Al-Ahkam: Jurnal Ilmu Syari'ah dan Hukum
Vol. 9, Nomor 2, 2024, pp. 154-170
e-ISSN: 2527-8150; p-ISSN: 2527-8169
DOI: https://doi.org/10.22515/alahkam.v9i2.10269

Integrating Electronic Information and Transaction Law (UU ITE) and Islamic Criminal Law: Addressing Malware-Based Data Theft

Apipuddin[1*], Ulyan Nasri[2], R. Arif Mulyohadi[3], Asbullah Muslim[4]

[1]Universitas Islam Negeri Mataram, Indonesia
[2]Institut Agama Islam Hamzanwadi NW Lombok Timur, Indonesia
[3]Sekolah Tinggi Agama Islam Syaichona Moh. Cholil Bangkalan, Indonesia
[4]Institut Elkatarie, Indonesia
*Corresponding author's email: apipuddin@uinmataram.ac.id

Abstract

This study examines the phenomenon of information theft using malware, analyzed through the lens of Indonesian criminal law under Law No. 19 of 2016 on Electronic Information and Transactions (UU ITE) and Islamic criminal law principles. The research focuses on the legal implications and measures to address cybercrime, particularly data theft, in the digital era. Employing a normative juridical approach, the study analyzes primary and secondary legal materials, including statutory provisions, case laws, and relevant literature. Findings reveal that UU ITE provides detailed mechanisms for criminalizing and penalizing perpetrators of malware-based data theft, emphasizing preventive and repressive actions. From the perspective of Islamic criminal law, such acts are categorized under ta'zīr punishments, as they harm individuals and society by violating the principles of amanah (trust) and maslahah (public interest). The study concludes that while UU ITE effectively addresses cybercrime, integrating Islamic legal principles could enhance the ethical foundation of law enforcement, fostering a balanced approach between punitive measures and moral guidance. This research contributes to the discourse on harmonizing modern legal frameworks with religious values to strengthen cybersecurity law enforcement.

Keywords: *Data Theft, Malware, UU ITE, Islamic Criminal Law, Cybercrime, Information Protection.*

| Submitted: October 23, 2024 | Accepted: December 25, 2024 | Published: December 27, 2024 |

Introduction

The development of information and communication technology has brought various innovations that simplify human activities. However, this advancement also introduces threats, including cybercrimes such as data theft using malware (Anugerah & Tantimin, 2022; Hassanah, 2023). Malware, as harmful software, has become one of the primary tools in digital crime. In 2019, a perpetrator used malware to steal personal data from e-commerce customers, including credit card numbers and other sensitive information. After stealing the data, the perpetrator misused it for fraudulent activities. The South Jakarta District Court sentenced the perpetrator to 5 years in prison and a fine of IDR 1 billion. This case highlights the challenges in law enforcement, particularly in tracking perpetrators who use advanced malware techniques (Mahaputra et al., 2024). Data stolen through malware often involves sensitive information, such as financial records, personal information, and critical documents, which are then used for illegal purposes, including identity theft and extortion. In the context of Indonesian law, Law No. 19 of 2016 on Electronic Information and Transactions well known as UU ITE was designed to protect the security of electronic data and information (Nurrizki & Amin, 2024). This regulation not only governs activities considered unlawful but also establishes strict criminal sanctions for perpetrators of cybercrimes. However, the implementation of UU ITE faces various challenges, such as weak law enforcement, technological disparities, and the public's limited understanding of cyber threats (Jamba & Svinarky, 2023; Rumlus & Hartadi, 2020).

Meanwhile, Islamic criminal law provides ethical principles that can complement modern legal approaches (Karimullah, 2023; Nurrizki & Amin, 2024). In Islam, data theft can be categorized as a violation of *amanah* (trust) and may be subject to *ta'zīr* punishments, which are flexible and tailored to the severity of the crime. This approach emphasizes not only punitive measures but also prevention and moral rehabilitation, thus contributing to a safer and more ethical societal order (Junaidi et al., 2020; Syakban, 2024). For instance, during the time of Prophet Muhammad (PBUH), there were several cases that can be used as analogies or qiyās in understanding the application of Islamic principles to contemporary issues like data theft. One such case is the incident involving a companion named Shu'ayb ibn Harb, who was entrusted with a valuable item. When the item was stolen, the Prophet (PBUH) emphasized the importance of restoring trust and accountability. This principle of safeguarding amanah can be applied to modern scenarios of data theft, as individuals are entrusted with private information in the digital age (Vichi Novalia et al., 2024). Similarly, the principle of ta'zīr (discretionary punishment) can be drawn from the Prophet's decisions in cases where a fixed punishment was not specified in the Qur'an or Hadith, such as in the case of Ma'iz (who confessed to adultery). The flexibility of ta'zīr allows judges to tailor the punishment to the circumstances, ensuring justice is served while considering the rehabilitative aspect of the offense. These cases from the time of the

Prophet provide valuable lessons in applying Islamic criminal law to modern challenges, like cybercrimes (Syarbaini, 2023a).

The lack of broader insights into previous research on malware or cybercrime is evident in several studies. Junaedi et al. (2023), focus on the crime of administrative data leaks from *Higher* Education Database and Data regarding Lecturer Certification Committee - Proposing University well known as PDDIKTI and PSD-PTU under UU ITE (Electronic Information and Transaction Law). However, their analysis is limited to specific cases and does not explore the perspective of Islamic law. Similarly, Liu (2023), examines the crime of personal information invasion in criminal law but omits integration with Indonesian or Islamic legal frameworks. Aminat et al. (2024), investigate legal protections for personal information security but do not address the specific dynamics of malware-related crimes. Ahmad and Basuki (2024), discuss legal protections for phishing victims in mobile banking, emphasizing phishing over malware. Additionally, Sadjijono (2023), evaluates Article 27(3) of UU ITE from a human rights perspective but does not analyze malware-related crimes or incorporate cross-legal perspectives. These studies collectively highlight the need for research that bridges gaps in understanding malware crimes, especially from a multidisciplinary approach that includes both Islamic and Indonesian legal systems. The importance of integrating two types of law, such as Islamic law and Indonesian law, lies in their ability to provide a more comprehensive approach to modern legal issues, including cybercrimes like malware. Previous studies are often limited to specific legal perspectives, overlooking broader dimensions such as the ethical and religious values embedded in Islamic law. By integrating these two legal systems, we can create more holistic, fair, and relevant solutions to complex legal challenges, including technology-based crimes.

Given these gaps, this study seeks to contribute by offering a comprehensive analysis of data theft crimes committed using malware, framed within the context of UU ITE and Islamic criminal law. It is necessary to delve deeply into why the perspective of Islamic law is relevant, as it provides an ethical and moral framework that complements the existing legal structure in addressing cybercrimes. By integrating these two legal approaches, this research aims to deliver a more holistic solution for regulating and enforcing laws against cybercrimes in Indonesia. To effectively implement this integrated approach, policymakers and law enforcement agencies should prioritize collaboration with Islamic legal scholars to develop clear guidelines on applying *ta'zīr* for cybercrimes. Additionally, capacity-building programs for law enforcement must be enhanced, focusing on technological proficiency and ethical training rooted in Islamic principles. Strengthening international cooperation is also crucial to address transnational cybercrime challenges, ensuring that both legal and moral dimensions are upheld.

Methods

This research employs a qualitative approach with a normative legal design, focusing on the analysis of statutory frameworks and Islamic criminal law principles (Fuhrmann et al., 2018; Sasdelli & Trivisonno, 2023). The primary emphasis is on understanding how Law No. 19 of 2016 on Electronic Information and Transactions (UU ITE) addresses crimes involving malware-based data theft and how these provisions align with Islamic legal perspectives. The sources of data are divided into two categories. The first is primary legal sources, which include UU ITE as the statutory framework and key Islamic legal texts, such as classical *fiqh* books and contemporary interpretations of Islamic criminal. The second category comprises secondary legal sources, which consist of scholarly articles, legal commentaries, and relevant academic studies focusing on cybercrimes, particularly those involving malware and data protection. These secondary sources provide context and insights for the comparative analysis conducted in this study (Grenier, 2023; Laudien et al., 2024).

Data collection is carried out through document analysis, involving a detailed examination of legal texts, academic literature, and case studies. The study utilizes a legal interpretation method (*tafsir qānūn*) to analyze statutory provisions and Islamic principles. Content analysis is applied to interpret the provisions of UU ITE, exploring their implications for combating malware-related data theft. A comparative analysis is also conducted to evaluate the similarities and differences between the regulatory framework under UU ITE and Islamic legal principles in addressing cybercrimes. This includes an assessment of how each system handles issues such as data theft, punishment, and ethical considerations (Bhat, 2020; Deffains & Fluet, 2019). Furthermore, case study analysis is utilized to examine real-life applications and challenges in law enforcement related to malware crimes.

The overall goal of this methodological approach is to identify legal gaps, evaluate the effectiveness of existing regulations, and propose an integrated legal framework. This framework aims to enhance the ability of both modern and Islamic legal systems to address cybercrimes effectively, ensuring comprehensive protection for victims and promoting justice in the digital era.

Results and Discussion

Legal Framework Under Electronic Information and Transaction Law

Electronic Information and Transaction Law (UU ITE) categorizes malware-based data theft as an act of unauthorized access (illegal access) and unauthorized use of electronic systems or data. Articles 30 and 32 specifically address the criminalization of such acts, emphasizing the protection of personal and institutional data. Article 30 defines illegal access as intentionally and unlawfully accessing computers or electronic systems belonging to others and prescribes punishments of imprisonment and fines based on the severity of the offense. Meanwhile, Article

32 criminalizes actions such as altering, adding, reducing, transmitting, damaging, deleting, transferring, hiding, or making electronic information or documents inaccessible without rights, aiming to ensure the integrity of electronic systems and data. However, the study identifies gaps in enforcement due to the limited capacity of investigative agencies, technological challenges, and jurisdictional complexities, particularly in transnational cybercrimes.

To strengthen the analysis of the enforcement of Articles 30 and 32 of UU ITE, it is essential to incorporate real-world cases and comparative analysis. For instance, the case of Baiq Nuril Maknun highlights challenges in interpreting and enforcing the provisions of UU ITE, especially regarding unauthorized data use. Although this case revolved around privacy and defamation issues, it demonstrated gaps in investigative procedures and the potential for misuse of UU ITE to criminalize unintended acts. Similarly, the Riau Cybercrime Case in 2021, involving the hacking of government databases, underscores the limitations of investigative agencies in addressing complex cybercrime cases. Despite clear evidence of unauthorized access and manipulation of electronic data, the investigation faced delays due to inadequate technological resources and expertise (Kompas, 2021)

A comparative analysis with other jurisdictions, such as Singapore's Cybersecurity Act, reveals the need for more robust frameworks. Singapore's Act emphasizes proactive measures, including mandatory reporting of cybersecurity breaches and stringent penalties for non-compliance, which have led to successful enforcement and deterrence of cybercrimes. In contrast, UU ITE lacks clear guidelines for pre-emptive actions, relying heavily on reactive measures post-incident (Gorian, 2020). These cases and comparisons underscore the importance of strengthening investigative capacity, updating technological tools, and providing clearer enforcement guidelines. By addressing these issues, UU ITE can better fulfill its mandate to protect personal and institutional data while adapting to the evolving landscape of transnational cybercrimes.

The deterrence theory suggests that individuals are less likely to engage in unlawful acts if they perceive the risk of detection and punishment as high (Kocian, 2021). In the context of malware-based data theft, UU ITE’s Articles 30 and 32 criminalize such actions and prescribe penalties to protect electronic systems and data. However, enforcement gaps, such as limited investigative capacities, technological challenges, and jurisdictional complexities in transnational cybercrimes, undermine this deterrent effect. Strengthening enforcement mechanisms, including investments in digital forensic expertise and international cooperation, can enhance the perceived risk for potential offenders. This aligns with the deterrence theory by emphasizing the importance of certainty, severity, and swiftness of punishment, thereby ensuring better protection against cybercrimes (Bijlsma, 2021).

In addition, Islamic criminal law offers a complementary perspective through *ta'zīr*, which allows for flexible and rehabilitative punishments tailored to the context of the crime. Malware-based data theft, viewed as a breach of *amanah* (trust), harms individuals and society and necessitates moral accountability. Rooted in virtue ethics, *ta'zīr* emphasizes moral rehabilitation over mere punitive measures. Judges can impose penalties such as restitution, community service, or mandatory ethical education to address the harm caused while fostering the offender's moral development. This approach not only rectifies the immediate consequences of the crime but also promotes long-term behavioral change (Rahmatullah & Baharun, 2023a; Syarbaini, 2023b).

By integrating the deterrent objectives of UU ITE with the rehabilitative principles of *ta'zīr* in Islamic law, a holistic framework can be established to combat malware-based data theft. This combined approach ensures that justice is upheld while fostering ethical awareness and societal harmony, effectively addressing both the legal and moral dimensions of cybercrimes.

Principles of Islamic Criminal Law regarding data theft

Islamic law views malware-based data theft as a violation of *amanah* (trust) and a breach of ethical and social responsibilities. From a criminal law perspective, such actions fall under the category of *ta'zīr* offenses, where punishments are discretionary and determined by the judge (*qāḍī*). Key findings indicate that Islamic law emphasizes the moral and ethical dimensions of data protection, considering the theft of information as a betrayal of trust and an act of injustice (*ẓulm*). The flexibility of *ta'zīr* allows Islamic courts to impose penalties proportionate to the harm caused, such as fines, imprisonment, or public reprimand. Furthermore, preventative measures in Islamic teachings, such as fostering honesty and accountability, serve as complementary mechanisms to legal enforcement (Alotaibi, 2018).

Ta'zīr law in Islamic criminal law is a form of discretionary punishment, granting judges the freedom to determine the type and extent of the penalty based on the specific circumstances of the offense. It is applied to crimes not explicitly regulated in Islamic texts, such as *hudud* or *qisas*, but which harm society and contradict the moral and ethical principles of Islam. The flexibility of *ta'zīr* enables judges to tailor punishments to the severity of the offense and the individual circumstances of the offender, ensuring the relevance of Islamic law in addressing modern crimes like cybercrimes and malware-based data theft (Jaenudin & Nisa, 2021).

However, the application of ta'zīr in addressing malware-based data theft presents challenges, particularly regarding the lack of consistency and measurable standards in determining appropriate punishments. In Islamic criminal law, ta'zīr is a discretionary punishment applied for offenses where the specific punishment is not prescribed in the Qur'an or Hadith, allowing the judge to determine the most suitable penalty based on the circumstances of the crime. However, the absence of clear and standardized guidelines for applying ta'zīr to modern cybercrimes, such as malware-based data theft, creates ambiguity and inconsistency in legal decisions. This can lead to subjective rulings and potential injustices, as the severity of punishment might depend on the individual judge's interpretation. To address these challenges, it is essential for Islamic legal scholars to develop specific frameworks that provide clarity and fairness when applying ta'zīr to cybercrimes. This would ensure that Islamic criminal law can effectively respond to the complexities of modern crimes while maintaining justice and consistency in its application.

Integrating Electronic Information and Transaction Law and Islamic Criminal Law

The study highlights the complementary nature of UU ITE and Islamic criminal law in addressing cybercrimes. Both legal systems share similarities in recognizing the seriousness of data theft and the need for punitive measures to protect victims. However, they also differ in their approaches. UU ITE emphasizes statutory regulations and technical enforcement, focusing on concrete legal frameworks and technological measures to address cybercrimes. In contrast, Islamic criminal law incorporates ethical and moral considerations, offering a more holistic approach that includes prevention, punishment, and rehabilitation. This dual perspective enhances the overall effectiveness of efforts to combat cybercrimes, addressing both their legal and moral dimensions.

To expand on how the ethical principles of *amanah* (trust) and *maslahah* (public interest) in Islamic law can address gaps in the enforcement mechanisms of UU ITE, it is essential to understand how these principles operate within the Islamic legal framework. Firstly, *amanah* (trust) is a fundamental concept in Islam, emphasizing the responsibility to protect others' rights. In the context of digital crimes, this translates to safeguarding personal data and electronic information. Violating this trust, such as through data theft or misuse, is seen as a betrayal, which carries moral and legal consequences. In relation to UU ITE, Islamic law provides an additional perspective that not only considers the legal implications of data theft but also the broader ethical violation of trust (Kocian, 2021). By integrating the principle of *amanah* into the enforcement of UU ITE, offenders are reminded of the moral responsibility they hold towards others, which could strengthen the overall enforcement and deter potential cybercriminals by emphasizing the social and moral consequences of their actions.

Secondly, *maslahah* (public interest) prioritizes the welfare of the community and encourages laws that not only protect individuals but also ensure the safety and peace of society at large. In the context of UU ITE, the principle of *maslahah* can help address gaps in enforcement by advocating for a more proactive approach to prevent cybercrimes. Islamic law emphasizes not just punitive measures, but also prevention and rehabilitation, which aligns with the need to educate the public, raise awareness, and strengthen technological safeguards. By integrating *maslahah*, UU ITE could be further enhanced to focus not only on punishing cybercriminals but also on protecting public interests through proactive measures (Mukhammad et al., 2024).

Islamic law's focus on *amanah* and *maslahah* also supports the rehabilitative aspect of *ta'zīr* punishments. Unlike purely punitive measures, *ta'zīr* serves not only as a form of punishment but also as a tool for moral rehabilitation. By addressing the character and moral development of offenders, this approach aligns with virtue ethics, which emphasizes the cultivation of good character (Santoso & Purwaningsih, 2024). This rehabilitative focus ensures that punishment in the context of cybercrimes is not merely about deterrence but also about restoring the offender's moral integrity, ultimately contributing to a more ethical society. By combining the legal framework of UU ITE with the ethical dimensions of Islamic law, we can create a more holistic system that not only punishes cybercrimes but also prevents them through moral education and rehabilitation, offering a more effective and comprehensive approach to tackling digital crimes.

Challenges and Opportunities in Addressing Malware Crimes

The research identifies several challenges in applying UU ITE and Islamic criminal law to malware-related crimes. In the context of UU ITE, limited resources and expertise among law enforcement agencies pose significant obstacles to the effective investigation and prosecution of malware cases (Santoso & Purwaningsih, 2024). These limitations hinder the ability to address the technical complexities and evolving nature of cybercrimes. To better support the argument, it would be useful to provide more detailed figures or statistics regarding cybercrime trends in Indonesia, especially in relation to UU ITE enforcement. Including a visual element, such as a comparative table or graph, could also help illustrate the application of UU ITE versus Islamic law in addressing cybercrime (Anugrahwati et al., 2024).

In Islamic law, the application of *ta'zīr* (discretionary punishment) to modern crimes, particularly cybercrimes, faces significant challenges due to the absence of standardized mechanisms. While Islamic criminal law provides a rich theoretical framework for addressing moral and legal violations, its application to emerging threats like cybercrime remains ambiguous. The traditional framework of Islamic law was designed for an era that did not foresee the complexities of digital technology, data theft, or online harassment. This lack of clear and detailed provisions for modern crimes like cybercrimes leads to inconsistent application, where judges and scholars must rely on their discretion to determine punishments, which may vary significantly based on interpretation (Rahmatullah & Baharun, 2023a).

The absence of specific guidelines for addressing cybercrimes creates challenges in ensuring fairness and consistency in legal responses. For instance, while theft and fraud are clear offenses under Islamic law, the unlawful access, manipulation, or theft of data via malware may not be easily categorized within existing punishments like *ḥadd* (fixed punishments) or *qiṣāṣ* (retributive justice). *Ta'zīr*, being discretionary, could theoretically be applied to such crimes, but the lack of clear definitions and guidelines means there is room for ambiguity and uncertainty

(Alotaibi, 2018; Kutubi, 2024). To clarify this, Islamic legal scholars could look to past cases or theoretical applications of *ta'zīr* to similar offenses. For example, historical cases where ta'zīr was used for crimes such as bribery, corruption, or embezzlement could offer insights into how Islamic law might respond to cybercrimes. Scholars could also develop frameworks that address the ethical aspects of cybercrimes, such as violations of trust (*amanah*) and injustice (*ẓulm*), to guide judges in determining appropriate punishments, balancing deterrence with the principles of justice and rehabilitation inherent in Islamic law. This expansion of the discussion would help integrate modern issues into Islamic criminal law and ensure its relevance in addressing the challenges of the digital age (Syarbaini, 2023a).

To further elaborate on the case handled by the South Jakarta District Court, the Baiq Nuril Maknun case is a notable example involving the application of the UU ITE. Baiq Nuril, a teacher from West Nusa Tenggara, was accused under Article 27 of UU ITE for sharing a recorded conversation that allegedly defamed her superior. The case highlighted the challenges in applying traditional legal frameworks to digital privacy violations and defamation, especially when dealing with digital data sharing without consent. The court's difficulty in determining the defendant's intent and the lack of clear legal guidelines for such cases showcased the need for clearer regulations under UU ITE, particularly regarding digital privacy and defamation in the modern age.

The outcome of the case, with the South Jakarta District Court overturning the conviction, highlighted the complexity of applying UU ITE in situations where digital data sharing intentions were unclear. The case emphasizes the importance of developing more detailed provisions within UU ITE to address ambiguities related to privacy violations and data misuse. Moreover, it underscores the necessity of strengthening law enforcement's technological capacity to handle cybercrimes effectively, including specialized cybercrime units and better training in digital forensics. This would allow for fairer, more accurate legal outcomes, ensuring that digital crimes, especially those involving malware and data theft, are properly addressed under both UU ITE and Islamic criminal law.

Contribution to Legal and Policy Development

This study offers practical recommendations for policymakers to enhance the response to malware-based data theft crimes. First, revising UU ITE to include more specific provisions for evolving cyber threats, such as malware, is crucial to ensure its relevance and effectiveness in addressing modern challenges. Second, promoting cross-disciplinary collaboration can bridge the gap between modern and Islamic legal approaches, fostering a more comprehensive understanding and application of both systems. Third, educating the public on the ethical and legal implications of data theft through a combination of modern legal frameworks and Islamic teachings can raise awareness and promote accountability in digital interactions. These recommendations highlight the potential of an integrated approach that leverages both UU ITE and Islamic criminal law, providing a robust and comprehensive solution that addresses the legal and ethical dimensions of cybercrimes effectively.

Table 1 summarizes the key findings regarding malware-based data theft under both UU ITE (Law No. 19 of 2016) and Islamic criminal law. The table compares the two legal frameworks in terms of their legal provisions, punishments, ethical considerations, enforcement challenges, and proposed improvements. Under UU ITE, data theft is criminalized through Articles 30 and 32, with punishments including imprisonment and fines, while Islamic law treats data theft as a violation of trust (*amanah*) and injustice (*ẓulm*), with punishments being discretionary and based on ta'zīr.

The table also highlights the differences in focus, where UU ITE primarily addresses legal protection and enforcement through technological means, while Islamic law emphasizes moral responsibility and accountability. Enforcement challenges such as jurisdictional issues and the lack of standardized mechanisms in both systems are noted, along with recommendations for improvement. For UU ITE, it is suggested that the law be revised to address emerging cyber threats, while Islamic law recommends strengthening the integration of Islamic principles to address these crimes more effectively. Additionally, public education is proposed to raise awareness of both legal consequences and ethical considerations.

Table 1: Summary of Findings on Malware-Based Data Theft in UU ITE and Islamic Law

Aspect	UU ITE (Law No. 19 of 2016)	Islamic Criminal Law
Legal Provisions	Articles 30 and 32 criminalize unauthorized access and manipulation of electronic data.	Data theft considered a violation of amanah (trust) and ẓulm (injustice).
Punishments	Punishments include imprisonment and fines based on the severity of the offense.	Punishments are discretionary (ta'zīr), with penalties like fines, imprisonment, or public reprimand.
Ethical Considerations	Primarily focuses on legal protection and enforcement.	Emphasizes moral responsibility, accountability, and prevention through honesty.
Enforcement Challenges	Technological and jurisdictional issues hinder enforcement, with limited resources in law enforcement.	Lack of standardized mechanisms for addressing cybercrimes leads to ambiguity in applying punishments.
Comparison of Approaches	Focuses on technical enforcement and statutory regulations.	Focuses on ethical considerations and a holistic approach to justice, combining both punishment and rehabilitation.
Integrated Framework Proposal	Improve law enforcement capacity and expertise. Integrate technology-based solutions for better prosecution.	Incorporate Islamic principles to strengthen ethical practices in digital interactions and address legal gaps.

Aspect	UU ITE (Law No. 19 of 2016)	Islamic Criminal Law
Policy Recommendations	Revise UU ITE to include specific provisions for malware and emerging cyber threats.	Strengthen the connection between Islamic law and modern legal systems to better address emerging cybercrimes.
Public Education	Raise awareness about legal consequences of data theft under UU ITE.	Educate on the ethical implications of data theft, incorporating Islamic values of trust and accountability.

The table compares UU ITE (Law No. 19 of 2016) and Islamic criminal law regarding malware-based data theft. UU ITE criminalizes unauthorized access and manipulation of electronic data, with punishments including imprisonment and fines, focusing on legal enforcement. In contrast, Islamic law views data theft as a violation of trust (*amanah*) and injustice (*ẓulm*), with discretionary punishments such as fines or imprisonment, emphasizing moral responsibility and ethical behavior. Both systems face challenges: UU ITE struggles with technological and jurisdictional issues, while Islamic law lacks standardized mechanisms for addressing cybercrimes. The proposal recommends revising UU ITE to address emerging cyber threats and integrating Islamic principles to enhance ethical practices and strengthen both legal systems in tackling cybercrimes. Public education on legal and ethical implications is also necessary.

Table 1 presents a comparison between the Electronic Information and Transactions Law (UU ITE) and Islamic Criminal Law regarding malware-based data theft. In terms of legal provisions, UU ITE regulates data theft through Articles 30 and 32, which criminalize unauthorized access and manipulation of electronic data. Meanwhile, in Islamic Criminal Law, data theft is viewed as a violation of *amanah* (trust) and *ẓulm* (injustice), emphasizing the moral and ethical responsibility towards entrusted information.

Regarding punishments, UU ITE imposes penalties, including imprisonment and fines, depending on the severity of the offense, whereas Islamic Criminal Law provides *ta'zīr* punishments, which are discretionary and based on the judge's discretion, with possible penalties including fines, imprisonment, or public reprimand. This reflects a more technical approach in UU ITE and a more humane approach in Islamic Criminal Law, which considers rehabilitation of the offender (Haydar Ali Tajuddin & Hussin, 2021).

Ethical considerations in UU ITE are primarily focused on legal protection and enforcement in the digital context, while Islamic Criminal Law emphasizes moral responsibility and accountability in safeguarding personal data, as well as crime prevention through ethics and social awareness. In terms of enforcement challenges, UU ITE faces technological and resource constraints in law enforcement, while Islamic Criminal Law still struggles with applying relevant Islamic laws in the context of rapidly evolving technology (Ramadhani, 2023).

The comparison of approaches shows that UU ITE focuses on technical enforcement and clear regulations, whereas Islamic Criminal Law adopts a holistic approach that combines ethical considerations with punishment and rehabilitation. To strengthen the handling of cybercrime, an integrated framework is proposed, with improvements in law enforcement capacity under UU ITE and the incorporation of Islamic principles in Islamic Criminal Law to address existing legal gaps (Arafa, 2018).

To address these challenges, several policy recommendations are provided, including revising UU ITE to include more specific provisions for emerging cyber threats and strengthening the connection between Islamic law and modern legal systems. Additionally, public education is important to raise awareness about the legal consequences of data theft under UU ITE and instill Islamic values of trust and accountability in digital interactions. This explanation offers a more comprehensive overview of the comparison between the two legal systems in dealing with malware-based data theft (Bardavelidze, 2022).

The analysis of cybercrimes such as malware-based data theft shows significant differences between the legal approaches of the ITE Law and Islamic criminal law. The ITE Law provides a more specific and technical legal framework, enabling swift and clear law enforcement, but it lacks in addressing the moral and ethical dimensions of the crime. In contrast, Islamic criminal law, with its *ta'zir* approach, emphasizes the violation of *amanah* (trust) and the moral responsibility of the perpetrator, offering flexibility in sentencing based on the harm and intent of the crime (Jufri Yahya et al., 2023; Rahmatullah & Baharun, 2023b; Vichi Novalia et al., 2024). While this provides a more holistic approach, the application of ta'zir in the context of cybercrimes requires clearer guidelines and technological readiness to support the legal process. Therefore, integrating both legal systems could offer a more comprehensive solution to tackling cybercrime, balancing positive law with moral ethics (Lestari, 2024; Malekian, 2013; Rahimzai & Mushfiq, 2023).

The findings from this study highlight the intersection of technology-driven legal frameworks and ethical considerations in addressing cybercrimes (Alhadidi et al., 2024; Martin & Rice, 2011), such as malware-based data theft. The UU ITE provides clear legal provisions for combating cybercrimes, with Articles 30 and 32 criminalizing unauthorized access and manipulation of electronic data. However, the implementation of these laws faces challenges, particularly due to limited resources and the rapidly evolving nature of cybercrimes. While the UU ITE focuses on technological enforcement, it lacks a broader ethical framework that can foster social responsibility and preventive measures. On the other hand, Islamic criminal law offers an ethical foundation, emphasizing trust (*amanah*) and justice (*ẓulm*) in dealing with cybercrimes. This perspective focuses on the moral and social aspects of cybercrime, encouraging accountability and reform through flexible *ta'zīr* punishments, which are adaptable to the circumstances of each case.

Incorporating both frameworks legal and ethical could offer a more comprehensive approach to addressing malware-based data theft (Dong & Kotenko, 2024; Valeti & Rathore, 2024). Strengthening the enforcement of UU ITE with technological solutions is crucial, but integrating Islamic values of morality and social responsibility could further enhance preventive measures and public awareness. The combination of strict legal provisions and ethical education provides a balanced approach, addressing both the technical and moral dimensions of cybercrimes. This integrated approach could help overcome existing challenges in enforcement and promote a more socially responsible approach to combating cybercrimes, particularly in contexts where both legal and moral considerations are paramount.

Conclusion

In conclusion, the study reveals that addressing malware-based data theft requires a dual approach: a clear legal framework, as provided by Electronic Information and Transaction Law (UU ITE), and the ethical principles emphasized in Islamic criminal law. UU ITE effectively criminalizes cybercrimes such as unauthorized access and manipulation of data, but its implementation is challenged by resource limitations and the rapid evolution of technology. Islamic law, while offering valuable ethical guidance based on trust (*amanah*) and justice (*ẓulm*), lacks clear standards for dealing with cybercrimes. By integrating these two perspectives, legal enforcement and moral education, society can benefit from a more holistic approach to cybercrime prevention. Strengthening the capacity of UU ITE through technological solutions, alongside fostering public awareness through Islamic ethical teachings, can enhance both the deterrence and rehabilitation aspects of combating data theft in the digital age.

Based on the conclusion of this study, several recommendations for policymakers are as follows. Strengthening the enforcement of UU ITE is crucial by improving resources and technology to detect and prevent malware-based data theft. It is also important to establish clear guidelines in Islamic law regarding cybercrimes, particularly in the application of ta'zir. Public awareness campaigns should be increased to enhance understanding of legal compliance and Islamic ethics in preventing cybercrime. Collaboration between legal authorities and religious institutions should be encouraged to achieve an integrated approach. Additionally, periodic legal evaluations are needed to ensure that UU ITE aligns with technological developments and emerging threats. These steps will enhance the response to malware-based data theft, considering both legal and ethical aspects. For further research, it is recommended to explore the effectiveness of existing policies in addressing cybercrime through empirical studies. Future studies could also investigate the perceptions of various stakeholders, including legal experts, religious scholars, and the public, regarding the integration of Islamic principles into cybercrime legislation. Moreover, comparative studies between Indonesia and other countries with similar socio-legal contexts could provide valuable insights for developing comprehensive strategies to combat cybercrimes.

References

Akhmad Fery Hasanudin & A Basuki Babussalam. (2024). Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking. *Jurnal Gagasan Hukum*, *6*(01), 16–29. https://doi.org/10.31849/jgh.v6i01.18827

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Alotaibi, H. A. (2018). Inconsistency in Ta'zir Punishments in Islamic Juveniles' System. *Asian Social Science*, *14*(4), 70. https://doi.org/10.5539/ass.v14n4p70

Anugerah, F., & Tantimin, T. (2022). Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 419–435. https://doi.org/10.23887/jkh.v8i1.45434

Anugrahwati, L. M., Sang Khosana, K., & Hidayati, U. (2024). Empowering Batik Artisans: The Synergy of UU ITE and Smart Transaction Technologies in SMEs. *Journal of Economics, Finance and Management Studies*, *07*(01). https://doi.org/10.47191/jefms/v7-i1-15

Arafa, A. (2018). Islamic Criminal Law: The Divine Criminal Justice System between Lacuna and Possible Routes. *Journal of Forensic and Crime Studies*, *2*(1). https://doi.org/10.18875/2638-3578.2.104

Bardavelidze, N. (2022). Some Questions of Islamic Criminal Law. *Journal "Legal Methods."* https://doi.org/10.52340/lm.2021.04

Bhat, P. I. (2020). Qualitative Legal Research: A Methodological Discourse. In P. I. Bhat, *Idea and Methods of Legal Research* (pp. 359–382). Oxford University Press. https://doi.org/10.1093/oso/9780199493098.003.0012

Bijlsma, T. (2021). What's on the Human Mind? Decision Theory and Deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020* (pp. 437–454). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_23

Deffains, B., & Fluet, C. (2019). Social Norms and Legal Design. *The Journal of Law, Economics, and Organization*, ewz016. https://doi.org/10.1093/jleo/ewz016

Dong, H., & Kotenko, I. (2024). Image-based malware analysis for enhanced IoT security in smart cities. *Internet of Things*, *27*, 101258. https://doi.org/10.1016/j.iot.2024.101258

Fuhrmann, L., Kotzyba, K., & Lindacher, T. (2018). Normativität in der qualitativ-rekonstruktiven Forschungspraxis. In M. S. Maier, C. I. Keßler, U. Deppe, A. Leuthold-Wergin, & S. Sandring (Eds.), *Qualitative Bildungsforschung* (pp. 113–131). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-18597-8_7

Gorian, E. (2020). Singapore's Cybersecurity Act 2018: A New Generation Standard for Critical Information Infrastructure Protection. In D. B. Solovev (Ed.), *Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Economy and*

Production (Vol. 138, pp. 1–9). Springer International Publishing. https://doi.org/10.1007/978-3-030-15577-3_1

Grenier, A. (2023). The qualitative embedded case study method: Exploring and refining gerontological concepts via qualitative research with older people. *Journal of Aging Studies*, *65*, 101138. https://doi.org/10.1016/j.jaging.2023.101138

Hassanah, H. (2023). Tindakan Hukum Terhadap Pelaku Penyebaran Virus Komputer Melalui E-Mail (Cyber Spamming) Berdasarkan Ketentuan tentang Informasi dan Transaksi Elektronik. *Res Nullius Law Journal*, *5*(1), 1–8. https://doi.org/10.34010/rnlj.v5i1.8317

Haydar Ali Tajuddin, H., & Hussin, N. (2021). Islamic Criminal Law. In A. Trakic & H. Haydar Ali Tajuddin (Eds.), *Islamic Law in Malaysia* (pp. 29–42). Springer Singapore. https://doi.org/10.1007/978-981-33-6187-4_4

Jaenudin, J., & Nisa, R. R. (2021). Islamic Criminal Law Analysis of Cyber Crimes on Consumers In E-Commerce Transactions. *Eduvest - Journal of Universal Studies*, *1*(4), 176–181. https://doi.org/10.36418/edv.v1i4.33

Jamba, P., & Svinarky, I. (2023). Pertanggungjawaban Pidana Dalam Penyebaran Data Pribadi: Tinjauan Hukum Pidana Saat Ini. *Prosiding Seminar Nasional Ilmu Sosial Dan Teknologi (SNISTEK)*, *5*, 498–506. https://doi.org/10.33884/psnistek.v5i.8125

Jufri Yahya, Nazaruddin Nazaruddin, & Abdurrazak Abdurrazak. (2023). Ta`’zir bi Ihlakil Mal Dalam Perspektif Wahbah Zuhayli: Suatu Analisis Terhadap Kitab Fiqh Islam wa Adillatuh. *Siyasah Wa Qanuniyah : Jurnal Ilmiah Ma’had Aly Raudhatul Ma’arif*, *1*(2), 80–97. https://doi.org/10.61842/swq/v1i2.14

Junaedi, Said, T. G., & Tahir, M. (2023). Criminal for Leaking Administs Data of PDDIKTI and PSD-PTU According to Law Number 19 Year 2016 Concerning ITE. *East Asian Journal of Multidisciplinary Research*, *2*(2), 691–704. https://doi.org/10.55927/eajmr.v2i2.3026

Junaidi, M., Sukarna, K., & Sadono, B. (2020). Pemahaman Tindak Pidana Transaksi Elektronik dalam Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. *Budimas : Jurnal Pengabdian Masyarakat*, *2*(2). https://doi.org/10.29040/budimas.v2i2.1355

Karimullah, S. S. (2023). The Relevance of the Concept of Justice in Islamic Law to Contemporary Humanitarian Issues. *Al-Ahkam: Jurnal Ilmu Syari’ah Dan Hukum*, *8*(1). https://doi.org/10.22515/alahkam.v8i1.7654

Kocian, E. J. (2021). Deterrence Theory and Batman: The Dark Knight of Deterrence. In S. E. Daly (Ed.), *Theories of Crime Through Popular Culture* (pp. 7–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-54434-8_2

Kompas. (2021). *Kasus peretasan basis data pemerintah Riau, apa dampaknya? Kompas.* [Online post]. https://www.kompas.com/

Kusuma, E. & Sadjijono. (2023). Konsep Hukum Pasal 27 Ayat (3) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dalam Perspektif Hak Asasi Manusia. *Jurnal Magister Ilmu Hukum*, *13*(1), 153–181. https://doi.org/10.56943/dekrit.v13n1.157

Kutubi, M. S. (2024). التعزيرات البدنية في التشريع الإسلامي: دراسة مقارنة: التعزيرات البدنية. *AL-BURHĀN: Journal of Qurʾān and Sunnah Studies*, *8*(2). https://doi.org/10.31436/alburhn.v8i2.342

Laudien, S. M., Reuter, U., Sendra Garcia, F. J., & Botella-Carrubi, D. (2024). Digital advancement and its effect on business model design: Qualitative-empirical insights. *Technological Forecasting and Social Change*, *200*, 123103. https://doi.org/10.1016/j.techfore.2023.123103

Lestari, W. (2024). Ta'zir Crimes in Islamic Criminal Law: Definition Legal Basis Types and Punishments. *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam*, *5*(1), 22. https://doi.org/10.58836/al-qanun.v5i1.21486

Liu, Z., Bi, Y., & Liu, P. (2023). A conflict elimination-based model for failure mode and effect analysis: A case application in medical waste management system. *Computers & Industrial Engineering*, *178*, 109145. https://doi.org/10.1016/j.cie.2023.109145

Mahaputra, B. P., Muriman, C., & Nita, S. (2024). Use Of Digital Forensic Technology To Reveal The Identity Of Social Engineering Crimes. *Riwayat: Educational Journal of History and Humanities*, *7*(3), 1000–1008. https://doi.org/10.24815/jr.v7i3.39700

Malekian, F. (2013). Islamic Law Justice Systems. In J. S. Albanese (Ed.), *The Encyclopedia of Criminology and Criminal Justice* (1st ed., pp. 1–6). Wiley. https://doi.org/10.1002/9781118517383.wbeccj181

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803–814. https://doi.org/10.1016/j.cose.2011.07.003

Mukhammad, U. N., Nira, Y. A., & Hartanto, D. (2024). Sosialisasi UU ITE tentang Bersosial Media dengan Benar dan Bahaya Judi Online. *Muria Jurnal Layanan Masyarakat*, *6*(1), 51–55. https://doi.org/10.24176/mjlm.v6i1.12898

Nurrizki, F., & Amin, R. (2024). Criminal Sanctions Against Perpetrators of Misuse of Personal Data on Money Loans Based Technology: A Study in Bantul District Court, Indonesia. *International Journal of Social Science and Human Research*, *7*(08). https://doi.org/10.47191/ijsshr/v7-i08-89

Rahimzai, H., & Mushfiq, N. (2023). Ta'zir Punishment and Delegated Authority in Accordance with Islamic Jurisprudence and Afghanistan's Enacted Laws. *Integrated Journal for Research in Arts and Humanities*, *3*(5), 1–14. https://doi.org/10.55544/ijrah.3.5.1

Rahmatullah, A., & Baharun, S. (2023a). Ta'zir (Punishment) at Islamic Boarding Schools; Between Tradition, Conception, and Shadows of Human Rights Violations: *Tribakti: Jurnal Pemikiran Keislaman*, *34*(2), 267–280. https://doi.org/10.33367/tribakti.v34i2.3517

Rahmatullah, A., & Baharun, S. (2023b). Ta'zir (Punishment) at Islamic Boarding Schools; Between Tradition, Conception, and Shadows of Human Rights Violations: *Tribakti: Jurnal Pemikiran Keislaman*, *34*(2), 267–280. https://doi.org/10.33367/tribakti.v34i2.3517

Ramadhani, P. (2023). Islamic Criminal Law's View on The Crime of Attempted Rape. *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam*, *4*(2), 40. https://doi.org/10.58836/al-qanun.v4i2.21472

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285. https://doi.org/10.30641/ham.2020.11.285-299

Santoso, E. D., & Purwaningsih, S. B. (2024). *Analysis of Electronic Signature Standardization Based on UU ITE: Standarisasi Tanda Tangan Elektronik Berdasarkan UU ITE*. https://doi.org/10.21070/ups.6113

Sasdelli, D., & Trivisonno, A. T. G. (2023). Normative Diagrams as a Tool for Representing Legal Systems. *The Review of Socionetwork Strategies*, *17*(2), 217–231. https://doi.org/10.1007/s12626-023-00144-0

Syakban, M. Y. (2024). Penegakan Hukum Terhadap Tindak Pidana Ilegal Akses Kartu Kredit Studi Putusan Mahkamah Agung Nomor 837 /PID.SUS/2019/PN BYW. *Ex-Officio Law Review*, *2*(3), 249–256. https://doi.org/10.36294/exofficio.v2i3.3339

Syarbaini, A. (2023a). Konsep Ta'zir Menurut Perspektif Hukum Pidana Islam. *Jurnal Tahqiqa : Jurnal Ilmiah Pemikiran Hukum Islam*, *17*(2), 37–48. https://doi.org/10.61393/tahqiqa.v17i2.167

Syarbaini, A. (2023b). Konsep Ta'zir Menurut Perspektif Hukum Pidana Islam. *Jurnal Tahqiqa : Jurnal Ilmiah Pemikiran Hukum Islam*, *17*(2), 37–48. https://doi.org/10.61393/tahqiqa.v17i2.167

Valeti, K., & Rathore, H. (2024). GBKPA and AuxShield: Addressing adversarial robustness and transferability in android malware detection. *Forensic Science International: Digital Investigation*, *50*, 301816. https://doi.org/10.1016/j.fsidi.2024.301816

Vichi Novalia, Laudza Hulwatun Azizah, Novinda Al-Islami, & Surya Sukti. (2024). Ta'zir Dalam Pidana Islam: Aspek Non Material. *Terang : Jurnal Kajian Ilmu Sosial, Politik Dan Hukum*, *1*(2), 225–234. https://doi.org/10.62383/terang.v1i2.222