ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Legal Professionals' Perspectives on the Challenges of Cybercrime Legislation Enforcement

Elvin Shukurov[1]*, Uzeyir Jafarov[2]

[1] Doctor of Philosophy in Law, Ibn Haldun University, Istanbul, Türkiye
[2] Faculty of Law, Ibn Haldun University, Istanbul, Türkiye

*** Corresponding author email address**: elvinshukurov@gmail.com

Received: 2023-07-03 **Revised:** 2023-08-02 **Accepted:** 2023-08-13 **Published:** 2023-10-01

This study aims to explore the perspectives of legal professionals on the enforcement challenges of cybercrime legislation. It seeks to identify the key challenges within the legal framework, operational enforcement, and strategic policy-making that hinder the effective combat of cybercrime. Employing a qualitative research design, the study conducted semi-structured interviews with 30 legal professionals, including prosecutors, defense attorneys, judges, and legal scholars. The participant selection was based on purposive sampling to cover a broad range of insights into the enforcement of cybercrime legislation. Data collection adhered to the principle of theoretical saturation, ensuring a comprehensive exploration of the subject matter. Thematic analysis was utilized to identify patterns and themes within the data. Three main themes emerged from the analysis: Legal Framework Challenges, Operational Enforcement Challenges, and Strategic and Policy Challenges. Within these themes, several categories were identified, including the ambiguity of laws, jurisdictional issues, technological evolution, resource constraints, digital evidence management, cybercrime reporting and detection, interagency cooperation, prevention and awareness, legal professionals' preparedness, policy development and implementation, stakeholder engagement, and future-proofing legislation. Each category was further broken down into specific concepts highlighting the multifaceted challenges in cybercrime legislation enforcement. The study reveals that legal professionals face significant hurdles in the enforcement of cybercrime legislation, stemming from legal ambiguities, operational limitations, and strategic gaps in policy-making. Effective enforcement requires addressing these challenges through clearer legal definitions, enhanced interagency cooperation, increased resources for digital evidence management, and forward-looking policy development. By addressing these issues, there is potential to significantly improve the effectiveness of cybercrime legislation enforcement.

Keywords: *Cybercrime legislation, Legal framework, Operational enforcement, Strategic challenges, Legal professionals*

How to cite this article:

Shukurov, E., & Jafarov, U. (2023). Legal Professionals' Perspectives on the Challenges of Cybercrime Legislation Enforcement. *Interdisciplinary Studies in Society, Law, and Politics, 2*(4), 25-31. https://doi.org/10.61838/kman.isslp.2.4.5

1. Introduction

Cybercrime, an increasingly prevalent threat in the digital age, poses unique challenges for the legal system, demanding both rapid responses and nuanced approaches to law enforcement and policy development. As Ajayi (2016) points out, the enforcement of cyber-crimes laws is fraught with difficulties, stemming from the inherent complexities of the internet and information systems (Ajayi, 2016). The transnational nature of cybercrime, coupled with the pace of technological advancements, complicates the legal landscape, as Calderoni (2010) emphasizes the struggle for an effective implementation of the European legal framework on cybercrime (Calderoni, 2010).

The perception and readiness of law enforcement officers to tackle cybercrime further compound these challenges. Bossler and Holt (2012) highlight the gap in patrol officers' perceived role in responding to cybercrime, indicating a need for enhanced training and resources (Bossler & Holt, 2012). Similarly, Cockcroft et al. (2018) underline the significance of perceptions, pedagogy, and policy in police cybercrime training, suggesting that effective training programs are crucial for equipping officers with the skills necessary to combat cybercrime effectively (Cockcroft et al., 2018).

Moreover, the collaboration between law enforcement and industry plays a pivotal role in regulating cybercrime, as discussed by Holt (2018). This partnership is essential for developing strategies that address the dynamic nature of cyber threats (Holt, 2018). However, Holt and Bossler (2012) identify a gap in patrol officers' interest in cybercrime training and investigation, pointing to the importance of fostering a strong commitment to understanding and fighting cybercrime within police departments (Holt & Bossler, 2012).

The legal framework itself requires scrutiny and adaptation to keep pace with the evolving digital threat landscape. Khan et al. (2022) provide a systematic literature review on cybercrime legislation, highlighting the diversity of approaches and the need for harmonization to enhance the effectiveness of legal measures (Khan et al., 2022). The challenge of connecting evidence-based policing with cybercrime strategies is also critical, as Koziarski and Lee (2020) argue for the integration of empirical evidence into policing practices to strengthen the fight against cybercrime (Koziarski & Lee, 2020).

The perspectives of detectives and specialists in the field offer valuable insights into the complexities of policing cybercrime. Lee et al. (2019) examine the views of English and Welsh detectives on online crime, shedding light on the practical challenges faced in investigation and prosecution (Lee et al., 2019). Paoli et al. (2020) further explore the knowledge, forensic, and legal challenges from the viewpoint of police cybercrime specialists, emphasizing the need for specialized knowledge and resources (Paoli et al., 2020).

Comparative analyses, such as the work of Lu et al. (2010), examine the differences in cybercrimes and governmental law enforcement efforts between countries like China and the United States, suggesting that international cooperation and the sharing of best practices are essential for effective cybercrime management (Lu et al., 2010). Nugroho and Chandrawulan (2022) discuss the implications of cybercrime laws in the context of COVID-19 in Indonesia, pointing out the lessons that both developed and developing countries can learn from this experience (Nugroho & Chandrawulan, 2022).

Finally, the human security dimensions of cybersecurity are becoming increasingly relevant, as Salminen and Hossain (2018) explore the impact of digitalisation on human security in the European High North (Salminen & Hossain, 2018). Trufanova (2023) also addresses the notion of cyberspace as a crime scene, presenting current trends, features, and prevention measures, and highlighting the need for comprehensive strategies that encompass legal, operational, and strategic dimensions (Trufanova, 2023).

Therefore, this study aims to explore the perspectives of legal professionals on the enforcement challenges of cybercrime legislation. It seeks to identify the key challenges within the legal framework, operational enforcement, and strategic policy-making that hinder the effective combat of cybercrime.

2. Methods and Materials

2.1. Study Design and Participants

This study employed a qualitative research design to explore the perspectives of legal professionals on the challenges associated with the enforcement of cybercrime legislation. The research was guided by the principle of theoretical saturation, aiming to understand the depth and complexity of the issues involved in cybercrime law enforcement.

Participants were selected using purposive sampling to ensure a diverse representation of legal professionals, including prosecutors, defense attorneys, judges, and legal scholars with expertise in cybercrime. The recruitment process was conducted through professional legal associations and networks, with an emphasis on including professionals with direct experience in cybercrime cases. A total of 30 participants were recruited for the study, ensuring a wide range of insights and perspectives on the enforcement challenges of cybercrime legislation.

The study adhered to the principle of theoretical saturation, whereby data collection continued until no new themes or insights emerged from the interviews. This approach ensured a comprehensive understanding of the legal professionals' perspectives on the topic. Theoretical saturation was achieved after 30 interviews, but five additional interviews were conducted to confirm the saturation point and ensure the robustness of the findings.

2.2. Measures

2.2.1. Semi-Structured Interview

Data were collected through semi-structured interviews, which allowed for in-depth exploration of participants' views and experiences. The interview guide was developed based on a review of existing literature on cybercrime legislation and its enforcement challenges. It included open-ended questions designed to elicit detailed responses on the effectiveness of current laws, enforcement barriers, and recommendations for improving cybercrime legislation enforcement. Interviews were conducted via secure online video conferencing platforms to accommodate participants' schedules and geographical locations, ensuring a broad and inclusive sample. Each interview lasted approximately 60 to 90 minutes and was recorded with the consent of the participants for transcription and analysis purposes.

2.3. Data Analysis

Transcribed interviews were analyzed using thematic analysis to identify and interpret patterns and themes related to the challenges of enforcing cybercrime legislation. The analysis began with a process of familiarization, where researchers immersed themselves in the data by reading and re-reading the transcripts. Initial codes were generated to identify features of the data relevant to the research questions. These codes were then collated into potential themes, which were reviewed and refined to form a coherent pattern. The themes were further analyzed in relation to the existing literature on cybercrime legislation and enforcement challenges. Trustworthiness and credibility of the analysis were ensured through a process of peer debriefing and member checking, where initial findings were shared with participants for feedback and validation.

3. Findings and Results

In this qualitative study exploring the challenges of cybercrime legislation enforcement, a total of 30 legal professionals were interviewed. The demographic composition of the participants was diverse, reflecting a range of experiences and backgrounds within the legal field. Of these participants, 12 (40%) were prosecutors with firsthand experience in handling cybercrime cases, highlighting the prosecutorial perspective on enforcement challenges. Defense attorneys, who play a crucial role in navigating the complexities of cybercrime law, constituted 8 (26.7%) of the interviewees. The study also included 5 (16.7%) judges, offering insights into the adjudication of cybercrime and the application of relevant laws. Furthermore, legal scholars, who contributed academic perspectives on the evolution and effectiveness of cybercrime legislation, made up the remaining 5 (16.7%) participants.

Table 1

The Results of Thematic Analysis

Categories	Subcategories	Concepts (Open Codes)
Legal Framework Challenges	1. Ambiguity in Laws	- Lack of clear definitions- Overly broad terms- Outdated provisions
	2. Jurisdictional Issues	- Cross-border enforcement challenges- Conflicts of law- Lack of international cooperation
	3. Technological Evolution	- Rapid tech advancements- Laws lagging behind tech- Difficulty in understanding tech implications
Operational Enforcement Challenges	1. Resource Constraints	- Limited forensic capabilities- Insufficient funding- Lack of specialized training
	2. Digital Evidence Management	- Collection difficulties- Preservation issues- Chain of custody concerns

	3. Cybercrime Reporting and Detection	- Underreporting by victims- Detection delays- Reliance on victim reports
	4. Interagency Cooperation	- Lack of coordination- Information sharing barriers- Competing priorities
Strategic and Policy Challenges	1. Prevention and Awareness	- Public awareness levels- Preventive measures- Education and training for citizens
	2. Legal Professionals' Preparedness	- Training on cyber law- Understanding of digital technology- Engagement with cybersecurity experts
	3. Policy Development and Implementation	- Inclusive policy-making- Adaptability of policies- Implementation gaps
	4. Stakeholder Engagement	- Collaboration with tech firms- Public-private partnerships- International cooperation
	5. Future-Proofing Legislation	- Anticipating tech trends- Flexible legal frameworks- Continuous review mechanisms

In the qualitative exploration of legal professionals' perspectives on the challenges of cybercrime legislation enforcement, the analysis revealed a complex landscape characterized by three primary categories of challenges: Legal Framework Challenges, Operational Enforcement Challenges, and Strategic and Policy Challenges. Each category encompassed several subcategories, reflecting the multifaceted nature of the issue at hand.

3.1. Legal Framework Challenges

Legal professionals highlighted Ambiguity in Laws, noting the presence of "lack of clear definitions" and "overly broad terms," which one prosecutor described as "a significant barrier to effective enforcement." The Jurisdictional Issues subcategory was underscored by challenges in "cross-border enforcement," with a defense attorney noting, "We're constantly battling against the fluid nature of cyberspace, where traditional borders don't apply." Furthermore, the Technological Evolution subcategory captured the struggle to keep legislation abreast of rapid technological advancements, with a legal scholar commenting, "The law is perennially playing catch-up with technology."

3.2. Operational Enforcement Challenges

Under Operational Enforcement Challenges, the Resource Constraints subcategory was prominent, with participants citing "limited forensic capabilities" and "insufficient funding." A judge mentioned, "We often find our hands tied due to the lack of specialized training available." The Digital Evidence Management subcategory highlighted "collection difficulties" and "preservation issues," with a prosecutor stating, "Maintaining the integrity of digital evidence is a logistical nightmare." Cybercrime Reporting and Detection was noted for its "underreporting by victims" and "reliance on victim reports," with one participant observing, "Victims often don't realize they've been targeted until it's too late." Interagency Cooperation emerged as a challenge, with a defense attorney emphasizing, "The lack of coordination and competing priorities among agencies complicates matters further."

3.3. Strategic and Policy Challenges

Strategic and Policy Challenges included Prevention and Awareness, where a judge highlighted the need for "public awareness levels to match the pace of digital crime trends." The Legal Professionals' Preparedness subcategory focused on the "training on cyber law" and "engagement with cybersecurity experts," as one legal scholar put it, "There's a gap in understanding that needs to be bridged." Policy Development and Implementation drew attention to "inclusive policy-making" and "implementation gaps," with a participant advocating for "policies that are adaptable and can evolve." Stakeholder Engagement was critical, with a prosecutor noting, "Collaboration with tech firms and international cooperation are key to staying ahead." Lastly, Future-Proofing Legislation was discussed, with a defense attorney suggesting, "We need flexible legal frameworks that can quickly adapt to new technological realities."

4. Discussion and Conclusion

The qualitative analysis of legal professionals' perspectives on the enforcement challenges of cybercrime legislation yielded three main themes: Legal Framework Challenges, Operational Enforcement Challenges, and Strategic and Policy Challenges. Within these themes, a variety of categories were identified, encompassing Ambiguity in Laws, Jurisdictional Issues, and Technological Evolution under Legal Framework Challenges; Resource Constraints, Digital Evidence

Management, Cybercrime Reporting and Detection, and Interagency Cooperation under Operational Enforcement Challenges; and Prevention and Awareness, Legal Professionals' Preparedness, Policy Development and Implementation, Stakeholder Engagement, and Future-Proofing Legislation under Strategic and Policy Challenges.

The Legal Framework Challenges theme revealed complexities surrounding the current state of cybercrime legislation. The category of Ambiguity in Laws included concepts such as lack of clear definitions, overly broad terms, and outdated provisions, indicating significant hurdles in applying these laws to cybercrime effectively. Jurisdictional Issues highlighted cross-border enforcement challenges, conflicts of law, and a lack of international cooperation, reflecting the global nature of cybercrime and the difficulties in jurisdictional consensus. Technological Evolution was marked by rapid technological advancements, laws lagging behind technology, and difficulty in understanding technological implications, emphasizing the need for laws that evolve in tandem with technological progress.

Under Operational Enforcement Challenges, Resource Constraints were identified, including limited forensic capabilities, insufficient funding, and lack of specialized training, pointing to the need for better resources and training for law enforcement dealing with cybercrime. Digital Evidence Management emphasized collection difficulties, preservation issues, and chain of custody concerns, which are critical in prosecuting cybercrimes. Cybercrime Reporting and Detection brought attention to underreporting by victims, detection delays, and reliance on victim reports, indicating gaps in the initial stages of cybercrime response. Interagency Cooperation underscored the lack of coordination, information sharing barriers, and competing priorities among different agencies, suggesting the necessity for improved collaboration mechanisms.

The theme of Strategic and Policy Challenges covered broader, systemic issues. Prevention and Awareness focused on public awareness levels, preventive measures, and education for citizens, stressing the importance of informed and proactive cyber hygiene practices. Legal Professionals' Preparedness dealt with training on cyber law, understanding of digital technology, and engagement with cybersecurity experts, highlighting the gap in knowledge and preparedness among legal professionals. Policy Development and Implementation discussed inclusive policy-making, adaptability of policies, and implementation gaps, reflecting on the need for dynamic and responsive policymaking processes. Stakeholder Engagement and Future-Proofing Legislation addressed collaboration with tech firms, public-private partnerships, international cooperation, anticipating tech trends, flexible legal frameworks, and continuous review mechanisms, pointing towards the need for a forward-looking and collaborative approach to cybercrime legislation and enforcement.

The operational enforcement challenges, particularly the resource constraints and digital evidence management difficulties identified in this study, find support in Cockcroft et al.'s (2018) examination of police cybercrime training. The lack of specialized training and resources for law enforcement officers, as pointed out by Cockcroft et al., directly impacts their ability to manage and investigate cybercrimes effectively (Cockcroft et al., 2018). This is further compounded by Holt and Bossler's (2012) study on patrol officers' perceived role in responding to cybercrime, which suggests a gap between the existing training and the operational demands of cybercrime investigation (Holt & Bossler, 2012).

Our findings on the ambiguity of laws resonate with Ajayi's (2016) identification of the challenges to the enforcement of cybercrime laws and policy, highlighting the critical issue of vague legislation that hampers effective prosecution and adjudication of cyber offenses (Ajayi, 2016). Furthermore, the jurisdictional issues underscored in our study mirror Calderoni's (2010) discussion on the European legal framework, emphasizing the dire need for cross-border cooperation and harmonization of laws to combat the inherently transnational nature of cybercrime effectively (Calderoni, 2010).

The strategic and policy challenges, especially in terms of prevention and awareness, align with Salminen and Hossain's (2018) appraisal of cybersecurity's human security dimensions. Their work underscores the importance of enhancing public awareness and understanding of cybersecurity threats and prevention measures, a sentiment echoed in our findings (Salminen & Hossain, 2018). Moreover, our study's emphasis on the need for future-proofing legislation and enhancing legal professionals' preparedness finds parallel in Khan et al.'s

(2022) systematic review, which calls for adaptable and evolving cybercrime legislation (Khan et al., 2022).

The synthesis of our findings with existing literature underscores a shared recognition of the complex and evolving challenges in cybercrime legislation enforcement. As highlighted by Lu, Liang, and Taylor (2010), the comparative analysis between countries emphasizes the need for international cooperation and a unified approach to cybercrime, a theme that is evident in our study's emphasis on jurisdictional issues and stakeholder engagement (Lu et al., 2010). Furthermore, the critical role of training and resource allocation identified by Paoli et al. (2020) reinforces our findings on operational enforcement challenges, particularly the need for enhanced cybercrime training and resources for law enforcement (Paoli et al., 2020).

This qualitative study embarked on an exploration of legal professionals' perspectives on the enforcement challenges of cybercrime legislation. Through semi-structured interviews with 30 participants, including prosecutors, defense attorneys, judges, and legal scholars, the study unveiled three primary categories of challenges: Legal Framework Challenges, Operational Enforcement Challenges, and Strategic and Policy Challenges. The findings highlighted the ambiguity and rapid technological evolution of laws, jurisdictional issues, resource constraints, digital evidence management, cybercrime reporting and detection difficulties, interagency cooperation, the need for prevention and awareness, legal professionals' preparedness, policy development, stakeholder engagement, and the imperative of future-proofing legislation.

This study, while insightful, is not without limitations. The reliance on qualitative interviews, although rich in detail, limits the generalizability of the findings. The sample, confined to legal professionals within a specific geographical and legal jurisdiction, may not capture the full spectrum of global cybercrime enforcement challenges. Additionally, the rapid evolution of technology and cybercrime tactics may outpace the relevance of these findings over time, necessitating continuous research in this domain.

Future research should aim to broaden the scope of investigation to include a more diverse range of jurisdictions and legal systems, enhancing the generalizability of findings across different cultural and legal contexts. Quantitative studies could complement this qualitative research, providing statistical insights into the prevalence and impact of identified challenges. Additionally, longitudinal studies would offer valuable perspectives on how the challenges and strategies evolve alongside technological advancements and changing cybercrime patterns.

For practitioners, this study underscores the need for ongoing training and education for legal professionals in the nuances of cybercrime and digital evidence. Enhancing interagency and international cooperation emerges as a crucial strategy for addressing jurisdictional and operational challenges. The findings also highlight the importance of engaging stakeholders, including technology companies and international legal entities, in policy development processes to ensure comprehensive and adaptable cybercrime legislation. Ultimately, the study calls for a proactive and dynamic approach to legislative and enforcement practices, emphasizing the importance of anticipating technological advancements and adapting legal frameworks accordingly.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Ajayi, E. F. G. (2016). Challenges to Enforcement of Cyber-Crimes Laws and Policy. *Journal of Internet and Information Systems*. https://doi.org/10.5897/jiis2015.0089

Bossler, A. M., & Holt, T. J. (2012). Patrol Officers' Perceived Role in Responding to Cybercrime. *Policing an International Journal*. https://doi.org/10.1108/13639511211215504

Calderoni, F. (2010). The European Legal Framework on Cybercrime: Striving for an Effective Implementation. *Crime Law and Social Change*. https://doi.org/10.1007/s10611-010-9261-6

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C., & Trevorrow, P. (2018). Police Cybercrime Training: Perceptions, Pedagogy, and Policy. *Policing a Journal of Policy and Practice*. https://doi.org/10.1093/police/pay078

Holt, T. J. (2018). Regulating Cybercrime Through Law Enforcement and Industry Mechanisms. *The Annals of the American Academy of Political and Social Science*. https://doi.org/10.1177/0002716218783679

Holt, T. J., & Bossler, A. M. (2012). Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments. *Cyberpsychology Behavior and Social Networking*. https://doi.org/10.1089/cyber.2011.0625

Khan, S., Saleh, T. A., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A Systematic Literature Review on Cybercrime Legislation. *F1000research*. https://doi.org/10.12688/f1000research.123098.1

Koziarski, J., & Lee, J. R. (2020). Connecting Evidence-Based Policing and Cybercrime. *Policing an International Journal*. https://doi.org/10.1108/pijpsm-07-2019-0107

Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). Examining English and Welsh Detectives' Views of Online Crime. *International Criminal Justice Review*. https://doi.org/10.1177/1057567719846224

Lu, H., Liang, B., & Taylor, M. (2010). A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States. *Asian Journal of Criminology*. https://doi.org/10.1007/s11417-010-9092-5

Nugroho, A. D., & Chandrawulan, A. A. (2022). Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries. *Security Journal*. https://doi.org/10.1057/s41284-022-00357-y

Paoli, S. D., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M. C., & Martin, R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges From the Perspective of Police Cybercrime Specialists. *Policing a Journal of Policy and Practice*. https://doi.org/10.1093/police/paaa027

Salminen, M., & Hossain, K. (2018). Digitalisation and Human Security Dimensions in Cybersecurity: An Appraisal for the European High North. *Polar Record*. https://doi.org/10.1017/s0032247418000268

Trufanova, A. Y. (2023). Cyberspace as a Crime Scene: Current Trends, Features, Prevention Measures. *Current Issues of the State and Law*. https://doi.org/10.20310/2587-9340-2023-7-4-610-619