



Journal for Social  
Science Archives

## Journal for Social Science Archives

Online ISSN: 3006-3310

Print ISSN: 3006-3302

Volume 4, Number 1, 2026, Pages 2231 – 2238

Journal Home Page

<https://jssarchives.com/index.php/Journal/about>



# The Enforcement Gap: Assessing Legal Professionals' Knowledge of AI-Related Cyber Threats and Pakistan's Cybersecurity Legislation

Ahtashamul Hassan Narejo<sup>1</sup>, Dr. Abdul Basit Solangi<sup>2</sup>, Shakeela Ali<sup>3</sup> & Dr. Taha Shabbir<sup>4</sup>

<sup>1</sup>Advocate High Courts, LLM Scholar, Shaded Zulifqar Ali Bhutto University of Law, Clifton Karachi,  
Email: [narejo.ahtasham@gmail.com](mailto:narejo.ahtasham@gmail.com)

<sup>2</sup>Assistant Professor, Pakistan Studies, Shaheed Benazir Bhutto University, Shaheed Benazirabad,  
Email: [abdulbasit@sbbusba.edu.pk](mailto:abdulbasit@sbbusba.edu.pk)

<sup>3</sup>Advocate High Courts, LLM Scholar, Email: [shakeelaali.narejo@gmail.com](mailto:shakeelaali.narejo@gmail.com)

<sup>4</sup>Associate Professor, Hamdard University, Karachi, Email: [tahashabbir51@gmail.com](mailto:tahashabbir51@gmail.com)

| ARTICLE INFO                                                                                                                  |          |          | ABSTRACT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------|----------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Article History:</b>                                                                                                       |          |          | <p>The effectiveness of cybersecurity legislation depends not only on its statutory provisions but also on the awareness and competency of the legal professionals tasked with its interpretation and enforcement. This study examines the knowledge, attitudes, and preparedness of legal professionals in Karachi, Pakistan, regarding artificial intelligence (AI), its associated cybersecurity and social engineering threats, and the existing national legal framework principally the Prevention of Electronic Crimes Act (PECA) 2016. A quantitative survey was administered to 96 legal professionals, predominantly lawyers (85.4%), with data analyzed through descriptive statistics and bivariate Pearson correlation analysis. The findings reveal a significant “enforcement gap”: while 48% of respondents reported strong familiarity with AI and 63% were aware of AI-related legal risks, a striking 50% were entirely unaware of any specific Pakistani laws addressing AI-related threats. A strong positive correlation was identified between AI familiarity and concern about AI misuse (<math>r = 0.461</math>, <math>p &lt; 0.001</math>), and between concern and the perceived importance of professional education (<math>r = 0.276</math>, <math>p &lt; 0.01</math>). Despite these knowledge gaps, 88% advocated for new or updated AI-related legislation, and 82.4% considered AI-related education for legal professionals to be very important. These findings highlight a critical disconnect between the existence of legal tools and the professional capacity to deploy them, with significant implications for Pakistan's ability to prosecute and deter AI-powered cybercrimes.</p> |
| Received:                                                                                                                     | February | 15, 2026 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Revised:                                                                                                                      | March    | 08, 2026 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Accepted:                                                                                                                     | March    | 21, 2026 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Available Online:                                                                                                             | March    | 29, 2026 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Keywords:</b>                                                                                                              |          |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Legal Professionals, Artificial Intelligence, Cybersecurity, PECA 2016, Enforcement Gap, Pakistan, Continuing Legal Education |          |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Corresponding Author:</b>                                                                                                  |          |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Dr. Abdul Basit Solangi                                                                                                       |          |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Email:</b>                                                                                                                 |          |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <a href="mailto:abdulbasit@sbbusba.edu.pk">abdulbasit@sbbusba.edu.pk</a>                                                      |          |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



## **1. Introduction**

The global proliferation of artificial intelligence (AI) technologies has introduced a new frontier of cybersecurity challenges that transcend purely technical domains and demand robust legal responses. AI-powered phishing, deepfake impersonation, adaptive malware, and automated social engineering attacks have fundamentally altered the nature of cybercrime, requiring legal systems to evolve rapidly in both their statutory provisions and their professional capacity for enforcement (Guembe et al., 2022; Waizel, 2024). While much scholarly attention has focused on the adequacy of cybersecurity legislation in developing nations, considerably less research has examined whether the legal professionals responsible for interpreting and enforcing these laws possess the requisite knowledge to do so effectively.

Pakistan offers a compelling case study in this regard. The country's primary legal instruments for combating cybercrimes the Electronic Transactions Ordinance (ETO) 2002 and the Prevention of Electronic Crimes Act (PECA) 2016 provide a relatively comprehensive statutory framework. PECA 2016, in particular, addresses unauthorized access and data interference (Sections 3–5), offenses against critical infrastructure (Sections 6–8), terrorism-related cyber offenses (Section 9), electronic forgery and fraud (Sections 13–14), identity theft (Section 16), privacy and dignity violations (Sections 20–21), cyberstalking (Section 24), and spamming (Section 25). In principle, these provisions are sufficiently broad to encompass many AI-related cybercrime scenarios, including deepfake fraud, AI-automated phishing, and AI-assisted identity theft.

However, the existence of a legal framework is a necessary but insufficient condition for effective cybercrime governance. Laws are only as effective as the professionals who enforce them. If lawyers, judges, and law enforcement officers lack awareness of AI technologies, their associated threats, and the legal instruments available to address them, then the law remains a dormant instrument present in statute but absent in practice. This paper investigates the extent of this potential “enforcement gap” by surveying legal professionals in Karachi, Pakistan, regarding their knowledge of AI, their awareness of AI-related cybersecurity threats, their familiarity with relevant legislation, and their views on the need for professional education and legislative reform.

This study is derived from the LLM thesis of Ahtashamul Hassan Narejo at the Shaheed Zulfiqar Ali Bhutto University of Law, Karachi, under the supervision of Mujeeb-u-Rehman Khuhro. It addresses the following research questions: (1) What is the level of AI familiarity and threat awareness among legal professionals in Karachi? (2) What proportion of legal professionals are aware of Pakistan's existing cybersecurity legislation? (3) Is there a statistically significant relationship between AI familiarity, concern about AI misuse, and the perceived importance of professional education?

## **2. Literature Review**

### **2.1 AI-Driven Cybercrimes: An Evolving Landscape**

The integration of AI into cybercriminal operations has fundamentally shifted the threat landscape. AI-powered phishing leverages machine learning to generate personalized, context-aware communications that are significantly harder for recipients to identify as fraudulent (Waizel, 2024). Deepfake technology, which uses generative adversarial networks (GANs) to synthesize hyper-realistic audio and video, has emerged as a particularly potent tool for social engineering, enabling financial fraud through voice impersonation and political manipulation through fabricated video content (Westerlund, 2019; Sharma & Kaur, 2022). AI-enhanced malware employs polymorphic code generation to evade traditional signature-based detection, while AI-driven

botnets coordinate large-scale distributed denial-of-service (DDoS) attacks with unprecedented efficiency (Guembe et al., 2022).

Social engineering, broadly defined as the exploitation of human psychological vulnerabilities to obtain unauthorized access or information, has historically been among the most effective categories of cyberattack (Hatfield, 2018). The addition of AI amplifies every dimension of social engineering: reconnaissance is automated through data scraping, pretexts are crafted using natural language generation, and impersonation is enabled through deepfake synthesis. The result is a class of threats that are simultaneously more sophisticated, more scalable, and more difficult to detect than their pre-AI predecessors.

## **2.2 Pakistan's Cybersecurity Legal Framework**

Pakistan's legislative approach to cybercrimes has progressed through several stages. The Electronic Transactions Ordinance (ETO) 2002 established the legal validity of electronic records and digital signatures and addressed foundational offenses such as providing false information, privacy invasion, and unauthorized data alteration. The Prevention of Electronic Crimes Act (PECA) 2016 represented a major legislative advancement, providing a comprehensive penal framework that criminalizes a wide range of cyber offenses. PECA's provisions are, in many respects, sufficiently flexible to address AI-related crimes: deepfake creation and distribution can be prosecuted under sections relating to electronic forgery (Section 13), identity theft (Section 16), and privacy violations (Section 20); AI-powered phishing falls under fraud provisions (Section 14); and the use of AI to create or deploy malicious software is addressed by Section 15.

Despite this legislative breadth, multiple scholars have noted the gap between Pakistan's cybercrime statutes and their practical enforcement (Kundi et al., 2014; Magalla, 2018). The reasons for this gap are multifaceted: limited investigative capacity, insufficient technical expertise within law enforcement and the judiciary, low public reporting rates driven by lack of awareness, and the rapid evolution of AI technologies that outpaces legislative updates. This study focuses on one critical dimension of this enforcement gap the knowledge and preparedness of legal professionals themselves.

## **2.3 The Role of Legal Professionals in Cybersecurity Governance**

Legal professionals occupy a unique position in the cybersecurity ecosystem. Lawyers advise victims on their rights and available remedies, draft complaints and petitions, and represent parties in cybercrime prosecutions. Prosecutors must understand the technical mechanisms of AI-driven attacks to build effective cases. Judges must assess the admissibility and weight of digital evidence and interpret statutory provisions in the context of rapidly evolving technologies. If any of these professionals lack foundational knowledge of AI and its associated threats, the entire chain of legal recourse is compromised. This concern is not unique to Pakistan; studies across developing and developed nations have highlighted the need for legal professionals to acquire technological competency as a core professional skill (Surden, 2019).

# **3. Methodology**

## **3.1 Research Design and Sample**

This study employed a quantitative, survey-based research design within an empirical (non-doctrinal) legal research framework. A structured questionnaire consisting of 16 items was administered to legal professionals in Karachi. A total of 96 valid responses were collected through both print and online (Google Forms) distribution. The sample comprised 82 lawyers (85.4%), 9

respondents in other legal roles (9.4%), 3 law enforcement officers (3.1%), and 2 legal researchers (2.1%).

### **3.2 Questionnaire Design**

The questionnaire was designed to capture four domains: (1) demographic and professional background (age, gender, education, occupation, years of experience); (2) familiarity with AI and its applications; (3) awareness and concern regarding AI-related cybersecurity threats; and (4) familiarity with and attitudes toward Pakistan's cybersecurity legislation and the need for professional education. Each question was specifically linked to the study's research objectives, ensuring that the instrument systematically addressed all dimensions of the enforcement gap.

### **3.3 Data Analysis**

Descriptive statistics were used to summarize response distributions. Bivariate Pearson correlation analysis was performed on four key variables: AI familiarity (LP6), concern about AI misuse (LP9), perceived effectiveness of existing laws (LP12), and perceived importance of AI education for legal professionals (LP16). Scale reliability was assessed using Cronbach's Alpha.

## **4. Results**

### **4.1 Professional Profile**

The respondent pool was overwhelmingly composed of practicing lawyers (85.4%), providing high relevance to questions about legal awareness and enforcement capacity. The sample included professionals across experience levels, ensuring representation of both junior and senior practitioners.

### **4.2 AI Familiarity and Threat Awareness**

Approximately 48% of legal professionals reported being "very familiar" with AI, while 37.2% were "somewhat familiar" and the remainder had limited or no familiarity. When asked about awareness of legal issues or risks associated with AI, 63.2% answered in the affirmative while 36.8% were unaware. Regarding concern about the potential misuse of AI in cybercrimes and social engineering, 50.5% were "very concerned," 28.4% were "somewhat concerned," 13.7% were "not very concerned," and 7.4% were "not at all concerned." The fact that over 21% of legal professionals expressed minimal or no concern about AI-related cybercrimes is notable, given the professional obligation of this group to understand and respond to emerging crime typologies.

**Table 1: Summary of Legal Professionals' AI Knowledge and Attitudes (N = 96)**

| <b>Survey Item</b>                                     | <b>Affirmative (%)</b> | <b>Negative (%)</b> |
|--------------------------------------------------------|------------------------|---------------------|
| Very familiar with AI                                  | 47.9%                  | 52.1%               |
| Aware of legal risks of AI                             | 63.2%                  | 36.8%               |
| Very concerned about AI misuse                         | 50.5%                  | 7.4%                |
| Aware of AI-related laws in Pakistan                   | 50.0%                  | 50.0%               |
| Believe new/updated AI laws are needed                 | 88.3%                  | 11.7%               |
| AI education for legal professionals is very important | 82.4%                  | 5.5%                |

### 4.3 Legislative Awareness: The Enforcement Gap

The most consequential finding of this study pertains to legislative awareness. When asked whether they were familiar with any specific laws or regulations in Pakistan that address AI-related threats, exactly 50% of legal professionals responded “No.” This finding is both striking and deeply consequential: half of the professionals whose role includes the application and enforcement of these laws are unaware of their existence. This result empirically confirms the existence of a significant enforcement gap within Pakistan’s legal system.

Despite this lack of awareness, 88.3% of respondents believed that new or updated laws are needed to address AI-related threats. As the original thesis astutely observes, this high demand for new legislation may partly be driven by ignorance of existing laws respondents who are unaware that PECA 2016 exists would naturally call for new statutes to fill what they perceive as a legislative vacuum. This finding highlights that the primary gap may be not in the law itself but in professional awareness and application of existing legal instruments.

### 4.4 Demand for Professional Education

The demand for AI-related education among legal professionals was overwhelming. When asked how important it is for legal professionals to be educated about AI and its potential risks, 82.4% answered “very important” and 12.1% answered “somewhat important,” yielding a combined 94.5% endorsement. This near-universal recognition of the need for professional development provides a strong mandate for institutional action by bar associations, law schools, and government training bodies.

### 4.5 Correlation Analysis

Bivariate Pearson correlation analysis revealed the following significant relationships:

**Table 2: Pearson Correlation Matrix for Legal Professional Variables (N = 98)**

| Variable                             | LP6    | LP9    | LP12  | LP16   |
|--------------------------------------|--------|--------|-------|--------|
| <b>LP6 (AI Familiarity)</b>          | 1.000  | .461** | -.050 | .174   |
| <b>LP9 (Concern about AI Misuse)</b> | .461** | 1.000  | -.002 | .276** |
| <b>LP12 (Law Effectiveness)</b>      | -.050  | -.002  | 1.000 | .185   |
| <b>LP16 (Education Importance)</b>   | .174   | .276** | .185  | 1.000  |

\*\*  $p < 0.01$  (2-tailed)

The strongest correlation in the dataset was between AI familiarity (LP6) and concern about AI misuse (LP9), at  $r = 0.461$ ,  $p < 0.001$ . This robust positive relationship indicates that legal professionals who possess a deeper understanding of AI technology are significantly more likely to recognize and be concerned about its potential for misuse in cybercrimes and social engineering. A second significant correlation was found between concern about AI misuse (LP9) and the perceived importance of professional education (LP16), at  $r = 0.276$ ,  $p < 0.01$ . This establishes a positive feedback loop: knowledge drives concern, and concern drives demand for education.

Notably, the perceived effectiveness of existing laws (LP12) showed no statistically significant correlation with any other variable. This isolation of LP12 from the other constructs is itself informative it suggests that opinions about legal effectiveness may be based on general sentiment rather than on informed assessment of the actual legal provisions, consistent with the finding that 50% of respondents are unaware of these laws.

The reliability analysis yielded a Cronbach's Alpha of 0.445, which is below the conventional threshold of 0.700. This indicates low internal consistency among the four items, confirming that they measure distinct dimensions of professional knowledge rather than a single unified construct. The findings should therefore be interpreted as exploratory rather than confirmatory.

## **5. Discussion**

### **5.1 The Enforcement Gap: Law Without Awareness**

The central finding of this study that 50% of legal professionals are unaware of any specific laws in Pakistan addressing AI-related threats has profound implications for the country's cybersecurity governance. Pakistan's PECA 2016, while not perfect, provides a substantive legal arsenal for prosecuting many categories of AI-enabled cybercrime. Its provisions on electronic forgery, identity theft, malicious code, and privacy violations are directly applicable to deepfake fraud, AI-powered phishing, and other emerging threat types. Yet these tools remain dormant if the professionals responsible for wielding them are unaware of their existence.

This enforcement gap operates at multiple levels. Lawyers who do not know about PECA cannot advise cybercrime victims of their legal remedies. Prosecutors unfamiliar with the Act's provisions may fail to bring charges or may pursue cases under less appropriate statutes. Judges without foundational AI knowledge may struggle to evaluate technical evidence or interpret statutory provisions in the context of novel technologies. The cumulative effect is a legal system that, despite possessing adequate statutory tools, lacks the institutional capacity to deploy them effectively against AI-powered threats.

### **5.2 Knowledge as a Driver of Concern and Preparedness**

The strong positive correlation between AI familiarity and concern about AI misuse ( $r = 0.461$ ) carries an important practical implication: education does not merely fill a knowledge deficit; it actively catalyzes professional engagement with the issue. Legal professionals who understand AI are more alarmed by its potential for abuse, and that alarm translates into demand for further education ( $r = 0.276$  between concern and perceived education importance). This positive feedback loop suggests that even modest initial investments in AI education for legal professionals could generate cascading benefits, as early exposure triggers deeper engagement and advocacy for institutional change.

### **5.3 The Call for New Laws Versus Awareness of Existing Ones**

The finding that 88% of respondents believe new or updated laws are needed, while 50% are unaware of existing ones, presents a nuanced interpretive challenge. On one hand, the rapid evolution of AI technologies may indeed necessitate legislative updates for example, PECA 2016 does not explicitly address deepfake technology or algorithmic manipulation as distinct offense categories. On the other hand, a significant portion of the demand for new legislation may stem from ignorance of existing provisions rather than from a considered assessment of their adequacy. This suggests that before investing legislative energy in new statutes, a more immediate and cost-effective intervention would be comprehensive professional education on the existing legal framework, allowing informed assessments of where genuine legislative gaps exist.

### **5.4 Comparative Context**

Pakistan's enforcement gap is not unique. Legal systems globally are grappling with the challenge of keeping pace with AI-driven threats. However, the scale of the gap in Pakistan is notable. In more developed legal systems, continuing professional development (CPD) requirements typically

mandate technology-related education for practicing lawyers. Pakistan's bar associations and legal regulatory bodies have not yet systematically addressed this need, leaving the profession unprepared for a threat category that is growing exponentially.

### **5.5 Limitations**

This study has several limitations. The sample ( $N = 96$ ) was geographically limited to Karachi, which, while Pakistan's largest legal market, may not represent the knowledge levels of legal professionals in smaller cities and rural areas. The low Cronbach's Alpha (0.445) indicates that the four analyzed variables measure distinct constructs, limiting the ability to derive composite scores. The original thesis also included a combined cross-population correlation table that improperly merged data from two distinct populations (general public and legal professionals); this study appropriately restricts its analysis to the legal professional dataset alone. Finally, self-reported familiarity may overstate actual knowledge, as respondents may conflate superficial exposure with substantive understanding.

## **6. Conclusion and Recommendations**

This study empirically demonstrates the existence of a significant enforcement gap within Pakistan's legal profession regarding AI-related cybersecurity threats. Despite the availability of substantive legal tools in PECA 2016 and the ETO 2002, half of the surveyed legal professionals in Karachi are unaware of these instruments. The correlation analysis confirms that knowledge is a powerful catalyst: legal professionals who understand AI are more concerned about its misuse and more convinced of the need for professional education. The overwhelming demand for AI-related education (94.5%) provides a clear institutional mandate.

Based on these findings, the following recommendations are advanced:

First, the Pakistan Bar Council and provincial bar associations should introduce mandatory Continuing Legal Education (CLE) modules on AI, cybersecurity, and digital evidence. These modules should cover the technical fundamentals of AI and machine learning, the typology of AI-driven cybercrimes, the relevant provisions of PECA 2016 and other applicable statutes, and the principles of digital forensics and evidence admissibility.

Second, law schools across Pakistan should integrate AI and cybersecurity law into their core curricula at both LLB and LLM levels, ensuring that future legal professionals enter the profession with foundational technology literacy.

Third, the Federal Investigation Agency (FIA)'s Cyber Crime Wing should develop training programs for prosecutors and investigating officers specifically focused on AI-related offense types and evidence-gathering methodologies.

Fourth, the government should consider establishing a National Cybersecurity Legal Resource Center that provides legal professionals with regularly updated guidance on the application of existing laws to emerging AI threats, reducing the need for frequent legislative amendments.

Fifth, while the existing legal framework is more comprehensive than many professionals realize, targeted legislative refinements should be considered in particular, explicit provisions addressing deepfake creation and distribution, AI-generated disinformation, and the admissibility standards for AI-related digital evidence.

The AI-driven threat landscape will only accelerate. Pakistan's legal system possesses the statutory foundation to respond; the critical task now is to ensure that the professionals who operate within that system are equipped with the knowledge and competence to do so effectively.

## **References**

1. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence*, 36(1), 2037254.
2. Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102–113.
3. Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, 4(4), 61–71.
4. Magalla, A. (2018). Prevention and detection of cyber crimes in Tanzania as described by Cyber Crime Act, No. 13 of 2015.
5. Rawal, B. S., Eberhardt, G., & Lee, J. (2016). Cybersecurity snapshot: Google, Twitter, and other online databases. *Journal of Advanced Computer Science & Technology*, 5(1), 14–22.
6. Sharma, M., & Kaur, M. (2022). A review of Deepfake technology: An emerging AI threat. *Soft Computing for Security Applications: Proceedings of ICSCS 2021*, 605–619.
7. Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, 35(4).
8. Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. *Proceedings of TRUST Conference*.
9. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11).