Artificial Intelligence for Cybersecurity: Analyzing Legal Frameworks and Policy Implications

Muath Mohammed Alashqar[1], Haider Abdulrazaq Hameed[2] and Qusay Kanaan Kadhim[3]
[1]Faculty of Law and Judicial Practice, University of Palestine, 00970 Gaza City, Palestine
[2]Department of Administrative and Financial Affairs, University of Diyala, 32001 Baqubah, Iraq
[3]Department of Computer Science, University of Diyala, 32001 Baqubah, Iraq
muathalashqar@gmail.com, dr.haidarabd@uodiyala.edu.iq,dr.qusay.kanaan@uodiyala.edu.iq

Keywords: Cybersecurity, Artificial Intelligence, Legal Frameworks, Machine Learning, Deep Learning.

Abstract: The paper deeply studies three existing security mandates like the GDPR, NIST CSF, and CCPA so it can evaluate properly how they respond to Artificial Intelligence (AI) defines issues. The research finds significant problems in regulations about AI cybersecurity especially with attacks from outside sources, biased systems, and poor clarity, which create serious ethical problems. A doctrinal and analytical research methodology was applied within this study, which combines legal text analysis and case law review to define judicial rulings along with a framework evaluation and an investigation into social-moral effects on AI cybersecurity. In addition, actual data is collected from legal practitioners, IT security specialists, and policymakers through structured interviews to present a concrete approach of practical problems and regulatory requirements in an ever-growing field of this nature. The results stress the demand for powerful, proactive laws that make security demands and technological development compatible to each other, and emphasize the need for international collaboration and preventive regulatory approach. The recommendation for comprehensive legislative framework in regulating AI in cybersecurity is the concluding part of the study, seeking to promulgate laws that would weave its way through the makeovers engineered by AI in protecting cyber space, including realizing balance, practicality, and ethical vigilance.

1 INTRODUCTION

In 2024 cyber assault of corporations has foreseen international damage of greater than $1 trillion and emphasizes need for powerful cybersecurity strategies [1]. AI has highly developed before long and strongly affected various sphere; cybersecurity has been among the most severely affected [2]. AI technologies are widely applied in cybersecurity because it allows sophisticated threat detection [3]. AI integration in cybersecurity develops improved methods for both security maintenance and threat management systems. There are problems with existing legal structures together with policy. Threats continue growing in both number and complexity as data infrastructure along with organizational assets together with individual information remains endangered constantly. Solar Winds hack being combined with Colonial Pipeline ransomware attack shows that big destructive outcomes are possible due to cybersecurity incompetence [4].

AI legal Frameworks as the importance is intensifying rapidly the area of new technology AI therefore it insists the construction of separate legal system to manage the quantity and challenges presented with such technological devices. The current widest AI legislation proposal comes from the European Union (EU) with its AI Act presented in 2021 [5]. The EU AI Act sets risk categories that organize AI applications as unacceptable risk, high risk, restricted risk, and minimal risk applications respectively. The Act is to that extent preventive, for it presages dangers not yet or not apparent at the time. This prophylactic regulation will ensure the safety and reliability of AI systems; but it is important to understand the issues that occur when carrying out AI regulation and possible the negative impacts on innovation resulting from overly burdensome laws [6]. The FDA recommends on AI and Machine Learning (ML) in medical devices that is an instance of this. These recommendations in particular, emphasize on openness and post market surveillance (FDA) [7].

According to the Federal Trade Commission (FTC), data security and privacy are the key components in preventing deceptive and unfair practices related to the deployment of AI [8]. Customized legislation can be devised through the sectorial approach, so that sometimes regulatory inconsistencies and fragmentation may result making it difficult for firms operating under a number of sectors to comply [9].

There remains an effort to only have the enough regulations that can primarily regulate AI. The rapid pace of the development far outpaces that of regulatory development, leading to loopholes and outdated models [10]. Additionally, seeing as AI technology is virtually without border, it therefore requires international collaboration and harmonized legislative efforts to limit regulatory arbitrage and to establish unified standards[11].

2 LITERATURE REVIEW

The cybersecurity laws are composed of multiple national and international regulatory standards that carry different legal backgrounds and objectives. A study of the General Data Protection Regulation (GDPR) identifies how this set of rules deals with modern cybersecurity threats as well as its area of effectiveness and limitations [12].GDPR enhances data protection rules in the EU along with promoting privacy culture through accountability thus leading to elevated data protection standards. The rigorous regulatory standards appear problematic mainly to small businesses because they have limited resources to implement these requirements completely [13].The GDPR offers two key benefits through safeguarded confidentiality as well as clear standards and responsible practices for organizations. SMEs together with other organizations face difficulties with elevated GDPR standards and linked expenses since the GDPR delivers overall benefits.

Organizations from the US especially embrace this framework because its adaptable nature enables customization of cybersecurity approaches to fit individual organizational requirements and this solution proves very popular among U.S. businesses including SMEs [14]. Unlike the European Union GDPR mandatory data protection rules [15], the NIST framework enables businesses of various types to participate through its flexible approach although it remains optional [16]. The NIST framework takes a risk-based cybersecurity approach yet its voluntary nature reduces its value in protecting against new security threats because compliance success relies mostly on organizational commitment.

It changes the worldwide international frameworks’ policy shift to adapt to data privacy, governmental authority and to reconcile them with cybersecurity in several strategies. The Cybersecurity Law of China, enacted in 2017, emphasizes governmental authority in protecting data and network security, sometimes placing national objectives above personal private rights [17]. While this legislation exhibits a very different approach than the GDPR, which places emphasis on the protection of individual privacy, the use of national interests as a factor in governing the use of data reveals the impact of national interests on data governance regulations [18]. The stringent data sharing restrictions imposed by the GDPR show how striving for cybersecurity goals in different jurisdictions presents great challenges, particularly where the global cyber threats now require international cooperation for a coordinated response [19].

One of the first worldwide attempts to develop an international approach to cybercrime is the Budapest Convention on Cybercrime, which was set up in 2001. The aim of the agreement is to bring rules on the use of the internet in line internationally and improve the ability of countries to work together to investigate crimes online, but it has been criticized for failing to be properly implemented and for lack of strong backing from major players in cyberspace like Russia and China. However, existing frameworks are criticized for being weak in the enforcement and are not linked to the shared national agendas, as the critics argue they promote norms and collaboration [20]. The difference in the international collaboration and enforcement demonstrates persisting challenge of creating universally acknowledged cybersecurity legal framework [21].

The Cybersecurity, then, is improved because of AI with the use of sophisticated ML and deep learning (DL) techniques, for it makes analysis in big data better, and alarms occurrence faster, including eventualities that man could not notice [22]. AI-powered scored cybersecurity solutions to analyze a large throughput data much better than those done by the human in identifying the anomalies and potential threats in occurring [23]. The merging of AI with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) has greatly provided chances in detecting and preventing complex cyber threats, a progress over previous techniques [24].

The detection of AI system vulnerabilities requires robust protective strategies that need continuous monitoring to stop exploitation as well as maintain AI cybersecurity systems security integrity [25]. In this environment, employing AI produces several issues that concern government monitoring and liability when technology is utilized by businesses along with such autonomous systems more than people can account for and pay attention to [26]. Additionally, using AI in cybersecurity has a huge concern on data privacy, algorithm transparency and equity that are legal practice area necessary to make sure that it follows the ethics and avoid a person’s rights being violated. If AI is misused in surveillance, overly extensive interference in the individual privacy rights may occur in violation with the rules of data protection [27]. Since AI systems that are driven by flawed datasets tend to make discriminatory decisions that disproportionately favoring the underprivileged groups [28].Consequently, guaranteeing the transparency, equity, and accountability of AI applications in cybersecurity is both a technological necessity and a legal and ethical responsibility.

Despite the potential for great improvement in cybersecurity capabilities and the effectiveness of cybersecurity measures, the risks of adversarial attacks must be addressed, data privacy regulations must be complied with, and the potential for algorithmic bias must be defended to achieve sound and ethically appropriate use of AI.

3 RESEARCH METHODOLOGY

This study investigates the inclusion of AI into cybersecurity and its repercussions under existing. Doctrinal approach has been used to analyze a number of important legal documents and to investigate them including the GDPR the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the California Consumer Privacy Act (CCPA). The analysis of case law in AI and cybersecurity scientifically interprets and executes the meanings of legal laws with respect to judicial decisions that create precedents. This study also contains the stakeholders' obligations and viewpoints assessment. Socio legal research on the ethical and social consequences of AI for cybersecurity in particular aims to understand concerns around bias, transparency, as well as its implications for privacy rights and civil liberties. Consequently, empirical research is carried out through structured interviews with legal experts as well as cybersecurity professionals and policymakers. Such practice is done to gain fine-grained insights on how legal frameworks could be practically applied and have consequences. By conducting structured interviews, we received a large amount of data regarding obstacles, rewards and compliance issues experienced by different stakeholders. Normative analysis identifies significant deficiencies and difficulties in existing legal structures, and proposes new laws as appropriate. In addition, this analysis presents future research direction for the continuous adjusting legal framework to accommodate increasing technology advancement and increased cybersecurity threats. The research aims to approach the problems of the regulatory space where AI and cybersecurity interact as one whole, in a comprehensive way. It also aims to offer well-supported recommendations on how this landscape can be changed. Figure 1 illustrates the research method framework used in this study.

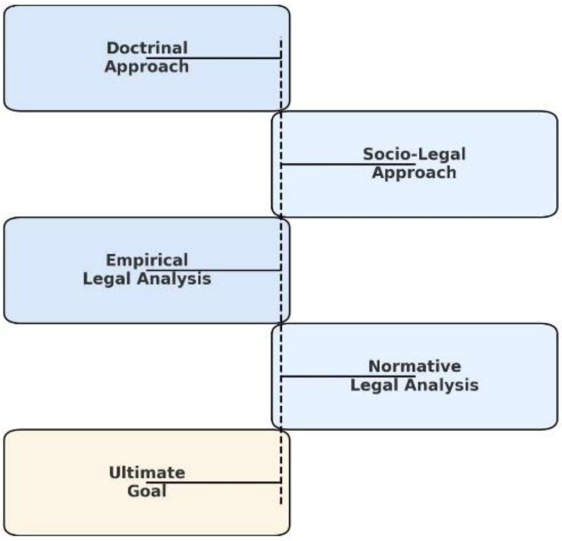

Figure 1: Research method framework.

4 ANALYSIS OF LEGAL FRAMEWORKS

4.1 Cybersecurity Laws and Regulations

In the area of cybersecurity, the laws and regulations are very important in order to expose sensitive information and minimize the risks of cyberattacks. Several key legislative frameworks can be illustrated as the myriad ways taken around the world’s congress.

Furthermore, the act forced people to disclose their actions within seventy two hours [29]. Therefore, the (GDPR) has brought about significant improvement to processes and concerning data protection and responsibility awareness. It may be effective for its being comprehensive and obligatory. In a sense, there is a need to set up a robust data security system in enterprises and the fines as a result are very high if the compliance is not met.

California Consumer Privacy Act (CCPA): Starting from 2020 consumers across California will gain CCPA access to view their data and request data deletion and data usage opt-out rights according to Section 1798.100 [30]. As per Section 1798. 100 of the California Civil Code businesses need to maintain protective security systems that handle personal information from their consumers. The United States of America now provides advanced data protection through the CCPA that both safeguards user information extensively while improving collection procedures [31]. The CCPA has personal information privacy as a major strength because it functions as legislation that protects consumers thoroughly.

The tasks that are included in the framework are Identify, Protect, Detect, Respond, and Recover [32]. Because of the framework's adaptability, it is extremely adaptable for various organizations to implement it according to their requirements, which has contributed to its widespread use in a variety of business domains (NIST, 2018). The flexibility of the framework is advantageous, but the absence of strict compliance results in diverse cybersecurity measures [33].

4.2 Legal Frameworks Related to AI

Different jurisdictions across the globe are creating regulations regarding AI technologies to handle unique AI issues together with possible risks through established frameworks.

The EU AI Act uses risk levels to sort AI systems and establishes strict standards for managing high-risk systems [34]. These standards include comprehensive policies together with activities for openness as well as human supervision systems and protective measures against cyberattacks and exploitation [35]. AI systems must be made safe and dependable by legislation that also protects basic rights throughout operations. The EU aims for standardized regulations across all member states by means of this policy [36]. This law achieves high effectiveness due to its proactive approach that stops potential issues from spreading before their full growth.

Under the U.S. Sectorial Approach, each specialized regulatory agency within the country develops specific rules for individual sectors. The system of regulatory oversight can be described as decentralized because different bodies handle the regulation of AI technologies that match the specific sector they serve. The Food and Drug Administration (FDA) has established particular guidelines regarding AI and ML in medical devices (MDs) which focus on visibility requirements and testing procedures and post-market monitoring for patient protection and effective use of the devices [37]. The Federal Trade Commission (FTC) ensures consumer protection through enacting regulations to prevent the act of fraudulent activities in AI technology, with matters related to data protection, algorithmic bias and helps to promote transparency with regard to the AI's impact on consumers. The framework provides organizations with a standardized method to detect, analyze, and manage possible hazards caused by AI while acting as a directive tool.

In China, the strategy is centralized. The government unifies its AI regulations in form of comprehensive regulations. China’s 2017 Next Generation AI Development Plan aims to make China the leading AI power in the world by 2030. The strategy focuses on three core priorities that include ethics as well security concerns and societal impact. AI research and practice need ethical norms and legal frameworks that their representatives argue should be established [38]. These tactics enable China’s plan through rapid well-coordinated regulatory measures that prompt the setting of clear and adequate standards that can quickly respond to technological characteristics.

4.3 Gaps and Challenges

There are several notable gaps and inconsistencies in the current legal frameworks governing AI and cybersecurity:

1) Lack of International Harmonization. This situation comes about because of lack of alliance in among global lawful organizations that thus causes deficient coordination. This fragmented nature is, however, susceptible to regulatory arbitrage in which entities leverage the fragmented nature to exploit the most rigorous set of regulations whilst maximizing profits posed considerably compliance problems for multinational organizations. Cyber threats are global in scope and cybersecurity legislation should therefore be one, with universal protections so as not to have any gaps in the legislation.
2) Outdated Regulations. The fast pace of technological development makes it difficult for law enforcement to produce current regulatory frameworks. The rules that emerge tend to be spread out over many pages despite their inability to address effectively the security and AI-related threats which advanced technologies create [39]. Standards should require special protection solutions because current ML security methods can be easily defeated.

4.4 Regulatory Challenges

Regulating AI within cybersecurity presents multiple complex challenges:

1) Technological Advancements. AI technology is evolving quite fast, which makes the process of regulating it quite a challenging task. The

reaction tends to become such, which creates legal uncertainty while exposing systems to novel risks. In order to do this, regulatory approaches must make use of innovative methods in order to adequately anticipate technical shifts and embed adaptive means to ensure compliance with high cybersecurity norms. It seems regulations for AI and risks associated with AI would make more sense if they were periodically reviewable [40].

2) Ethical Dilemmas. Ethics in AI technology creates several difficult problems to solve such as implicit bias, personal responsibility and open actions. Governments should create laws that let people observe how AI systems work and need them to act fairly to win public faith in the system. To build trust with the public we need to make sure AI systems avoid receiving and spreading existing unfair practices. For AI systems to use the technology companies have to prove that their systems will not be biased during tests and validations before public use [41].
3) Privacy Concerns. There are serious privacy issues when relating AI to data analysis and surveillance. Laws that are effective should contain strong safeguards for the individual privacy while permitting the beneficial use of tools using AI. This includes further questions of ensuring that data protection legislation is not broken and that procedures are transparent in order to maintain public trust. Keeping in mind the benefits of data analysis of personal information with the need to prevent the misuse of surveillance. In the end all that is required is a guarantee of privacy with measures such as affirmative consent and data minimization practices [42].
4) Human Oversight. It is important to ensure that humans are active in managing the risk associated with uses of AI, are responsible for AI systems. In some cases however, certain ethical, legal standards require critical AI driven decisions to be reviewed by humans [43]. Current laws regarding both AI and cybersecurity form a crucial foundation for direct technological risk control yet prove insufficient against the complete range of issues expected from AI development speedups. Since the evolution of AI technology, regulators need to take proactive measures that combine with flexibility and review process with responsiveness in their regulatory strategies.

4.5 Legal Frameworks

The integration of AI into cybersecurity demands complex knowledge from policymakers because responsible implementation requires a thorough approach to AI-based cybersecurity. Through promotion of responsible development, equitable access and public trust, policymakers can reduce risks in the use of AI in cybersecurity, and enable the enhancement of the broader public value of AI in cyber. Thus, to accommodate the AI advancements policies must undergo some adjustments:

1) Harmonization of Regulations. For common international standards to be set for AI and cybersecurity, international cooperation is of importance to avoid fragmentation and to ensure that global standards are implemented uniformly by countries [44]. A regulatory framework that is globally aligned helps in reducing legal complexities of organizations operating outside the borders and promotes global cybersecurity awareness.
2) Proactive Regulation. It is important for policymakers to focus on proactive instead of reactive regulation, prepared to counter the potential risks of the technology emerging in AI. It requires constant monitoring, and updating of legal frameworks to render the regulations applicable [45].
3) Support for SMEs. Special help must reach small and medium-sized businesses because they need specific guidance to understand AI and cybersecurity permissions. Subsidies, grants and consultative services should be adjusted into the policy to help SMEs to comply with rigorous standards [46].
4) Ethical AI Development. Current ethical AI development should have precise legal prescriptions for procedures which focus on performance fairness while ensuring system clarity and maintenance accountability standards [47]. The laws must enforce full visibility in algorithm development principles as well as data management standards with safety protocols to monitor and prevent improper usage and maintain control of AI systems. The establishment of ethical protocols remains essential to earn public trust while safeguarding persons from possible damages of AI technology.
5) Privacy Protections. Data protection policies should be very effective and completely ban any form of unauthorized surveillance so as to

encourage public trust in AI systems [48]. This means the update of data protection laws that will incorporate privacy as a central principle in the development of AI, together with sanctions that can be enforced when there is a breach.

The integration of AI into cybersecurity creates difficulties and advantages that policymakers have to handle. The responsible utilization of AI technology to bolster cybersecurity requires governments to perform assessments related to legal impacts as well as social and economic aspects followed by regulatory framework modifications. Timely regulatory adjustments that enable adoption of AI technology allow the detection of emerging threats and utilization of its benefits to build a safer dynamic cybersecurity environment. Methods to update laws according to technology advances allow decision-makers to navigate complex AI security problems.

5 IMPROVEMENT OF LEGAL FRAMEWORK

Since the increasing complexity given by AI and cybersecurity, it is necessary to propose practical and target-based changes to existing legislation.

Strengthening to overcome these challenges, current legislation should be strengthened by updating with specific rules that take into consideration those specific rules that should apply for data protection in the case of AI. In particular, this should involve mandatory annual inspections of AI systems in terms of data protection policy, in order to reinforce data minimization, purpose limitation and accountability principles.

Improving transparency and explain ability: legal requirements for AI developers and operators should require that they perform the actions to make the functioning of AI more transparent and comprehensible. In other words, they may involve compulsory disclosure of decision making processes and algorithms and the development of a public database that reveals details about AIs, their models, and their decision-making processes.

Promote International Collaboration. The countries and take initiatives should adopt harmonized or compatible AI and cybersecurity regulations. There would be multilateral treaties and the formation of international organizations owning the duty to lay down standards in international level and promote international cooperation interstate.

Invest in Research. The public policy must allocate funds to support AI research along with cybersecurity innovation to guide capital toward educational institutions and technology development programs managed by the government.

6 CONCLUSIONS

Artificial intelligence (AI) is playing a very important role in augmenting the cybersecurity, especially for threat detection, anomaly detection and automated response protocols. Decision systems with AI improve cybersecurity but their implementation carries two main drawbacks that include adversarial vulnerability along with bias-related ethical issues and lack of transparency. The effective management of AI’s role in cybersecurity requires stringent safeguards because of the identified risks. Current laws prove insufficient since no national consensus exists on AI controls nor do the regulations match the present-day AI threats adequately.

This paper is an in-depth analysis of the integration of AI in cyber security with which is dealt a special focus of legal challenges and policies around the influences of AI in cyber security devices. Important findings of this Analysis Current Legal Frameworks: By way of example, significant legislative innovations, for example, European Union’s GDPR as well as CCPA in the United States, making headways privacy eligible data protection.

The paper adds important findings to AI and cybersecurity knowledge base. The paper examines current laws and policies through identification of implementation challenges organizations encounter when deploying AI-based cybersecurity tools. This study proposes specific recommendations for improving relevant legal frameworks together with security protocols that protect and make responsible the deployment of AI in cybersecurity systems.

In future research directions for developing the field of AI and cybersecurity, research should focus primarily on creating legal frameworks for emerging AI cyber threats along with creating universal global laws for AI and cybersecurity.

REFERENCES

[1] B. Saha and Z. Anwar, “A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework,” J. Inf. Secur., vol. 15, no. 01, pp. 24-39, 2024, [Online]. Available: https://doi.org/10.4236/jis.2024.151003.

[2] A. I. Altameemi, S. J. Mohammed, Z. Q. Mohammed, Q. K. Kadhim, and S. T. Ahmed, “Enhanced SVM and RNN Classifier for Cyberattacks Detection in Underwater Wireless Sensor Networks,” Int. J. Saf. Secur. Eng., vol. 14, no. 5, pp. 1409-1417, Oct. 2024,

[Online]. Available: https://doi.org/10.18280/ijsse.140508.

[3] L. A. Ogundele, F. E. Ayo, A. M. Adeleye, and S. O. Hassan, "A Hybrid Network Intrusion Detection Framework using Neural Network-Based Decision Tree Model," Int. J. Appl. Sci. (IJApSc), vol. 2, no. 1, pp. 74-93, Mar. 2025, [Online]. Available: https://doi.org/10.69923/95zt9v71.

[4] D. A. S. George, D. T. Baskar, and D. P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," Partners Univers. Int. Innov. J., vol. 2, no. 1, pp. 51-75, 2024, [Online]. Available: https://doi.org/10.5281/zenodo.10639463.

[5] J. Laux, S. Wachter, and B. Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk," Regul. Gov., vol. 18, no. 1, pp. 3-32, 2024, [Online]. Available: https://doi.org/10.1111/rego.12512.

[6] H. A. A. Mohammed, A. A. Kasim Jizany, I. M. Mahmood, and Q. K. Kadhim, "Predicting Alzheimer's Disease Using a Modified Grey Wolf Optimizer and Support Vector Machine," Ing. des Syst. d'Information, vol. 29, no. 2, pp. 669-676, 2024, [Online]. Available: https://doi.org/10.18280/isi.290228.

[7] V. V. Zinchenko et al., "Methodology for Conducting Post-Marketing Surveillance of Software as a Medical Device Based on Artificial Intelligence Technologies," Sovrem. Tehnol. v Med., vol. 14, no. 5, pp. 15-25, 2022, [Online]. Available: https://doi.org/10.17691/stm2022.14.5.02.

[8] M. James, "The Ethical and Legal Implications of Using Big Data and Artificial Intelligence for Public Relations Campaigns in the United States," Int. J. Commun. Public Relat., vol. 9, no. 1, pp. 38-52, 2024, [Online]. Available: https://doi.org/10.47604/ijcpr.2273.

[9] A. U. Akang, "Regulatory Compliance and Access To Finance: Implications for Business Growth in Developing Economies," Sci. J. Educ. Humanit. Soc. Sci., vol. 1, no. 2, pp. 8-23, 2024, [Online]. Available: https://doi.org/10.62536/sjehss.2023.v1.i2.pp8-23.

[10] A. Khalaf and K. Lakhtaria, "A Hybrid System Based on Three Levels to Hide Information using JPEG Color Images," Int. J. Appl. Sci. (IJApSc), vol. 1, no. 2, pp. 30-45, Sep. 2024, [Online]. Available: https://doi.org/10.69923/8rjqxq24.

[11] H.-W. Liu and C.-F. Lin, "Artificial Intelligence and Global Trade Governance: A Pluralist Agenda," Artif. Intell. Glob. Trade Gov. A Plur. Agenda, vol. 61, no. 2, p. 61, 2020, [Online]. Available: https://perma.cc/6ZFR-2LRT.

[12] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," Comput. Secur., vol. 120, p. 102820, Sep. 2022, [Online]. Available: https://doi.org/10.1016/j.cose.2022.102820.

[13] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales," Int. J. Inf. Manag. Data Insights, vol. 3, no. 2, p. 100191, Nov. 2023, [Online]. Available: https://doi.org/10.1016/j.jjimei.2023.100191.

[14] P. Permatasari and J. Gunawan, "Sustainability policies for small medium enterprises: WHO are the actors?," Clean. Responsible Consum., vol. 9, no. October 2022, p. 100122, Jun. 2023, [Online]. Available: https://doi.org/10.1016/j.clrc.2023.100122.

[15] C. Labadie and C. Legner, "Building data management capabilities to address data protection regulations: Learnings from EU-GDPR," J. Inf. Technol., vol. 38, no. 1, pp. 16-44, Mar. 2023, [Online]. Available: https://doi.org/10.1177/02683962221141456.

[16] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," Electronics, vol. 11, no. 14, pp. 1-20, Jul. 2022, [Online]. Available: https://doi.org/10.3390/electronics11142181.

[17] R. Creemers, "Cybersecurity Law and Regulation in China: Securing the Smart State," China Law Soc. Rev., vol. 6, no. 2, pp. 111-145, Mar. 2023, [Online]. Available: https://doi.org/10.1163/25427466-06020001.

[18] K. Yeung and L. A. Bygrave, "Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship," Regul. Gov., vol. 16, no. 1, pp. 137-155, Jan. 2022, [Online]. Available: https://doi.org/10.1111/rego.12401.

[19] E. Buçaj and K. Idrizaj, "The need for cybercrime regulation on a global scale by the international law and cyber convention," Multidiscip. Rev., vol. 8, no. 1, pp. 1-30, Sep. 2024, [Online]. Available: https://doi.org/10.31893/multirev.2025024.

[20] I. M. Alramamneh and A. Abuanzeh, "International and National Procedural Framework for Combating Cybercrime," Int. J. Cyber Criminol., vol. 17, no. 2, pp. 330-349, 2023, [Online]. Available: https://doi.org/10.5281/zenodo.4766719.

[21] A. Abdullahi and I. G. Musa, "The legitimacy of international law: challenges and the emerging issues," J. Glob. Soc. Sci., vol. 4, no. 16, pp. 14-34, Nov. 2023, [Online]. Available: https://doi.org/10.58934/jgss.v4i16.217.

[22] A. Abdulkarem and A. Krivtsun, "An Analysis of Automated Essay Scoring Frameworks," Int. J. Appl. Sci. (IJApSc), vol. 1, no. 3, pp. 71-81, Dec. 2024, [Online]. Available: https://doi.org/10.69923/av1gt264.

[23] Q. K. Kadhim, A. I. Altameemi, R. M. Abdulkader, and S. T. Ahmed, "Enhancement of Data Center Transmission Control Protocol Performance in Network Cloud Environments," Ing. des Syst. d'Information, vol. 29, no. 3, pp. 1115-1123, 2024, [Online]. Available: https://doi.org/10.18280/isi.290329.

[24] S. T. Ahmed and S. M. Kadhem, "Alzheimer's disease prediction using three machine learning methods," Indones. J. Electr. Eng. Comput. Sci., vol. 27, no. 3, pp. 1689-1697, 2022, [Online]. Available: https://doi.org/10.11591/ijeecs.v27.i3.pp1689-1697.

[25] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," J. Big Data, vol. 11, no. 1, pp. 1-38, Aug.

2024, [Online]. Available: https://doi.org/10.1186/s40537-024-00957-y.

[26] J. Afolabi, "Enhancing Cybersecurity Through Artificial Intelligence: Challenges and Opportunities," Researchgate, vol. 9, no. 1, pp. 50-67, 2024.

[27] R. Mühlhoff, "Predictive privacy: Collective data protection in the context of artificial intelligence and big data," Big Data Soc., vol. 10, no. 1, pp. 1-24, Jan. 2023, [Online]. Available: https://doi.org/10.1177/20539517231166886.

[28] M. Shahvaroughi Farahani and G. Ghasemi, "Artificial Intelligence and Inequality: Challenges and Opportunities," Qeios, vol. 2, no. 21, pp. 1-14, Feb. 2024, [Online]. Available: https://doi.org/10.32388/7HWUZ2.

[29] H. S. Mahdi Alsultani and A. H. Aliwy, "Boosting Arabic Named Entity Recognition with K-Fold Cross Validation on LSTM and Bi-LSTM Models," J. Comput. Sci., vol. 18, no. 9, pp. 792-800, Sep. 2022, [Online]. Available: https://doi.org/10.3844/jcssp.2022.792.800.

[30] V. P. Shehu and V. Shehu, "Human rights in the technology era – Protection of data rights," Eur. J. Econ. Law Soc. Sci., vol. 7, no. 2, pp. 1-10, Jun. 2023, [Online]. Available: https://doi.org/10.2478/ejels-2023-0001.

[31] I. Technology, "A comparative analysis between General Data Protection Regulations and California Consumer Privacy Act," J. Comput. Sci. Inf. Technol. Telecommun. Eng., vol. 4, no. 1, pp. 326-332, Mar. 2023, [Online]. Available: https://doi.org/10.30596/jcositte.v4i1.13330.

[32] I. Mishkhal, N. Abdullah, H. H. Saleh, N. I. R. Ruhaiyem, and F. H. Hassan, "Facial Swap Detection Based on Deep Learning: Comprehensive Analysis and Evaluation," Iraqi Journal for Computer Science and Mathematics, vol. 6, no. 1, pp. 109-123, 2025.

[33] K. Pipyros and S. Liasidou, "A new cybersecurity risk assessment framework for the hospitality industry: techniques and methods for enhanced data protection and threat mitigation," Worldw. Hosp. Tour. Themes, vol. 1, no. 1, pp. 1-14, Feb. 2025, [Online]. Available: https://doi.org/10.1108/WHATT-12-2024-0296.

[34] B. Solaiman and A. Malik, "Regulating algorithmic care in the European Union: evolving doctor–patient models through the Artificial Intelligence Act (AI-Act) and the liability directives," Med. Law Rev., vol. 33, no. 1, pp. 1-22, Jan. 2025, [Online]. Available: https://doi.org/10.1093/medlaw/fwae033.

[35] T. H. Hadi, J. Kadum, Q. K. Kadhim, and S. T. Ahmed, "An Enhanced Cloud Storage Auditing Approach Using Boneh-Lynn- Shacham ' s Signature and Automatic Blocker Protocol," Ingénierie des Systèmes d'Information, vol. 29, no. 1, pp. 261-268, 2024, [Online]. Available: https://doi.org/10.18280/isi.290126.

[36] S. L. Shaelou and Y. Razmetaeva, "Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values," ERA Forum, vol. 24, no. 4, pp. 567-587, Dec. 2023, [Online]. Available: https://doi.org/10.1007/s12027-023-00777-2.

[37] I. Mishkhal, S. A. AL Kareem, H. H. Saleh, A. Alqayyar, I. Hussein, and I. A. Jassim, "Solving Course Timetabling Problem Based on the Edge Coloring Methodology by Using Jedite," in 2019 1st AL-Noor International Conference for Science and Technology (NICST), Sulimanyiah, Iraq, 2019, pp. 68-72, [Online]. Available: https://doi.org/10.1109/NICST49484.2019.9043794.

[38] Y. Liu, W. Fu, and D. Schiller, "The making of government-business relationships through state rescaling: a policy analysis of China's artificial intelligence industry," Eurasian Geogr. Econ., vol. 00, no. 00, pp. 1-29, Aug. 2024, [Online]. Available: https://doi.org/10.1080/15387216.2024.2388890.

[39] H. S. M. Alsultani and A. H. Aliwy, "Improving Arabic Named Entity Recognition with a Modified Transformer Encoder," J. Comput. Sci., vol. 19, no. 5, pp. 599-609, May 2023, [Online]. Available: https://doi.org/10.3844/jcssp.2023.599.609.

[40] A. Drake et al., "Legal contestation of artificial intelligence-related decision-making in the United Kingdom: reflections for policy," Int. Rev. Law, Comput. Technol., vol. 36, no. 2, pp. 251-285, May 2022, [Online]. Available: https://doi.org/10.1080/13600869.2021.1999075.

[41] O. Akinrinola, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu, "Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability," GSC Adv. Res. Rev., vol. 18, no. 3, pp. 050-058, Mar. 2024, [Online]. Available: https://doi.org/10.30574/gscarr.2024.18.3.0088.

[42] M. Alkaeed, A. Qayyum, and J. Qadir, "Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: A survey," J. Netw. Comput. Appl., vol. 231, p. 103989, Nov. 2024, [Online]. Available: https://doi.org/10.1016/j.jnca.2024.103989.

[43] L. Cavalcante Siebert et al., "Meaningful human control: actionable properties for AI system development," AI Ethics, vol. 3, no. 1, pp. 241-255, Feb. 2023, [Online]. Available: https://doi.org/10.1007/s43681-022-00167-3.

[44] P. S. Dhoni, "Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity," TechRxiv, pp. 1-10, 2023.

[45] S. Reddy, "Global Harmonization of Artificial Intelligence-Enabled Software as a Medical Device Regulation: Addressing Challenges and Unifying Standards," Mayo Clin. Proc. Digit. Heal., vol. 3, no. 1, p. 100191, Mar. 2025, [Online]. Available: https://doi.org/10.1016/j.mcpdig.2024.100191.

[46] A. Papathanasiou, G. Liontos, A. Katsouras, V. Liagkou, and E. Glavas, "Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era," J. Inf. Secur., vol. 16, no. 01, pp. 1-43, 2025, [Online]. Available: https://doi.org/10.4236/jis.2025.161001.

[47] O. Hoxhaj, B. Halilaj, and A. Harizi, "Ethical Implications and Human Rights Violations in," Balk. Soc. Sci. Rev., vol. 22, pp. 153-171, 2023.

[48] O. F. Alwan, Q. K. Kadhim, R. B. Issa, and S. T. Ahmed, "Early Detection and Segmentation of Ovarian Tumor Using Convolutional Neural Network with Ultrasound Imaging," Rev. d'Intelligence Artif., vol. 37, no. 6, pp. 1503-1509, 2023, [Online]. Available: https://doi.org/10.18280/ria.370614.