutes)?* California Globe June 9 2022. <https://californiaglobe.com/fr/how-many-sections-are-in-californias-codes-statutes/>
- [59]. Binhammad M, et al. *The Role of AI in Cyber Security: Safeguarding Digital Identity*. *J Info Sec*. 2024;15(02):245-78.
- [60]. Martin G. *Generative AI and Fabricated Evidence Ploys: A Threat to Procedural Justice and the Legitimacy of Police*. Available at SSRN 4895606. Apr 1 2024.
- [61]. Rouhiainen L. *Unethical use of artificial intelligence*. 2024. <https://lasserouhiainen.com/unethical-use-of-artificial-intelligence/>
- [62]. Kronman AT. *The lost lawyer: Failing ideals of the legal profession*. Harvard University Press, Cambridge, MA, USA. 1993.
- [63]. Wang C, et al. *Quality assurance for artificial intelligence: A study of industrial concerns, challenges and best practices*. arXiv preprint arXiv:2402.16391. Feb 26 2024.
- [64]. Balan A. *Examining the ethical and sustainability challenges of legal education's AI revolution*. *Int J Legal Prof*. 2024;31(3):323-48.
- [65]. Shumway DO, Hartman HJ. *Medical malpractice liability in large language model artificial intelligence: legal review and policy recommendations*. *J Osteo Med*. 2024;124(7):287-90.
- [66]. Johnson VR. *Artificial Intelligence and Legal Malpractice Liability*. *Mary's J on Legal Mal & Ethics*. 2024;14:55.
- [67]. Morgan J. *Wrongful Convictions and Claims of False or Misleading Forensic Evidence*. *J Forensic Sci*. 2023; 68:1-54.
- [68]. Yant MD. *Presumed guilty: When innocent people are wrongly convicted*. Prometheus Books, Buffalo, NY. USA. 2009.
- [69]. Sachoulidou A. *Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence*. *Artif Intellig Law*. Feb 22 2023:1-54.
- [70]. Sanford A. *Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated*. Innocence Project. February 14 2024. <https://innocenceproject.org/artificial-intelligence-isputting-innocent-people-at-risk-of-being-incarcerated/>
- [71]. Moy L. *Facing injustice: How face recognition technology may increase the incidence of misidentifications and wrongful convictions*. *Wm & Mary Bill Rts J*. 2021;30:337.
- [72]. Simon WH. *The practice of justice: a theory of lawyers' ethics*. Harvard University Press. Jun 30 2009.
- [73]. Walters E. *The Model Rules of Autonomous Conduct: Ethical Responsibilities of Lawyers and Artificial Intelligence*. *Ga. St. UL Rev*. 2018;35:1073.

-
- [74]. Scatiggio V. *Tackling the issue of bias in artificial intelligence to design ai-driven fair and inclusive service systems. How human biases are breaching into ai algorithms, with severe impacts on individuals and societies, and what designers can do to face this phenomenon and change for the better*. Biblioteche e Archivi. 2020. <https://www.politesi.polimi.it/handle/10589/186118>
- [75]. Pierce NA, Goutos SL. *Why lawyers must responsibly embrace generative AI*. Berkeley Bus LJ. 2024;21:469.
- [76]. Browning JG. *Robot Lawyers Don't Have Disciplinary Hearings-Real Lawyers Do: The Ethical Risks and Responses in Using Generative Artificial Intelligence*. Ga St UL Rev. 2023;40:917.
- [77]. Chanda SS, Banerjee DN. *Omission and commission errors underlying AI failures*. AI & Soc. 2024;39(3):937-60.
- [78]. Javadi SA, et al. *Monitoring misuse for accountable' artificial intelligence as a service'*. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society Feb 7 2020, pp. 300-306.
- [79]. Yu R, Ali GS. *What's inside the black box? AI challenges for lawyers and researchers*. Leg Inf Manag 2019;19(1):2-13.
- [80]. Snyder TJ. *Attorney-Client Confidentiality Is a Moral Good: Expanding Protections of Confidentiality and Limiting Exceptions*. Geo. J Legal Ethics. 2019;32:411.
- [81]. Janssen M, Brous P, Estevez E, et al. *Data governance: Organizing data for trustworthy Artificial Intelligence*. Gov Inf Q. 2020;37(3):101493.
- [82]. Hauptman WD, Beckwith KN. *The Duty of Competence in the New Normal*. Colo. Law. 2021:40-1.
- [83]. Delorey CW, et al. *A Construction Lawyer's Duty of Technological Competence-Ethical Implications of the Use of Technology and Artificial Intelligence*. Constr Law 2023;43(1).
- [84]. Kruse KR. *The jurisprudential turn in legal ethics*. Ariz L Rev 2011;53:493.
- [85]. Rogers J, Bell F. *The ethical AI lawyer: What is required of lawyers when they use automated systems?* Law Tech & Hum. 2019;1:80.
- [86]. Chhabra S, et al. *Determining the causes of user frustration in the case of conversational chatbots*. Behav Inform Technol. 2024 Jun 13:1-9.
- [87]. Morris N. *The Astounding Reason 50% of Clients Hate Their Attorneys*. Filevine, 9 May 2023. <https://www.filevine.com/blog/why-clients-hate-their-attorneys>
- [88]. Cheong BC. *Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making*. Frontiers in Human Dynamics 2024;6:1421273.
- [89]. Novelli C, et al. *Accountability in artificial intelligence: what it is and how it works*. AI Soc. 2023;23:1635.
- [90]. Lukianchenko A. *AI Development Cost: Analyzing Expenses and Returns*. TechMagic July 8 2024. <https://www.techmagic.co/blog/ai-developmentcost#:~:text=Conclusion,the%20most%20beneficial%20way%20possible>.
- [91]. The Florida Bar. *Consumer Pamphlet: Attorneys' Fees*. 2018. <https://www.floridabar.org/public/consumer/pamphlet003/#:~:text=Determination%20of%20Fees>,
-

Lawyers%20base%20their&text=A%20lawyer's%20overhead%20normally%20is,can%20be%20very%20time%2Dconsuming.

- [92]. Brock C. *How Much is a Lawyer? Hourly Rates by State and More*. LawPay. November 12 2024. <https://www.lawpay.com/about/blog/lawyer-hourly-rate-by-state/>
- [93]. Brescia RH. *What's a Lawyer For? Artificial Intelligence and Third-Wave Lawyering*. *Artificial Intelligence and Third-Wave Lawyering*. Fla. St U Law Rev. 2023.
- [94]. Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).
- [95]. Herbert v. Lando, 441 U.S. 153 (1979).
- [96]. Williams v. Florida, 399 U.S. 78 (1970).
- [97]. 42 U.S.C. § 2000e. Title VII.
- [98]. Wachter S, et al. *Why fairness cannot be automated: Bridging the gap between EU nondiscrimination law and AI*. *CLS Rev*. 2021;41:105567.
- [99]. Yang CS, Dobbie W. *Equal protection under algorithms: A new statistical and legal framework*. *Michigan Law Rev*. 2020;291-395.
- [100]. Kashefi P, et al. *Shaping the future of AI: balancing innovation and ethics in global regulation*. *Uniform Law Rev*. Nov 19 2024:unae040.
- [101]. O'Brien A. *Legal Malpractice Claim Values Reach an 'All-Time High' in Last Year*. *The American Lawyer*. May 15. <https://www.law.com/americanlawyer/2024/05/15/legal-malpractice-claimvalues-reach-an-all-time-high-in-last-year/>
- [102]. Hodes WW. *Truthfulness and Honesty Among American Lawyers: Perception, Reality, and the Professional Reform Initiative*. *SCL Rev*. 2001;53:527.
- [103]. Camello ML, et al. *Chatbots in the criminal justice system: An overview of chatbots and their underlying technologies and applications*. National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. 2021. <https://cjtec.org/files/chatbots-criminal-justice>
- [104]. Medianik K. *Artificially intelligent lawyers: updating the model rules of professional conduct in accordance with the new technological era*. *Cardozo L Rev*. 2017;39:1497.
- [105]. Nielsen A, et al. *Building a better lawyer: Experimental evidence that artificial intelligence can increase legal work efficiency*. *J. Empir Leg Stud*. 2024;21(4):979-1022.
- [106]. Dorr C. *Vagueness without ignorance*. *Philos Perspect*. 2003;17:83-113.
- [107]. Cirocco WC. *Rules are made to be broken*. *Tech. Coloproctol*. 2022;26:841-842.
- [108]. Wirth R, et al. *This Is How To Be a Rule Breaker*. *Adv Cogn Psychol*. 2018;31;14(1):21-37.
- [109]. Gaetano C. Study: *Complex Rules Are Broken More Often Than Simple Ones*. *The trusted professional*. 2019. <https://www.nysscpa.org/news/publications/the-trusted-professional/article/study-complex-rulesare-broken-more-often-than-simple-ones-100719>

-
- [110]. Lehman DW, et al. *Why Some Rules Are More Likely to Be Broken*. Harvard Bus Rev. October 7 2019. <https://hbr.org/2019/10/why-some-rules-are-more-likely-to-be-broken>
- [111]. Carson CN, Park J. *The lawyer statistical report: The U.S. legal profession in 2005*. American Bar Foundation. 2005. https://www.americanbarfoundation.org/wpcontent/uploads/2023/05/2005_lawyer_statistical_report.pdf
- [112]. The State Bar of California. 2017 Demographic survey. 2017.
- [113]. <https://www.calbar.ca.gov/Portals/0/documents/reports/ORIA/Survey-2017.pdf> [113]. Wilkins DB. *Who should regulate lawyers?* Harvard Law Rev. 1992;799-887.
- [114]. United States Constitution. 1787. Article 1, § 9 and Article 1, § 10.
- [115]. Teixeira A, et al. *Students' perceptions of corporate social responsibility: evidences from a Portuguese higher education institution*. Int. Rev Public Nonprofit Market. 2018;15, 235–252.
- [116]. Mirzayeva Q. *The benefits of teaching and learning self-study in the educational process*. Mod Sci & Res. 2024;3(1), 1–3.
- [117]. Vo T. *Regulator Says Attys Hit For AI Use Have Themselves To Blame*. Law360. May 30 2024. <https://www.law360.com/pulse/articles/1842532/regulator-says-attys-hit-for-ai-use-havethemselves-to-blame>
- [118]. Cahn AF, Loshkajian N. *Shifting AI Litigation Burden Would Help Plaintiffs in Court*. Bloomberg Law. February 22 2024. <https://news.bloomberglaw.com/us-law-week/shifting-ai-litigationburden-would-help-plaintiffs-in-court>
- [119]. Frank P. *The law of causality and its limits*. Springer Science & Business Media. 2012. 9789401063234 / 9401063230
- [120]. Bieber C Ramirez A. *How Much Do Lawyers Cost? 2024 Guide*. Forbes, January 3, 2024. <https://www.forbes.com/advisor/legal/how-much-lawyers-cost/>
- [121]. Braf D. *The fate of billable hours is in the hands of artificial intelligence*. American Bar Journal. March 10, 2024. <https://www.abajournal.com/web/article/the-fate-of-billable-hours-is-in-aishands>
- [122]. MacEwen B, Stanton J. *Pricing AI-driven legal services: The billable hour is dead, long live the billable hour*. Thomson Reuters September 10 2024. <https://www.thomsonreuters.com/enus/posts/legal/pricing-ai-driven-legal-services-billable-hour/>
- [123]. Saurabh K, et al., *Unleashing the Potential of Data Science Driven Society 5.0: Applications and Implications*. In 2024 IEEE 5th India Council International Subsections Conference (INDISCON) IEEE. 2024.
- [124]. Disphan R. *Generative AI Could Automate Almost Half of All Legal Tasks, Goldman Sachs Estimates*. Legal Tech News. March 29, 2023. <https://www.law.com/legaltechnews/2023/03/29/generative-ai-could-automate-almost-half-of-alllegal-tasks-goldman-sachs-estimates/>
- [125]. Davis LK. *AI Poses a Serious Threat to the Legal Profession. It Also Presents an Extraordinary Opportunity*. The Federalist Society. April 1 2024.
-

- [126]. Khan MI, Nisar A, Kanwel S. *From Punishment to Progress: The Legal Evolution of Criminal Rehabilitation*. Pak J Law Analysis Wisdom. 2023;2(02):556-63.
- [127]. Forsberg L, Douglas T. *What is Criminal Rehabilitation?* Crim Law Philos. 2022; 16(1):103-126.
- [128]. Kamal O. *Organizational change is tough. Here are three rules to help get it right*. World Economic Forum. November 16, 2017. <https://www.weforum.org/stories/2017/11/changing-yourorganization-is-tough-heres-how-to-get-it-right/>
- [129]. Katz L. *Before and After: Temporal Anomalies in Legal Doctrine*. U Pa L Rev. 2002;151:863.
- [130]. White & Case LLP. *AI Watch: Global regulatory tracker - United States*. December 18, 2024. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states>
- [131]. Baekgaard M, Tankink T. *Administrative burden: Untangling a bowl of conceptual spaghetti*. Perspect Public Manag Gov. 2022;5 (1): 16–21.
- [132]. Schwartz M. *The Good and The Bad of Bureaucracy*. IT Revolution. October 26, 2020. <https://itrevolution.com/articles/the-good-and-the-bad-of-bureaucracy/>
- [133]. Glaser J, Borna S. *AI: the new legal powerhouse — why lawyers should befriend the machine to stay ahead*. October 24, 2024. <https://www.reuters.com/legal/legalindustry/ai-new-legalpowerhouse-why-lawyers-should-befriend-machine-stay-ahead-2024-10-24/>
- [134]. Maleki N, Padmanabhan B, Dutta K (2024) *AI hallucinations: a misnomer worth clarifying*. In 2024 IEEE Conference on Artificial Intelligence (CAI) IEEE. 2024.
- [135]. Apolo Y, Michael K. *Beyond a reasonable doubt? Audiovisual evidence, AI manipulation, deepfakes, and the law*. IEEE Transactions on Technology and Society. 2024;5(2):156-68.
- [136]. Wall DS. *Catching Cybercriminals: Policing the Internet*. Int Rev L Comput Tech. 1998;12(2):201–218.
- [137]. Silva KK. *Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?* Int Rev L Comput Tech. 2018;32(1):21-36.
- [138]. Button M, et al. *Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective*. Criminology Crim Just. 2022;17488958221128128.
- [139]. Brown CS. *Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice*. Int. J Cyber Criminol. 2015;9(1):55.
- [140]. Awan JH, et al. *A defensive model to mitigate cyber activities*. Mehran Univ Res J Eng Technol. 2018;37(2):359-66.
- [141]. Fiorinelli G and MV Zucca, *Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU*. In Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024). 2024;3731: 1-16.