

Blackmail in the Digital Era as a Form of Modern Injustice: An Analysis of Victim Protection from an Islamic Legal Perspective

Muhammad Farrel Maulana¹, Hardianto Djanggih², Arfah Tjolleng³

^{1,2,3} Faculty of Law, Universitas Muslim Indonesia, Indonesia

Surel Koresponden: papazmurf123@gmail.com

Abstrak: Perkembangan teknologi informasi telah mendorong munculnya berbagai bentuk kejahatan siber, salah satunya adalah pemerasan digital yang kian marak terjadi melalui media sosial. Kejahatan ini tidak hanya menimbulkan kerugian materiil, tetapi juga berdampak serius terhadap kondisi psikologis dan kehormatan korban. Penelitian ini bertujuan untuk menganalisis karakteristik pemerasan di era digital sebagai bentuk kezaliman modern, mengkaji perlindungan hukum bagi korban dalam hukum positif Indonesia, serta menelaah perlindungan tersebut dalam perspektif hukum Islam. Metode penelitian yang digunakan adalah penelitian hukum empiris dengan pendekatan deskriptif-preskriptif. Data diperoleh melalui wawancara, observasi, dan studi dokumentasi di wilayah hukum Kepolisian Daerah Sulawesi Selatan. Data yang terkumpul dianalisis secara kualitatif dengan mengintegrasikan temuan empiris dan prinsip-prinsip hukum Islam, khususnya maqāsid al-syarī‘ah. Hasil penelitian menunjukkan bahwa pemerasan digital memiliki karakteristik anonim, lintas batas, dan berpotensi menyebar secara cepat, sehingga menempatkan korban dalam posisi yang rentan. Perlindungan hukum dalam hukum positif telah diatur melalui berbagai regulasi, namun implementasinya belum optimal akibat keterbatasan regulasi yang spesifik, kapasitas aparat, serta faktor sosial budaya. Dalam perspektif hukum Islam, pemerasan digital merupakan bentuk kezaliman yang melanggar prinsip perlindungan terhadap kehormatan (ḥifz al-‘ird) dan harta (ḥifz al-māl). Oleh karena itu, diperlukan rekonstruksi perlindungan hukum yang mengintegrasikan nilai-nilai keadilan, kemaslahatan, dan pemulihan korban secara komprehensif. Penelitian ini merekomendasikan penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta edukasi masyarakat sebagai upaya menciptakan perlindungan hukum yang lebih efektif dan berkeadilan di era digital.

Kata Kunci: Pemerasan Digital, Cyber Crime, Perlindungan Korban, Hukum Islam, Maqāsid al-Syarī‘ah.

Abstract: The rapid development of information technology has led to the emergence of various forms of cybercrime, one of which is digital extortion that increasingly occurs through social media platforms. This type of crime not only causes material losses but also has serious psychological and reputational impacts on victims. This study aims to analyze the characteristics of digital extortion as a form of modern injustice, examine legal protection for victims under Indonesian positive law, and explore such protection from the perspective of Islamic law. This research employs an empirical legal method with a descriptive-prescriptive approach. Data were collected through interviews, observations, and document analysis within the jurisdiction of the Regional Police of South Sulawesi. The collected data were analyzed qualitatively by integrating empirical

findings with the principles of Islamic law, particularly maqāṣid al-sharī‘ah. The results indicate that digital extortion is characterized by anonymity, borderless operation, and rapid dissemination potential, which places victims in a highly vulnerable position. Legal protection within the framework of positive law has been established through various regulations; however, its implementation remains suboptimal due to the lack of specific regulations, limited technical capacity of law enforcement officers, and socio-cultural barriers. From the perspective of Islamic law, digital extortion constitutes a form of injustice that violates the principles of protecting honor (ḥifẓ al-‘ird) and property (ḥifẓ al-māl). Therefore, a comprehensive reconstruction of legal protection is required by integrating the values of justice, public welfare, and victim recovery. This study recommends strengthening legal frameworks, enhancing the capacity of law enforcement agencies, and increasing public awareness as strategic efforts to establish effective and equitable legal protection in the digital era.

Keywords: Digital Extortion, Cybercrime, Victim Protection, Islamic Law, Maqāṣid al-Sharī‘ah.



This work is licensed under a Creative Commons Attribution 4.0 International License

A. INTRODUCTION

The rapid development of information and communication technology has brought about significant changes in the lifestyles of modern society. Technology no longer functions merely as a communication tool but has become a central part of various human activities, including social, economic, educational, cultural, governmental, and legal matters. The presence of the internet allows everyone to access information, communicate, conduct transactions, work, study, and build social relationships without being limited by time and space.[1] This condition indicates that digital technology has created a new living space known as cyberspace, a space for interactions that take place through internet networks and electronic systems. In this space, humans can carry out various activities quickly, openly, and broadly. Social media is one of the forms of digital technology development most widely used by society. Through social media, individuals can express opinions, share information, build self-image, expand their social circle, and build relationships with others. Social media also provides a space for people to express themselves freely and gain access to a variety of information. However, freedom in the digital space is not always used positively. In practice, social media can also become a means of deviance, ethical violations, and even crime. This occurs because the digital space often provides opportunities for perpetrators to conceal their identities, manipulate information, and reach victims more easily and quickly.[2]

These technological developments have ultimately given rise to new forms of crime that differ from conventional crimes. Crimes that were once committed in person can now be committed through electronic devices, messaging apps, social media, and other digital platforms. Cybercrime is a form of modern crime that continues to grow with the increase in internet usage. This crime has complex characteristics because it can be committed anonymously, across

regions, is difficult to trace, and often leaves a far-reaching impact on victims. Thus, technology has two opposing sides.[3] On the one hand, technology brings great benefits to human life, but on the other hand, it can become a means of committing crimes that harm society.

In the context of criminology, technology can be understood as a criminogenic factor, that is, a factor that can encourage or facilitate the commission of crime. Technology is not only a tool for perpetrators but also expands the modus operandi of crimes. Perpetrators can utilize social media, fake accounts, messaging apps, or digital storage to pressure, threaten, and exploit victims.[4] One form of cybercrime that is increasingly attracting attention is digital-based extortion, specifically sextortion. Sextortion is a form of blackmail carried out by threatening to disseminate personal or intimate content belonging to the victim in order to obtain certain benefits. These benefits can be money, a certain relationship, the victim's compliance, or other forms of coercion that harm the victim physically, psychologically, socially, or economically. Sextortion demonstrates a shift in the form of extortion crimes from conventional patterns to digital ones. In conventional extortion, threats are usually made directly or through physical and verbal pressure.[5] Meanwhile, in sextortion, threats are made through digital spaces, utilizing data, images, videos, private conversations, or sensitive content. Perpetrators can use this content as a tool to control victims. Victims often find themselves in a vulnerable position due to fear, shame, pressure, and anxiety about their personal content being shared with family, friends, the workplace, or the wider community. This situation makes victims vulnerable to repeated pressure and makes it difficult to escape the perpetrator's clutches.[6]

The crime of sextortion has very serious consequences, not only causing material losses but also attacking the victim's dignity, honor, and psychological well-being. Victims can experience anxiety, excessive fear, trauma, depression, sleep disturbances, reduced self-confidence, and even social isolation. In some circumstances, victims are also reluctant to report the crime due to shame, fear of being blamed, or fear of public exposure. This situation demonstrates that sextortion is not simply a legal violation but also a humanitarian issue related to the protection of the victim's dignity and recovery. Therefore, handling sextortion must be taken seriously, not only by punishing the perpetrator but also by ensuring that the victim receives adequate protection, support, and recovery.[7]

From an Islamic legal perspective, digital blackmail and sextortion can be viewed as forms of modern injustice. Injustice in Islam is not limited to physical violence, but also includes any act that harms, oppresses, humiliates, or unlawfully takes away the rights of others. Sextortion is an act that contradicts the principles of justice, trustworthiness, protection of honor, and protection of property. Within the framework of the *maqāṣid al-syarī‘ah*, this act violates several of the main objectives of sharia, particularly *ḥifẓ al-‘ird* or protection of honor, *ḥifẓ al-māl* or protection of property, and *ḥifẓ al-nafs* or protection of life and personal security. Victims of sextortion not only suffer economic harm, but also suffer from degraded dignity and disturbed peace of mind. Islam places great emphasis on protecting human dignity. Every human being has a dignity that must be maintained and must not be damaged through insults, harassment, threats, or the spread of disgrace. In the context of sextortion, the perpetrator uses the victim's shame and honor as a tool for blackmail. This action clearly contradicts Islamic values because

it involves coercion, threats, exploitation, and misuse of personal information. Furthermore, it also contradicts the prohibition against approaching adultery as stated in Surah Al-Isra', verse 32: "And do not approach adultery; indeed, it is an abomination and an evil path." This verse can be understood not only as a direct prohibition against adultery, but also as a warning against all paths that can lead to moral corruption, sexual exploitation, and the degradation of human dignity.[8]

Thus, sextortion can be understood not only as a violation of positive law but also as a violation of Islamic moral and ethical values. Under Islamic law, threatening, blackmailing, humiliating, and exploiting a victim's vulnerability are prohibited. The perpetrator is not only legally responsible but also morally and spiritually. This responsibility includes the obligation to stop the act, restore the victim's rights, and accept sanctions commensurate with the degree of wrongdoing and the losses incurred. In the context of Islamic criminal law, such acts can be categorized as ta'zir crimes, namely crimes for which sanctions are not specifically specified in the text but are left to the competent authorities to maintain public order, welfare, and justice. In Indonesia, the issues of digital extortion and sextortion have become increasingly important as internet and social media use continues to increase. People of all ages, including young people, schoolchildren, workers, and the general public, are increasingly actively using digital platforms. However, this increased use of technology has not been fully matched by adequate legal awareness and digital literacy.[9] Many users do not understand the importance of protecting personal data, limiting access to personal information, and recognizing manipulation patterns employed by digital criminals. As a result, the public is vulnerable to various forms of cybercrime, including extortion based on personal content.[10]

The state, as the law enforcer, has an obligation to protect citizens from all forms of violence, threats, and exploitation, including those occurring in the digital space. This protection is part of the state's responsibility to ensure a sense of security and justice for the public. The enactment of Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence is an important foundation for providing protection for victims of sexual violence, including those involving the digital dimension. Furthermore, provisions in laws and regulations related to electronic information and transactions also serve as legal instruments to address the unlawful distribution or threat of distribution of personal content. However, in practice, law enforcement against sextortion still faces various obstacles.

Some of these obstacles include low reporting rates, fear and shame experienced by victims, limited public understanding of victims' rights, and the suboptimal capacity of authorities to handle cases involving digital evidence. Victims often find themselves in a difficult position due to fear of being blamed or negatively stigmatized by their social environment. Stigma against victims is a serious obstacle to law enforcement, as it can lead victims to remain silent and not report their experiences. However, this silence can allow perpetrators to continue threatening and repeat their actions against other victims. Furthermore, sextortion crimes have distinct evidentiary characteristics than conventional crimes. Evidence in these cases often takes the form of electronic messages, screenshots, recorded conversations, social media accounts, digital links, or other electronic traces. This digital evidence requires careful handling to prevent

loss, damage, or questioning its validity during the legal process. Therefore, law enforcement against sextortion requires collaboration between law enforcement officials, digital platform providers, victim protection agencies, psychologists, and the community. Treatment that focuses solely on the criminal aspects without considering the victim's condition is feared to be incapable of providing comprehensive justice.

The impact of digital extortion also demonstrates that legal protection is not sufficient only after a case has reached the courts. Protection must begin from the moment the victim experiences threats, reports them, undergoes investigations, and continues through the recovery process. Victims need to feel secure that their personal content is not disseminated, their identity is protected, and their psychological well-being is restored. From an Islamic legal perspective, victim protection aligns with the objectives of sharia law, which is to prevent harm and achieve public welfare. Victims should not be left to bear the social and psychological burden alone, as the perpetrators of threats and extortion must be held accountable. One case illustrating the complexity of this issue occurred in South Sulawesi, involving alleged sexual harassment and extortion by law enforcement officers. This case demonstrates that power- and technology-based crimes can occur at all levels of society, including by those who should be obligated to protect. If the perpetrator holds a position of power, the victim can experience greater pressure due to fear, helplessness, or hesitation to report. This situation demonstrates that the issue of sextortion is not solely related to technology, but also relates to power relations, the integrity of the authorities, the courage of the victim, and the effectiveness of the legal protection system. Based on this background, this research is crucial to examine digital extortion as a form of modern injustice from an Islamic legal perspective.

This study places the victim as the primary focus, as they are the ones who experience direct losses, whether material, psychological, social, or moral. This research not only views sextortion as a criminal act under positive law, but also as a violation of the values of the *maqāṣid al-syarī'ah* (the principles of Islamic law), which emphasize the protection of honor, property, life, and human dignity. With this approach, this research is expected to provide a more comprehensive understanding of the importance of victim protection in cases of digital extortion. This research is also relevant because technological developments require the law to be adaptive. Law should not be understood solely as formal written rules but must also be able to address real issues that arise in society. In this regard, Islamic law can make normative and ethical contributions to building a more equitable victim protection system. Values such as justice, public welfare, protection of honor, prohibition of injustice, and moral responsibility can form the basis for formulating legal policies that not only punish perpetrators but also provide reparation for victims. Thus, this research is expected to identify weaknesses in the legal protection system for victims of digital extortion, analyze obstacles to law enforcement, and formulate strategic recommendations from an Islamic legal perspective. This study is expected to provide theoretical contributions to the development of contemporary Islamic criminal law, particularly in responding to the growing prevalence of cybercrime. Furthermore, this research is also expected to provide practical benefits for law enforcement officials, the government, victim protection agencies, and the public in building a legal system that is more

responsive, imbued with integrity, and oriented toward substantive justice for victims of extortion in the digital era.

B. METHOD

This research is a descriptive-prescriptive empirical legal study, with the aim of describing and formulating legal protection for victims of extortion in the digital era from an Islamic legal perspective. The approach used is a field research approach combined with an Islamic normative approach through an analysis of the *maqāṣid al-syarī'ah*, specifically the protection of honor (*ḥifẓ al-'ird*) and property (*ḥifẓ al-māl*).^[4] The research was conducted within the jurisdiction of the South Sulawesi Regional Police, with the research subjects being cyber unit investigators who handle digital extortion cases. The sample was determined purposively based on the relevance of the informants' experience and competence. The data used consists of primary data through in-depth interviews and observations, as well as secondary data in the form of laws and regulations, scientific literature, and Islamic legal sources. Data collection techniques include interviews, observations, and documentation. Furthermore, the data is analyzed qualitatively by linking empirical findings with Islamic legal principles to produce a comprehensive analysis and recommendations oriented towards substantive justice.

C. DISCUSSION

1. Characteristics of Marketing in the Digital Era as a Form of Modern Injustice.

The development of digital technology has given rise to new forms of crime with distinct characteristics from conventional crime. Blackmail in the digital age, particularly in the form of sextortion, is one concrete manifestation of this transformation. This crime is generally committed through social media, instant messaging apps, or other digital platforms, exploiting the victim's personal data as a means of pressure. Not limited to specific individuals, this crime can target anyone regardless of age, gender, or social background, making it a universal threat.^[11]

The main characteristics of digital blackmail lie in its anonymous, borderless nature, and its potential for rapid spread. Anonymity allows perpetrators to easily conceal their identities, making tracking difficult for law enforcement. Meanwhile, the cross-border nature of this crime often involves perpetrators located in different jurisdictions, creating challenges for law enforcement. Furthermore, the speed of information distribution in the digital space makes the threat posed by perpetrators highly potent, as private content can spread widely in a short time and be difficult to control.^[12] Furthermore, digital blackmail also has a powerful psychological dimension. Unlike conventional blackmail, which is generally physical or direct, digital blackmail exploits fear, shame, and social pressure as primary tools to control victims. In many cases, victims experience significant mental distress, such as anxiety, stress, and even depression, due to the threat of disseminating private content. This situation is exacerbated by a social culture that tends to blame the victim (victim blaming), leading victims to remain silent and not report their experiences.^[13]

Furthermore, digital blackmail often intersects with other crimes, such as privacy violations, the distribution of pornographic content, and online gender-based violence. This

demonstrates that digital blackmail is not a standalone crime, but rather part of a complex cybercrime ecosystem. Therefore, addressing it requires a multidisciplinary approach that focuses not only on legal aspects but also on social, psychological, and technological ones. From an Islamic legal perspective, this act can be categorized as a form of injustice (*ẓulm*) that violates the principles of justice and the public interest. Digital blackmail not only causes material harm but also violates the victim's honor (*'ird*), which in Islam is a fundamental right that must be protected. This concept of protecting honor aligns with the objectives of sharia (*maqāṣid al-syarī'ah*), particularly in safeguarding human dignity from all forms of humiliation and exploitation.[14]

Furthermore, digital extortion also violates the principle of the prohibition of spying and spreading another person's disgrace (*ifsyā' al-'uyūb*), which are expressly prohibited in Islamic teachings. Accessing, storing, and threatening to disseminate personal information without permission constitutes a violation of an individual's right to privacy. In this context, the perpetrator not only commits a crime against the individual victim but also undermines the social order that upholds the values of honor and trust. Thus, extortion in the digital era can be understood as a form of modern injustice that has not only legal dimensions, but also moral and spiritual dimensions. This crime reflects the misuse of technology that should be used for the benefit, but instead becomes a tool of oppression. Within the context of positive law in Indonesia, protection for victims of digital extortion essentially has a fairly diverse normative basis. Several relevant regulations include Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence (TPKS), the Electronic Information and Transactions Law (UU ITE), and provisions in the Criminal Code (KUHP) regarding extortion and threats. These regulations provide the legal basis for the state to take action against perpetrators while also providing protection to victims, including legal protection, restitution, and guarantees of their rights during the judicial process.

Normatively, the TPKS Law recognizes various forms of electronic-based sexual violence, including those related to the distribution of intimate content without the victim's consent. This law also emphasizes the importance of a victim-oriented approach, providing the right to protection, assistance, restitution, and rehabilitation. Meanwhile, the ITE Law serves as a legal instrument for prosecuting perpetrators of technology-based crimes, particularly those related to the distribution of illegal content and violations of privacy. However, empirical findings indicate that the implementation of this legal protection has not been fully optimal. One major obstacle is the lack of specific and comprehensive regulations governing sextortion as a form of digital-based extortion. This gap in norms often leads to multiple interpretations in the application of articles, forcing law enforcement officials to construct laws by combining several existing provisions. This situation has the potential to create inconsistencies in law enforcement and legal uncertainty for victims.

Furthermore, the limited technical capacity of law enforcement officials also poses a significant challenge. Handling digital extortion cases requires specialized expertise in digital forensics, electronic footprint tracking, and an understanding of ever-evolving information technology. In practice, perpetrators often use fake identities, anonymous accounts, or virtual private networks (VPNs) to disguise their tracks. In fact, these crimes are often committed across borders, requiring complex international cooperation in the law enforcement process. Furthermore, victim protection also faces challenges in terms of

accessibility and the courage to report. Many victims are reluctant to report their cases due to psychological factors, such as shame, fear of being blamed, and concerns about social stigma. The persistent phenomenon of victim blaming in society exacerbates this situation, leading victims to choose to resolve their problems secretly, even by complying with the perpetrator's demands. This demonstrates a gap between normative legal protection and the social realities faced by victims.

Furthermore, the victim recovery aspect has not been fully and effectively addressed. Although victims are legally entitled to psychological and social rehabilitation, in practice, these services remain limited, both in terms of availability and quality. The impact of digital extortion is not only material but also deeply impacts the mental and emotional well-being of victims. Therefore, strengthening an integrated service system involving various parties, such as law enforcement officials, victim protection agencies, psychologists, and civil society organizations, is necessary. From a legal policy perspective, this situation indicates that legal protection for victims of digital extortion needs to be directed towards a more comprehensive and integrated approach. Protection should not only focus on repressive aspects through prosecution of perpetrators, but should also encompass preventative efforts through digital literacy education for the public, as well as rehabilitative efforts to restore victims' well-being. Furthermore, harmonization of existing regulations is crucial to avoid overlapping norms and strengthen legal certainty.

2. Analysis of Victim Protection from an Islamic Law Perspective.

In Islamic law, protection of crime victims is an integral part of the objectives of sharia (maqāsid al-syarī'ah), which are directed at safeguarding five fundamental aspects of human life: religion (ḥifẓ al-dīn), life (ḥifẓ al-nafs), reason (ḥifẓ al-'aql), property (ḥifẓ al-māl), and honor (ḥifẓ al-'ird). In the context of digital extortion, the two most relevant aspects are the protection of honor (ḥifẓ al-'ird) and property (ḥifẓ al-māl), as this crime directly attacks personal dignity and has the potential to cause economic harm to victims. The concept of ḥifẓ al-'ird places human honor as a highly valued value in Islam. Every individual has the right to be protected from all forms of insult, defamation, or exploitation of private aspects of their lives. In the digital context, the threat of disseminating personal or intimate content is a serious violation of this principle, as it not only damages the victim's reputation but can also have widespread and lasting social impacts. Therefore, digital blackmail based on the threat of disseminating such content substantially contradicts the objectives of Sharia.[15]

Furthermore, the principle of ḥifẓ al-māl is also relevant in analyzing the crime of digital blackmail. The perpetrator's actions in forcing the victim to hand over a certain amount of money or benefits through threats constitutes unlawful seizure of property. Under Islamic law, any form of unauthorized appropriation of another person's property, whether through fraud, coercion, or intimidation, is categorized as a prohibited act (ḥarām) and must be subject to strict sanctions. Thus, digital blackmail encompasses two dimensions of violation: the victim's honor and property. Digital blackmail also violates the principles of tajassus (spying), backbiting, and namīmah (spreading disgrace or information that is detrimental to others). In many cases, perpetrators obtain victims' personal data or content through illegitimate means, such as manipulation, fraud, or hacking. This constitutes a violation of

an individual's right to privacy, which is strictly protected in Islam. In fact, the Quran explicitly forbids the act of searching for and publicizing others' faults, as it can damage social order and foster hostility.[16] Furthermore, digital blackmail also involves an element of *ikrah* (coercion), which deprives victims of their freedom of choice. The threats made by perpetrators, particularly regarding the dissemination of intimate content, create intense psychological pressure, placing victims in a compelled position. Under Islamic law, any act committed under duress has its own legal implications, and victims cannot be held fully accountable for their actions under such circumstances. This demonstrates that Islam provides strong protection for individuals under duress.

Within the framework of law enforcement, Islam not only emphasizes punishment for perpetrators but also prioritizes restorative justice oriented towards victim recovery. This principle is reflected in the concepts of *islāh* (peace) and *ta'wīd* (compensation), which aim to restore the victim to their original condition, both materially and immaterially. This recovery includes protecting the victim's identity, eliminating social impacts, and restoring psychological well-being. Thus, the Islamic legal approach is not only repressive, but also rehabilitative and preventative. Furthermore, from an Islamic ethical perspective, preventing digital extortion crimes must also be carried out by strengthening the moral values of individuals and society. The principle of *al-amr bi al-ma'rūf wa al-nahy 'an al-munkar* (encouraging good and forbidding evil) is an important foundation for creating a healthy social environment, including in the digital space. Education regarding social media ethics, privacy protection, and awareness of the legal and moral consequences of extortion are integral parts of prevention efforts. Based on field research, several structural, technical, and cultural obstacles exist in law enforcement against digital extortion cases. First, limited human resources and technology within police cyber units are a major obstacle. Handling digital crimes requires specialized expertise in digital forensics, electronic data analysis, and the ever-evolving capabilities of cross-platform tracking. In practice, not all law enforcement officers possess these competencies equally, impacting the effectiveness of the investigation and prosecution process.[17] Limited technological infrastructure, such as digital tracking devices and access to international databases, also slows down the process of solving cases.

Second, low public legal awareness is an equally significant factor. Many victims of digital extortion do not understand that their actions constitute a crime that can be reported and prosecuted. Lack of knowledge about reporting mechanisms, victims' rights, and the legal procedures required leads victims to be passive and choose not to pursue their cases. In some cases, victims even comply with the perpetrators' demands as a quick solution, which ultimately strengthens the perpetrators' position and expands the criminal practice. Third, cultural barriers in the form of social stigma against victims also hamper law enforcement. In a society still highly sensitive to morality, victims of intimate content-based blackmail often experience victim blaming, a tendency to blame the victim for the incident. This creates significant social pressure, leaving victims feeling afraid, ashamed, and reluctant to report the incident.[18] As a result, many digital blackmail cases remain unresolved (a dark number of crimes), leaving perpetrators free and potentially repeating their actions.

Furthermore, there are legal obstacles in the form of the lack of optimal integration of various regulations governing cybercrime and victim protection. The fragmentation of legal norms requires law enforcement officials to employ complex interpretations when prosecuting

perpetrators, particularly in cases of sextortion, which have specific characteristics. This has implications for a lack of legal certainty and the potential for differences in the handling of similar cases. To overcome these obstacles, a more comprehensive, adaptive, and substantive justice-based legal protection system is needed. From an Islamic legal perspective, this reconstruction can be achieved by strengthening the principles of al-'adl (justice), maṣlaḥah (benefit), and raf' al-zulm (elimination of injustice). The principle of al-'adl demands fair treatment of victims by ensuring that their rights are optimally protected at every stage of the legal process. The principle of maṣlaḥah directs legal policy to provide the greatest benefit to society, including in creating a sense of security in the digital space. Meanwhile, the principle of raf' al-zulm emphasizes the obligation of the state and society to eliminate all forms of injustice, including the crime of digital extortion.[19]

This reconstruction also needs to be realized through institutional strengthening and capacity building of law enforcement officials, particularly in the fields of information technology and digital forensics. Continuous training, the provision of adequate facilities and infrastructure, and cross-institutional and cross-national cooperation are strategic steps to increase the effectiveness of law enforcement. Furthermore, the creation of more specific regulations related to digital extortion is also an urgent need to provide legal certainty and strengthen the basis for prosecution against perpetrators. In addition to repressive aspects, preventive and educational approaches must also be integral parts of the reconstruction of legal protection. Public education regarding digital literacy, social media ethics, and awareness of legal rights and obligations needs to be systematically enhanced. From an Islamic perspective, these efforts align with the principle of al-amr bi al-ma'ruf wa al-nahy 'an al-munkar, which emphasizes the importance of an active role for society in preventing crime and upholding moral values.

Furthermore, a rehabilitative approach to victims must be strengthened through the provision of integrated legal, psychological, and social support services. The state needs to ensure that victims receive not only legal justice but also comprehensive recovery from the impacts they have experienced. This aligns with the principle of restorative justice in Islamic law, which places victim recovery as a crucial component of law enforcement objectives.

D. CONCLUSION

Digital extortion is a modern form of crime characterized by its anonymity, cross-border nature, and the rapid spread of information. This crime not only causes material losses but also seriously impacts the psychological well-being and honor of victims. From an Islamic legal perspective, digital extortion is categorized as a form of injustice (zulm) because it violates the principles of protecting honor (ḥifz al-'ird) and property (ḥifz al-māl), and contradicts the moral and ethical values upheld by Sharia law. Under Indonesian positive law, protection for victims of digital extortion has a normative basis through various regulations, such as the Law on Sexual Violence and the Law on Information and Electronic Transactions. However, its implementation has not been optimal due to limited specific regulations, the technical capacity of law enforcement officers, and low public legal awareness. Furthermore, cultural factors such as social stigma against victims also hamper the process of law enforcement and victim recovery. From an Islamic legal perspective, victim protection emphasizes not only punishing the perpetrator but also encompasses comprehensive victim recovery through a restorative

justice approach. The principles of the maqāṣid al-syarī‘ah (laws of justice) provide a comprehensive framework for addressing digital extortion, emphasizing the protection of human dignity, justice, and public welfare. Therefore, a more comprehensive and integrative reconstruction of the legal protection system is needed, combining a positive legal approach with Islamic legal values. These efforts include strengthening regulations, increasing the capacity of law enforcement officers, educating the public, and providing recovery services for victims. Thus, legal protection for victims of digital extortion is expected to be optimal, just, and able to address the challenges of crime in the digital era.

E. REFERENCE

- [1] M. F. Ramadhan, S. Nawī, H. Khalid, and I. Abbas, “The Nature of Legal Regulations on The Merauke Integrated Food and Energy Plantation Project,” vol. 11, no. 1, pp. 3001–3006, 2026.
- [2] F. A. Ningsih, S. N. Sumantri, S. A. Fachri, A. Setiawan, S. Luthfie, and A. Ghaffar, “Analisis Jarimah Judi Online Dalam Perspektif Fiqh Jinayah Fakultas Syariah dan Hukum Universitas Islam Negeri Sumatera Utara,” vol. 10, no. 36, pp. 132–142, 2025.
- [3] D. G. Yambo, L. Marsuni, and A. Aswari, “Legal Force of Information Technology-Based Money Lending Agreements,” vol. 1, no. 2, pp. 1–8, 2025.
- [4] M. Romdoni, R. Aulia, and R. Ms, “Online Gambling In The Perspectives of Islamic Law and Criminal Law : A Critical Analysis of Current Cases In Indonesia,” vol. 15, no. 02, pp. 535–548, 2025, doi: 10.58471/justi.v15i02.
- [5] ... D. Y.-P. dan S. K. (PPSK) B. and undefined 2005, “Bank syariah: Gambaran umum,” *ipief.ummy.ac.id*, Accessed: Apr. 14, 2025. [Online]. Available: <https://ipief.ummy.ac.id/wp-content/uploads/2020/02/14.-Bank-Syariah-Gambaran-Umum.pdf>
- [6] Mubarak Nafi, “SOSIO YUSTISIA: Jurnal Hukum dan Perubahan Sosial SISTEM PEMERINTAHAN DI NEGARA-NEGARA RUMPUN MELAYU,” vol. 1, 2021, [Online]. Available: <https://www.bing.com/ck/a?!&&p=b30e29e4014e0b8dfbc6a73a31e5e5f21dee3fabd45ae1debeba88b79f192772JmltdHM9MTc0MjA4MzlwMA&ptn=3&ver=2&hsh=4&fclid=08d2f883-c725-6071-1353-ed9c67361f4&psq=SISTEM+PEMERINTAHAN+DI+NEGARA-NEGARA+RUMPUN+MELAYU&u=a1aHR0cDovL3JlcG9za>
- [7] I. Amerini *et al.*, “Deepfake Media Forensics : Status and Future Challenges,” pp. 1–42, 2025.
- [8] M. M. F. ramadhan. Andi Muhammad Fikri, “Law Enforcement in Child Fighting Crimes That Result in Death,” *J. Huk. HorizonPublicLegal Stud.*, vol. 4, no. 1, pp. 1–30, Feb.

2024, doi: 10.15294/panjar.v4i1.55017.

- [9] K. Angelia and Y. Pratiwi, "Mystery Box Transactions on the Tokopedia Marketplace : A Legal Analysis of Consumer Protection in Indonesian Civil Law," vol. 4, no. 4, 2025, doi: 10.30999/ph.v6i1.2810.3.
- [10] S. Walby *et al.*, *The Concept and Measurement of Violence Against Women and Men*. Chicago: The University Of Chicago, 2017.
- [11] K. K. Nawawi Fakultas Agama Islam UIKA Bogor Jl Sholeh Iskandar, "Harta Bersama Menurut Hukum Islam dan Perundang-undangan di Indonesia * (TREASURE HOUSEHOLDS ACCORDING TO ISLAMIC LAW AND POSITIVE LAW IN INDONESIA)," 2013.
- [12] K. A. El Fadl, A. A. Ahmad, and S. F. Hassan, "Routledge handbook of Islamic law," *Routledge Handb. Islam. Law*, pp. 1–450, Jan. 2019, doi: 10.4324/9781315753881.
- [13] E. Y. Purwanti, "Implementation of Environmental Education Value in Islamic Education (Analysis of Tafsir Al Qur'an Surah Al-A'raf Ayat 56-58)," *Lisyabab J. Stud. Islam dan Sos.*, vol. 2, no. 2, pp. 161–172, 2021, doi: 10.58326/jurnallisyabab.v2i2.87.
- [14] F. Hukum and U. Padjadjaran, "JURNAL BERKONFLIK DENGAN HUKUM DALAM SISTEM PERADILAN PIDANA ANAK: STUDI PADA LEMBAGA PENYELENGGARAAN KESEJAHTERAAN ISLAM I ' ANATUSH -SHIBYAN LEGAL PROTECTION OF CHILDREN IN CONFLICT WITH LAW IN JUVENILE JUSTICE SYSTEM: STUDY AT LEMBAGA PENYELENGGARAAN KESEJAHTERAAN SOSIAL YAYASAN PENDIDIKAN ISLAM I ' ANATUSH - sendiri yang setidaknya dapat dipengaruhi oleh beberapa faktor , antara lain : (1) melatarbelakangi terjadinya penyimpangan tingkah laku anak , yakni : (1) motivasi Undang-Undang Perlindungan Anak . Seorang anak belum dapat melindungi dirinya," no. 42, pp. 114–129, 2021.
- [15] D. Anindya, H. Stie, and M. Riau, "PERBANDINGAN PEMBAGIAN HARTA BERSAMA MENURUT HUKUM POSITIF DAN HUKUM ISLAM," *J. Gagasan Huk.*, vol. 03, no. 02, 2021, [Online]. Available: <https://journal.unilak.ac.id/index.php/gh/>
- [16] L. Yulianti, F. Hayati, A. Sobarna, and U. I. Bandung, "Nilai-Nilai Pendidikan Islam Berdasarkan AL- Qur ' an Surat Al - Maidah Ayat 8 long period of time . Therefore , rules are needed that are able to regulate human life fairly . The Quran has set about how humans maintains his relationship with Allah Praise," pp. 13–20.
- [17] M. F. Khoiruddin, "ETIKA BISNIS ISLAM: PELAJARAN DARI QS . AL-MUTHAFFIFIN," vol. 3, no. 3, pp. 76–86, 2025.
- [18] H. H. Nasution, N. Azizah, A. R. Siregar, M. Sosial, and P. L. Kerja, "Kebijakan Hukum

Pidana Islam dalam Upaya Penanggulangan Tindak Pidana Penipuan dengan Modus Lowongan Pekerjaan di Media Sosial Islamic Criminal Law Policy in Efforts to Combat Criminal Acts of Fraud Using Job Vacancies as a Mode on Social Media,” vol. 21, no. April, pp. 305–314, 2026.

- [19] T. Polem, ... A. T.-... : J. E. dan, and undefined 2024, “Jejak Muhammad Nejatullah Siddiqi dalam Perekonomian Islam Modern: Relevansi dan Adaptasi Teori Klasik dalam Konteks Kontemporer,” *journal.um-surabaya.ac.id*, doi: 10.30651/jms.v9i4.23164.