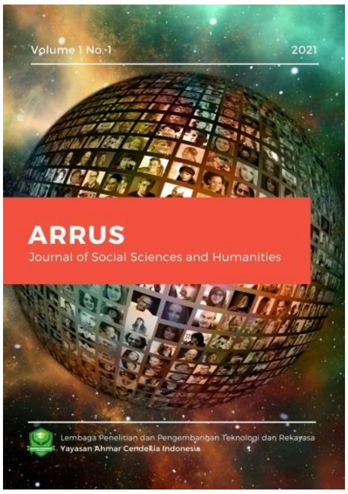
Dahlan, et.al., *ARRUS Journal of Social Sciences and Humanities*, Vol. 6, No. 4 (2026)
https://doi.org/10.35877/soshum5084

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)



*Corresponding author: Maulana Dahlan, Law Department, Faculty of Law, Brawijaya University, Malang, Indonesia

E-mail:
maulanadahlan15@student.ub.ac.id

RESEARCH ARTICLE

Regulatory Gaps in Addressing Cyber Begging in Indonesia: A Criminal Policy Perspective

Maulana Dahlan*, Yuliati, & Faizin Sulistio

Law Departement, Faculty of Law, Brawijaya University, Malang, Indonesia.

Abstract: The rapid advancement of information and communication technology has given rise to cyber begging, a phenomenon whereby individuals exploit digital platforms to solicit financial assistance from the public, often through systematic manipulation of digital empathy. This study aims to analyze the regulatory gaps within Indonesia's criminal law system concerning cyber begging practices and to formulate an ideal criminal policy response. Employing normative legal research through statute, conceptual, and comparative approaches, this study finds that Indonesia's National Criminal Code (Law No. 1/2023) and the Electronic Information and Transactions Law (Law No. 1/2024) fail to comprehensively address the characteristics of cyber begging based on digital empathy exploitation. The essence of cyber begging as a legal problem lies in four core elements: narrative manipulation, empathy exploitation, information asymmetry, and systematic economic orientation. This study proposes a multi-layered regulation model integrating preventive, administrative, and selective penal approaches grounded in the ultimum remedium principle. Criminalization should be restricted to cyber begging involving information manipulation, exploitation of vulnerable groups, and use of false identities, while honest and transparent solicitation of assistance should remain outside the scope of criminal law.

Keywords: Cyber Begging, Digital Empathy Exploitation, Criminal Law Policy, Legal Vacuum, Multi-Layered Regulation.

1. Introduction

Over the past two decades, rapid advances in information and communication technology have accelerated digital transformation across various aspects of social life. Digitalization has not only reshaped communication patterns but has also transformed economic structures, social relations, and the ways individuals seek support to meet their needs. The expansion of the internet, smartphones, and social media has created a new sphere of interaction known as cyberspace, where human activities can take place beyond geographical boundaries.

One phenomenon emerging from this digital transformation is the practice of seeking financial assistance online, commonly referred to as cyber begging. This practice occurs through social media, live-streaming features, and donation-based platforms, where individuals appeal to unknown members of the public for financial support. Unlike conventional begging, which takes place physically in streets or public spaces, cyber begging uses digital technology to reach a much wider audience within a short period of time.

The main concern arises when cyber begging is no longer limited to voluntary requests for assistance but instead involves the exploitation of digital empathy. In such cases, the public may be persuaded to donate through narratives of suffering that are manipulative,

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

exaggerated, or lacking transparency regarding the use of funds. This practice may cause economic harm, as donors may lose money without assurance that their contributions are used as intended. It may also produce social harm by reducing public trust in online donations, as well as psychological harm by exploiting sympathy and emotional vulnerability. In addition, cyber begging creates regulatory harm due to legal uncertainty, as Indonesia has not yet established specific regulations addressing this phenomenon.

This concern carries immediate practical weight in Indonesia, where digital fundraising has expanded rapidly alongside relatively low levels of digital and financial literacy among the public. Indonesia's internet user base exceeded 212 million people in 2023, with social media penetration among the highest in the world, creating an exceptionally fertile environment for digitally mediated solicitation (APJII, 2023). Reports from Indonesia's cybersecurity and consumer-protection bodies indicate that online solicitation scams, including manipulative charitable appeals, have contributed to measurable financial losses and declining public trust in digital philanthropy (BSSN, 2019). The socio-economic impact is compounded by the fact that Indonesia's poverty rate, while declining, leaves tens of millions of households economically vulnerable and therefore more susceptible to making impulsive donations in response to emotionally manipulative narratives. Because online donation platforms are increasingly used as an informal social safety net by both givers and receivers, unresolved regulatory gaps in this area carry direct socio-economic consequences: they expose donors to financial harm, distort charitable giving toward fraudulent actors, and undermine the legitimacy of genuine digital philanthropy. These consequences make the formulation of a responsive criminal policy an urgent, rather than merely theoretical, priority.

Conceptually, digital empathy exploitation can be understood as the use of pity, sympathy, and public solidarity in cyberspace through emotionally constructed narratives designed to influence people's decision to donate. Unlike conventional fraud, which generally requires a material falsehood, digital empathy exploitation operates through psychological manipulation that may not always meet the legal threshold of deception but can still produce harmful consequences (Falade, 2018).

From a criminal law perspective, digital empathy exploitation occupies a gray area. It does not always fulfill the legal elements of fraud, extortion, or threats, yet it contains elements of abuse of the victim's psychological condition. This raises a fundamental question regarding the boundaries of criminal liability in digital spaces. Sudarto (1981) emphasized that criminal law should be used selectively, while Arief (2017) argued that punishment should function as a last resort, or ultimum remedium.

Based on these considerations, this study aims to, first, analyze the characteristics and conceptual construction of cyber begging based on digital empathy exploitation within Indonesian criminal law; second, identify regulatory gaps in Indonesia's positive law concerning cyber begging practices; and third, formulate an ideal criminal policy framework to regulate and address cyber begging in the digital era. This study employs a normative legal research method using statutory, conceptual, and comparative approaches.

2. Literature Review

2.1. *Legal Certainty Theory*

Legal certainty is one of the fundamental objectives of law, alongside justice and utility. Legal norms must be formulated in a clear, precise, and predictable manner so that individuals can distinguish between conduct that is permitted and conduct that is prohibited. According to Gustav Radbruch, positive law should possess normative clarity, consistency in its application, and institutional stability in order to provide effective legal protection for society (Rahardjo, 2012).

Within the context of criminal law, legal certainty is closely associated with the principle of legality (nullum crimen, nulla poena sine lege), which provides that no individual may be

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

subjected to criminal punishment unless the prohibited conduct has been previously prescribed by law. In relation to this study, cyber begging has not been expressly regulated under either the Indonesian Criminal Code (Kitab Undang-Undang Hukum Pidana [KUHP]) or the Law on Electronic Information and Transactions (ITE Law). This regulatory omission has created a legal vacuum, resulting in uncertainty regarding whether such conduct can be classified and prosecuted as a criminal offense (Soeroso, 2011).

2.2. *Criminal Law Policy Theory*

The rapid development of information and communication technology has generated new forms of criminal activity occurring within cyberspace. These evolving characteristics of crime require continuous reform of criminal law to ensure that legal frameworks remain responsive to the dynamics of the digital society. In this regard, criminal law policy (penal policy) provides an essential theoretical framework for examining how the state formulates, implements, and enforces criminal law in addressing technology-based crimes effectively (Arief, 2018).

Sudarto argues that criminal law policy constitutes a rational effort to design and develop criminal legislation that is appropriate and responsive to the needs of society. Similarly, Barda Nawawi Arief emphasizes that criminal law should function as an instrument of social protection (social defence) and should be applied selectively as an ultimum remedium, meaning that criminal sanctions should only be imposed when other legal mechanisms are insufficient to address the problem effectively (Adji, 2018). This perspective suggests that criminalization should not be excessive but must instead be guided by considerations of justice, public benefit, proportionality, and the overall effectiveness of law enforcement.

2.3. *Theory of Punishment*

The theory of punishment explains both the normative justification and the objectives underlying the imposition of criminal sanctions on offenders. Four major theories are generally recognized. First, the retributive theory emphasizes punishment as a proportionate response to violations of the law. Second, the preventive theory focuses on deterrence through both general prevention (general deterrence) and special prevention (special deterrence). Third, the rehabilitative theory seeks to reform offenders by promoting behavioral change and social reintegration. Fourth, the restorative theory prioritizes restoring relationships among offenders, victims, and the broader community through processes of accountability and reconciliation (Chazawi, 2010).

In the context of cyber begging, punishment theory provides an important analytical framework for assessing whether criminal sanctions constitute the most appropriate response or whether non-penal approaches should be prioritized. Not all individuals engaged in cyber begging should necessarily be subjected to criminal punishment, particularly when their conduct is primarily driven by structural poverty or socioeconomic vulnerability. However, where cyber begging involves elements of fraud, deception, exploitation, or manipulation, preventive criminal sanctions may be justified as a means of protecting the public and maintaining public trust in digital environments.

3. Research Method

This study employs normative legal research (doctrinal legal research), which focuses on the examination of secondary legal materials, particularly primary legal sources derived from statutory regulations and other formal legal instruments. Three complementary research approaches are applied. First, the statutory approach examines relevant legislation as the primary source of legal analysis. Second, the conceptual approach draws upon established legal doctrines, theories, and scholarly opinions to construct the analytical framework. Third, the comparative approach compares the regulation of criminal law concerning cyber begging in Indonesia with the legal frameworks adopted in three specifically selected foreign jurisdictions: Saudi Arabia, which has amended its Anti-Begging Law (Royal Decree No.

M/20 of 2021) to explicitly cover digital solicitation; the United Arab Emirates, which enacted a distinct offense of begging by information-technology means under Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes; and Jordan, which has adopted a predominantly administrative approach through its Ministry of Social Development since 2019. These three jurisdictions were selected because they represent a spectrum of regulatory responses from full criminalization (Saudi Arabia and UAE) to administrative regulation (Jordan) within legal traditions that share with Indonesia an emphasis on social order and the protection of vulnerable groups. The comparison aims to identify regulatory similarities, differences, and potential policy alternatives that may inform Indonesia's legislative reform (Muhaimin, 2020; Adiyanta, 2019; Bourtal, 2025).

The legal materials used in this research consist of three categories. Primary legal materials include Law No. 1 of 2023 on the Indonesian Criminal Code (KUHP) and Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (ITE Law). Secondary legal materials comprise legal doctrines, scholarly journal articles, and previous research relevant to cybercrime, criminal law, and criminal policy. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference sources that support the interpretation of legal concepts.

4. Results and Discussion

4.1. *The Phenomenon of Cyber Begging as Digital Empathy Exploitation*

The rapid advancement of information and communication technology has fundamentally transformed various aspects of modern society, including the ways individuals interact, work, and generate income. The widespread adoption of the internet and social media has not only created new channels of communication but has also fostered a digital economic ecosystem in which individuals can obtain financial benefits through a wide range of online activities. Within this evolving landscape, numerous new forms of digital occupations and economic activities have emerged that were previously unknown in conventional society, including content creators, influencers, live streamers, affiliate marketers, and platform-based crowdfunding initiatives. At the same time, technological advancement has also given rise to various forms of social behavior that exist within a legal gray area, one of which is the phenomenon of cyber begging.

Cyber begging refers to the practice of soliciting financial assistance or obtaining economic benefits through digital media by utilizing the internet as the primary platform. Unlike conventional street begging, which takes place through face-to-face interactions in public spaces, cyber begging relies on digital platforms such as TikTok, Instagram, Facebook, YouTube, and other live-streaming applications to reach substantially larger audiences without geographical limitations. Falade (2018) defines cyber begging as a form of online solicitation in which individuals request money from strangers to satisfy either urgent needs or planned personal objectives.

The legal and social concerns arise when such activities involve information manipulation and the exploitation of public emotions. In practice, many cyber beggars deliberately construct narratives of hardship, vulnerability, or personal suffering to attract public sympathy. These narratives are strategically designed to evoke compassion, pity, and empathy, thereby increasing the likelihood that audiences will provide financial contributions. Research conducted by Dhamayanti, Sari, and Rahmawati (2024) demonstrates that some cyber beggars intentionally cultivate emotional relationships with their audiences in order to sustain a continuous flow of donations.

One of the most widely discussed cases in Indonesia involved a live-streaming broadcast in which an elderly individual was repeatedly shown bathing in mud for extended periods to generate virtual gifts from viewers. The incident sparked significant public debate regarding the boundaries between digital creativity, human exploitation, and online begging. From a sociological perspective, this phenomenon illustrates the commodification of empathy,

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

whereby social and moral values are transformed into economic assets that can be exchanged within digital markets. In the context of cyber begging, empathy which fundamentally represents a moral and social value is converted into an economic instrument with measurable financial value.

The characteristics of digital environments further reinforce this phenomenon. The internet enables perpetrators to reach thousands or even millions of users within a relatively short period while incurring minimal operational costs. Moreover, the anonymity afforded by cyberspace makes it difficult for potential donors to verify the authenticity of the information presented by cyber beggars. Consequently, a condition of information asymmetry emerges, consistent with George Akerlof's (1970) The Market for Lemons theory, in which donors lack sufficient information to accurately evaluate the credibility of the narratives used to solicit financial assistance. This informational imbalance creates opportunities for deception, emotional manipulation, and various forms of digital exploitation that challenge existing legal frameworks governing online activities.

4.2. *The Conceptual Construction of Cyber Begging under Indonesian Criminal Law*

4.2.1. *An Analytical Framework Based on Digital Empathy Exploitation*

This study analyzes cyber begging through the framework of digital empathy exploitation. This approach is grounded in the assumption that the principal legal concern surrounding cyber begging does not lie in the act of requesting financial assistance itself, but rather in the deliberate exploitation of the public's psychological and emotional responses for economic gain. Within this framework, four key indicators constitute the conceptual foundation of cyber begging.

The first indicator is narrative manipulation. Narratives serve as the primary instrument through which cyber beggars shape public perceptions and influence audience behavior. In digital communication, narratives possess the capacity to construct meaning, evoke emotional responses, and influence individuals' perceptions of social reality (Couldry, 2012). Narrative manipulation occurs when individuals intentionally create, exaggerate, distort, or fabricate stories to generate public sympathy and increase the likelihood of receiving financial support.

The second indicator is empathy exploitation. Empathy fundamentally refers to an individual's capacity to understand and share the emotional experiences of others. Within social life, empathy performs an important prosocial function by encouraging solidarity, compassion, and assistance toward individuals experiencing hardship (Batson, 2011). However, within digital environments, empathy may be transformed into an economic resource that is deliberately exploited for financial benefit. Rather than functioning solely as a moral value, empathy becomes a strategic mechanism for attracting donations and sustaining economic transactions within online platforms.

The third indicator is information asymmetry. The concept of information asymmetry describes a situation in which one party possesses substantially more information than another, thereby creating an imbalance in decision-making processes (Akerlof, 1970). In cyber begging, perpetrators generally possess complete knowledge regarding their actual circumstances, whereas potential donors rely exclusively on information presented through digital narratives. This informational imbalance limits donors' ability to verify the authenticity of claims and consequently increases their vulnerability to deception and emotional manipulation.

The fourth indicator is systematic economic purpose. Not every activity that evokes public empathy should be categorized as cyber begging. The defining characteristic lies in the intentional pursuit of direct or indirect economic gain through the systematic exploitation of public emotions. Based on these four indicators, this study defines cyber begging based on digital empathy exploitation as any activity conducted through digital media to obtain economic benefits by creating or exploiting particular narratives that intentionally evoke

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

public empathy, capitalize on information asymmetry between the perpetrator and the audience, and systematically convert emotional responses into financial gain.

Translating these four sociological and communicative indicators into legal elements requires distinguishing them analytically from ordinary descriptive or communication-theory constructs. Narrative manipulation and empathy exploitation correspond to the unlawfulness (wederrechtelijkheid) element of an offense, insofar as they describe the deceptive or exploitative manner in which assistance is solicited; information asymmetry functions evidentially, marking the point at which a donor's reasonable reliance on the perpetrator's representations becomes legally significant; and systematic economic purpose supplies the element of intent (dolus), signifying a deliberate and repeated pursuit of financial gain rather than an isolated, honest appeal for help. Read together, these four indicators are proposed not as freestanding sociological categories but as an analytical bridge that operationalizes digital empathy exploitation into elements a prosecutor would need to establish under the actus reus, unlawfulness, and mens rea framework discussed in the following section.

4.2.2. Analysis of the Elements of Criminal Offenses in Cyber Begging

Determining whether particular conduct constitutes a criminal offense represents a fundamental inquiry within criminal law. In the context of cyber begging, the primary legal challenge arises from the absence of explicit statutory provisions regulating such conduct under Indonesian legislation. According to Moeljatno (2008), a criminal offense refers to an act prohibited by law and accompanied by the threat of criminal sanctions for those who violate the legal prohibition.

From the perspective of actus reus, activities such as conducting live-streaming broadcasts, uploading digital content, soliciting donations, presenting particular narratives, and receiving virtual gifts constitute voluntary human acts performed consciously by the perpetrator. However, from the standpoint of wederrechtelijkheid (unlawfulness), the legal assessment becomes considerably more complex. The element of unlawfulness arises only when cyber begging involves deceptive conduct, including the manipulation of information, the dissemination of false statements, the exploitation of vulnerable individuals, or the use of false identities that induce members of the public to make decisions based on misleading information (Lamintang, 2014).

With respect to mens rea, the principle of geen straf zonder schuld (no punishment without fault) establishes that criminal liability may only be imposed when culpability can be attributed to the offender (Sudarto, 2018). In cyber begging, the element of fault is most appropriately examined through the concept of intent (dolus). Intent is established when an individual deliberately fabricates narratives of hardship, misrepresents personal circumstances, uses false identities, or exploits the vulnerable conditions of others to obtain financial contributions. Conversely, where an individual is genuinely experiencing economic hardship and truthfully requests assistance without engaging in deception or manipulation, the element of criminal fault necessary to establish criminal liability becomes considerably more difficult to prove.

From the perspective of criminal responsibility, Van Hamel argues that an individual may be considered criminally responsible only if he or she possesses the capacity to understand the consequences of the conduct, recognize its social significance, and exercise control over his or her own actions (Chazawi, 2010). In most cases of cyber begging, perpetrators consciously utilize digital technology as a means of obtaining economic benefits. Nevertheless, criminal responsibility cannot be imposed solely because an individual seeks financial assistance through online platforms. Rather, criminal liability should depend upon the existence of additional elements, particularly deception, fraudulent intent, manipulation, or other forms of unlawful conduct that justify the intervention of criminal law.

4.3. *Regulatory Gaps in Indonesia's Positive Law*

4.3.1. Analysis of the Indonesian Criminal Code in Relation to Cyber Begging

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

The Indonesian Criminal Code enacted under Law No. 1 of 2023 does not contain any provision that specifically regulates cyber begging. Historically, Indonesian criminal law has recognized the offense of begging. Under the former Criminal Code, begging was regulated under Article 504, which provided that individuals engaging in begging in public places could be subject to imprisonment. In contrast, the 2023 Criminal Code regulates the issue under Article 425, which primarily focuses on prohibiting the exploitation of minors for begging rather than criminalizing begging itself.

Nevertheless, cyber begging differs fundamentally from conventional begging. It is conducted through digital platforms, relies on information and communication technologies, and enables perpetrators to reach audiences without geographical limitations. These distinctive characteristics prevent traditional criminal provisions on begging from being automatically applied to cyber begging. Although the offense of fraud may potentially encompass certain forms of cyber begging, its application is limited to situations in which objective evidence of deception or fraudulent conduct can be established. In practice, however, many forms of cyber begging based on digital empathy exploitation do not involve explicit falsehoods but instead operate through psychological manipulation, making them difficult to prosecute under conventional criminal law provisions.

4.3.2. Analysis of the Electronic Information and Transactions (ITE) Law

Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions (ITE) Law represents another relevant legal instrument because all cyber begging activities are conducted through electronic media. However, most criminal provisions under the ITE Law were designed to address offenses with clearly identifiable characteristics, including unauthorized access to electronic systems, manipulation of electronic data, dissemination of false information, online defamation, and electronic fraud. By contrast, digital empathy exploitation represents a more complex phenomenon that operates primarily through psychological mechanisms rather than overtly unlawful technological conduct (Brenner, 2010; Koops, 2006).

The ITE Law may be applicable where cyber begging involves the dissemination of false information, the use of false identities, manipulation of electronic data, or other deceptive conduct that satisfies the criminal elements set forth under Articles 27, 28, and 29 of the ITE Law. However, where cyber begging relies solely on the exploitation of public empathy without involving objectively verifiable falsehoods or fraudulent misrepresentations, the ITE Law does not provide an adequate legal basis for criminal prosecution. According to Al Asyari (2023), the ITE Law primarily focuses on cybercrime, illegal online content, and the misuse of internet technologies, rendering it insufficiently adaptive to emerging legal gray-area phenomena such as cyber begging

4.3.3. Protection of Vulnerable Groups and Existing Legal Loophole

One distinguishing characteristic of contemporary cyber begging is the frequent exploitation of vulnerable groups as instruments for generating economic gain. Across various social media platforms, perpetrators often feature children, older adults, persons with disabilities, and individuals experiencing difficult socioeconomic conditions in order to evoke public sympathy and encourage financial contributions.

Although Law No. 35 of 2014 on Child Protection provides legal safeguards against the economic exploitation of children, its application to cyber begging remains challenging because of evidentiary limitations. Likewise, the United Nations Convention on the Rights of the Child (1989) and the Convention on the Rights of Persons with Disabilities (2006) recognize the right of vulnerable groups to be protected from all forms of exploitation. However, within the context of cyber begging, the exploitation of vulnerable individuals is frequently carried out in ways that do not produce sufficient material evidence to satisfy the formal legal elements required to establish the criminal offense of exploitation (Lestari, 2020).

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

The Circular Letter of the Indonesian Minister of Social Affairs No. 2 of 2023 concerning the Prohibition and Control of Begging Practices in Public Spaces and Cyberspace is currently the only governmental policy instrument that explicitly addresses online begging. Nevertheless, the Circular Letter has significant limitations because it merely constitutes an administrative policy recommendation rather than a legally binding criminal regulation. It does not establish clear enforcement procedures or criminal sanctions, resulting in inconsistent implementation across different regions of Indonesia.

4.3.4. Digital Platform Policies and Their Limitations

Major digital platforms, including TikTok, Instagram (Meta), and YouTube, have developed self-regulatory mechanisms intended to address various forms of technological misuse. TikTok's Community Guidelines prohibit content that promotes the exploitation of individuals or vulnerable circumstances. Similarly, Meta prohibits content involving the exploitation of children or the commercialization of human suffering, while YouTube restricts the monetization of content that depicts degrading or dehumanizing activities.

Despite these efforts, self-regulation faces significant structural limitations. Black (2008) argues that self-regulatory frameworks frequently encounter conflicts of interest because digital platforms pursue commercial objectives that do not always align with broader public interests. Furthermore, platform policies lack the legal authority and enforceability of statutory regulations. Consequently, in cases where cyber begging results in substantial social harm or involves the exploitation of vulnerable individuals, self-regulatory mechanisms often fail to provide adequate legal protection or ensure consistent accountability. These limitations underscore the need for a comprehensive statutory framework capable of addressing the unique legal and ethical challenges posed by cyber begging in the digital era.

4.3.5. Comparative Perspectives from Other Jurisdictions

A genuinely comparative reading of cyber begging regulation shows that several jurisdictions, particularly within civil law and Gulf legal traditions, have moved further than Indonesia toward explicit criminalization of digitally mediated begging. Saudi Arabia's Anti-Begging Law (Royal Decree No. M/20 of 2021) defines begging broadly enough to capture solicitation "in public places, shops, or through modern means of technology and communication," thereby extending an existing offense to digital conduct rather than leaving it in a separate legal category (Bourtal, 2025). The United Arab Emirates goes further still: Article 51 of Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes creates a distinct offense of begging by information-technology means, punishable by imprisonment of up to three months and a fine, and separately penalizes bad-faith appeals for assistance directed at government entities (Bourtal, 2025). Jordan, by contrast, has addressed the problem primarily through administrative rather than penal channels, empowering its Ministry of Social Development since 2019 to pursue unlicensed online fundraising in coordination with financial authorities, without necessarily treating every instance as a criminal matter (Bourtal, 2025).

These comparative examples are instructive for two reasons. First, they confirm that legal systems addressing this phenomenon converge on similar underlying concerns to those identified in this study deception, exploitation of vulnerable groups, and organized, profit-driven solicitation even though they differ in whether the primary response is penal (Saudi Arabia, UAE) or administrative (Jordan). Second, Algeria's continued reliance on a traditional, technologically neutral begging provision, despite scholarly calls for a dedicated electronic-begging offense, illustrates the same regulatory lag observed in Indonesia, and reinforces the argument that technologically neutral penal codes are ill-suited to capturing conduct that is defined by its digital method and empathy-based manipulation rather than by the act of begging alone (Bourtal, 2025). Rather than adopting wholesale criminalization on the Gulf model, however, this study finds Jordan's layered administrative approach more compatible with Indonesia's ultimum remedium tradition, and accordingly draws on it,

https://doi.org/10.35877/soshum5084

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

together with the UAE's narrower penal provision for deceptive appeals, in constructing the multi-layered regulatory model proposed in Section 4.4.

4.4. *Toward an Ideal Criminal Law Policy for Regulating Cyber Begging*

4.4.1. *The Urgency of Establishing a Criminal Law Policy*

According to Radbruch (2006), one of the fundamental objectives of law is to ensure legal certainty. In the context of cyber begging, the absence of a clear legal framework has resulted in differing interpretations among the public, law enforcement authorities, and digital platform providers regarding the legality of such practices. Arief (2017) argues that criminal law fundamentally serves as an instrument for protecting legal interests that society considers essential.

Cyber begging has the potential to undermine several protected legal interests, including public trust, the protection of vulnerable groups, the integrity of digital spaces, and the certainty of social interactions and electronic transactions. Fukuyama (1995) explains that social trust constitutes an essential form of social capital within modern societies. When trust is eroded by manipulative practices, broader social solidarity is likewise weakened, ultimately reducing public confidence in digital communication and online charitable activities.

The urgency of developing a criminal law policy does not imply that every form of cyber begging should be criminalized. Sudarto (2018) emphasizes that criminal law should be applied selectively and proportionately because criminal punishment functions as an ultimum remedium, or a measure of last resort, in addressing social problems. Accordingly, policymakers must avoid the criminalization of poverty, which contradicts the broader objectives of criminal law and the pursuit of social justice (Wacquant, 2009).

4.4.2. *A Model of Selective Criminalization*

The findings of this study indicate that a blanket criminalization approach encompassing all forms of cyber begging would constitute an inappropriate legal policy. Duff (2018) argues that criminal law should be directed toward conduct that produces social harm rather than behavior that is merely considered morally objectionable. Likewise, Arief (2017) warns that excessive criminalization may result in overcriminalization, ultimately diminishing the effectiveness and legitimacy of criminal law enforcement.

This study proposes four indicators as the basis for the selective criminalization of cyber begging. First, narrative manipulation, involving the creation or dissemination of misleading or fabricated information for economic gain. Second, empathy exploitation, whereby perpetrators intentionally capitalize on suffering, hardship, or vulnerable conditions to obtain financial benefits. Third, intentional information asymmetry, in which perpetrators knowingly exploit the public's limited access to accurate information in order to create false perceptions. Fourth, systematic economic purpose, characterized by repeated, organized, and sustained activities designed to generate continuous financial profit.

Based on these indicators, this study proposes classifying cyber begging into three categories. The first is social cyber begging, which consists of honest, transparent, and genuine requests for assistance and therefore should not be subject to criminal sanctions. The second is manipulative cyber begging, involving misleading information or deceptive narratives that warrant closer legal oversight and administrative intervention. The third is exploitative cyber begging, involving the exploitation of children, older persons, persons with disabilities, or other vulnerable groups as instruments for generating public sympathy and financial contributions. This final category represents the most serious form of cyber begging and should be considered appropriate for criminal sanctions (Nurullah et al., 2024).

4.4.3. *A Multi-Layered Regulatory Model*

The increasing prevalence of cyber begging demonstrates that reliance on criminal law alone is insufficient to provide effective protection for society. Consistent with Barda Nawawi

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Arief's (2017) concept of criminal policy, crime prevention should combine penal and non-penal measures. Accordingly, this study proposes a multi-layered regulatory model consisting of three complementary levels of intervention.

The first layer consists of preventive policies designed to reduce the occurrence of cyber begging before it causes broader social harm. These measures include strengthening digital literacy and promoting responsible online donation practices. Livingstone (2014) emphasizes that digital literacy encompasses not only technological competence but also the ability to critically evaluate information and recognize risks within digital environments. Preventive strategies should therefore include public awareness campaigns promoting transparency and accountability in digital fundraising, alongside strengthened social welfare programs aimed at reducing the economic vulnerability that often motivates online begging.

The second layer involves administrative regulation focusing on improving platform governance. Recommended measures include requiring verification mechanisms for publicly conducted online fundraising activities, imposing obligations on digital platforms to actively monitor content indicating the exploitation of vulnerable individuals, and authorizing administrative sanctions such as restricting content visibility, suspending monetization features, removing accounts, or blocking access to offending content. This approach is consistent with the theory of responsive regulation, which views regulatory intervention as a graduated process employing increasingly stringent measures when voluntary compliance proves inadequate (Ayres & Braithwaite, 1992).

The third layer consists of selective penal intervention, reserved exclusively for exploitative forms of cyber begging that cause substantial social harm. Criminal sanctions should be imposed only where cyber begging: (1) involves deceptive information or false identities; (2) exploits children, older persons, persons with disabilities, or other vulnerable groups; (3) is conducted in an organized manner for systematic economic gain; and (4) causes demonstrable social or economic harm. Under this model, criminal law functions as an ultimum remedium, consistent with the principles advanced by Sudarto (2018) and Arief (2017).

A recurring practical challenge for this model is how law enforcement can distinguish genuine, honest requests for assistance from manipulative cyber begging without unduly restricting freedom of expression or the right to seek help. Because narrative manipulation and empathy exploitation are, by definition, difficult to observe directly, this study proposes that investigators rely on objective, verifiable indicators rather than subjective assessments of a narrative's sincerity: repeated or serialized fundraising for claims that cannot be substantiated, discrepancies between the funds solicited and documented needs, the use of multiple accounts or false identities to solicit the same claim, and the systematic, organized character of the activity. Limiting administrative and penal scrutiny to these observable patterns rather than to the emotional tone of an appeal helps ensure that civil liberties, particularly the right to request help in situations of genuine hardship, are not compromised by an overly broad application of the model.

The practical success of the administrative layer also depends on the institutional capacity of the Ministry of Social Affairs, which is currently designated as the lead agency under the 2023 Circular Letter but operates without dedicated digital-monitoring infrastructure, specialized cyber-investigation staff, or direct authority to compel platform cooperation. Strengthening this capacity would require, at minimum, a memorandum of understanding between the Ministry, the Ministry of Communication and Digital Affairs, and major platform operators to enable expedited content review; a dedicated unit trained to verify fundraising claims and coordinate with regional social services; and a clear escalation pathway referring cases that meet the criminalization threshold in Section 4.4.b to law enforcement. Without such capacity-building, the multi-layered model risks remaining a normatively sound but practically unenforceable framework, echoing the same implementation gap that has limited the effectiveness of the existing Circular Letter.

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

4.4.4. Policy Reconstruction and Normative Formulation

The emergence of cyber begging demonstrates a widening gap between the realities of the digital society and the existing legal framework. Consequently, criminal law policy should shift its regulatory focus from the traditional concept of begging toward the broader concept of digital empathy exploitation. Retaining the traditional focus on the act of requesting assistance risks criminalizing individuals who genuinely require support. Conversely, emphasizing digital empathy exploitation enables criminal law to identify more precisely those forms of conduct that generate genuine social harm.

Accordingly, this study proposes that the concept of digital empathy exploitation be expressly recognized within Indonesia's national criminal law policy. Such recognition should not encompass every instance of cyber begging but should instead apply only to conduct satisfying the following cumulative elements: (1) intentional pursuit of economic gain; (2) reliance on misleading information or fabricated circumstances; (3) exploitation of vulnerable groups or human suffering; and (4) the creation of measurable social or economic harm.

An ideal criminal law policy for regulating cyber begging should therefore be founded upon three fundamental principles. First, the principle of selectivity, under which only cyber begging involving manipulation and exploitation is subject to criminal sanctions. Second, the principle of proportionality, which positions criminal law as a measure of last resort after preventive and administrative interventions have proven ineffective. Third, the principle of protecting vulnerable groups, which prioritizes safeguarding children, older persons, persons with disabilities, and other individuals who are particularly susceptible to digital exploitation (Kristanto & Rakhmat, 2025). Furthermore, effective implementation of this policy requires international cooperation, including collaboration within the United Nations framework, to strengthen cross-border cybercrime prevention and promote a coordinated response to emerging forms of digital exploitation (Nuraeny, 2011).

4.5. *Findings And Theoretical Implications*

This study produces four principal findings. First, cyber begging constitutes an emerging legal phenomenon that has not been adequately accommodated within Indonesia's existing legal framework. Neither the Indonesian Criminal Code (Law No. 1 of 2023) nor the Electronic Information and Transactions (ITE) Law comprehensively addresses the distinctive characteristics of cyber begging based on digital empathy exploitation. This regulatory deficiency reflects a legal vacuum that creates uncertainty regarding the legal status of such conduct and limits the effectiveness of criminal law enforcement.

Second, the defining characteristic of cyber begging lies not in the act of requesting financial assistance through digital media, but rather in the systematic exploitation of digital empathy for economic gain. This study identifies four essential elements that collectively constitute cyber begging based on digital empathy exploitation: narrative manipulation, empathy exploitation, information asymmetry, and systematic economic purpose. Together, these elements form a cycle of digital empathy exploitation that represents the central criminal law concern underlying contemporary cyber begging (International Journal of Cyber Criminology, 2019; BSSN, 2019).

Third, not every form of cyber begging should be subject to criminal sanctions. A clear distinction must be drawn between genuine, honest, and transparent requests for assistance and exploitative forms of cyber begging that manipulate public emotions for financial benefit. Overly broad criminalization risks contributing to the criminalization of poverty, a consequence that is inconsistent with the principles of social justice and proportionality in criminal law (Wacquant, 2009; Pansariadi & Soekorini, 2023).

Fourth, a multi-layered regulatory model offers a more effective policy response than comprehensive criminalization. Because cyber begging encompasses legal, social, economic, technological, and psychological dimensions, an effective regulatory framework should integrate preventive, administrative, and selective penal measures. Such an approach is

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

consistent with Arief's (2017) conception of criminal policy, which emphasizes that crime prevention should combine penal and non-penal strategies in a complementary manner to achieve greater effectiveness and social protection (Idy, 2022).

From a theoretical perspective, this study contributes to the development of criminal law scholarship by introducing the concept of digital empathy exploitation as a normative analytical framework for understanding cyber begging. Rather than conceptualizing cyber begging solely as an online form of begging, this framework shifts the analytical focus toward the exploitation of emotional vulnerability and information asymmetry as the principal sources of legal harm. Consequently, the proposed framework provides a more precise basis for distinguishing between legitimate online fundraising and exploitative digital practices, while also offering a conceptual foundation for future criminal law reform in response to emerging forms of technology-enabled social exploitation.

5. Conclusion

This study concludes that cyber begging based on digital empathy exploitation represents an emerging legal phenomenon that has not been adequately accommodated within Indonesia's current legal framework. Neither the Indonesian Criminal Code (Law No. 1 of 2023) nor the Electronic Information and Transactions (ITE) Law (Law No. 1 of 2024) comprehensively addresses the distinctive characteristics of cyber begging, particularly those involving narrative manipulation, information asymmetry, and the systematic monetization of public empathy. While the ITE Law may apply to cases involving objectively verifiable deception or manipulation of electronic information, it remains insufficient to regulate exploitative practices that rely primarily on psychological and emotional manipulation. Accordingly, this study argues that the legal focus should shift from the traditional concept of online begging toward the broader concept of digital empathy exploitation, providing a more appropriate normative framework for identifying harmful conduct while avoiding the criminalization of genuine requests for assistance.

Based on these findings, this study recommends the development of a multi-layered regulatory framework that integrates preventive, administrative, and penal measures in accordance with the principle of ultimum remedium. Criminal sanctions should be applied selectively and limited to cyber begging involving intentional deception, the exploitation of vulnerable groups, false identities, or other forms of conduct that produce demonstrable social harm. Furthermore, legislators should consider incorporating the concept of digital empathy exploitation into future criminal law reform, either through amendments to the ITE Law or through dedicated legislation governing digital fundraising activities. In parallel, digital platforms should strengthen verification and content moderation mechanisms, while the government should expand digital literacy initiatives to improve public awareness, encourage responsible online donations, and enhance protection against exploitative practices in the digital environment.

References

Adiyanta, F. C. S. (2019). Hukum dan studi penelitian empiris: Penggunaan metode survey sebagai instrumen penelitian hukum empiris. Administrative Law and Governance Journal, 2(4), 697–709. https://doi.org/10.14710/alj.v2i4.697-709

Adji, I. S. (2018). Kebijakan kriminal dalam perspektif hukum pidana. Diadit Media.

Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84(3), 488–500. https://doi.org/10.2307/1879431

Al Asyari, H. (2023). Between freedom and protection: A critical review of Indonesia's cyberspace law. Prophetic Law Review, 5(1), 79–103. https://doi.org/10.20885/plr.vol5.iss1.art5

Arief, B. N. (2017). Bunga rampai kebijakan hukum pidana. Prenadamedia Group.

Arief, B. N. (2018). Masalah penegakan hukum dan kebijakan hukum pidana. Prenada Media.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2023). Laporan survei pengguna internet Indonesia 2022–2023. APJII.

Ayres, I., & Braithwaite, J. (1992). Responsive regulation: Transcending the deregulation debate. Oxford University Press.

Badan Siber dan Sandi Negara (BSSN). (2019). Laporan tahunan keamanan siber: Modus penipuan dan eksploitasi empati di dunia maya. BSSN RI.

Batson, C. D. (2011). Altruism in humans. Oxford University Press.

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & Governance, 2(2), 137–164.

Bourtal, A. (2025). Criminalization of electronic begging in Algerian legislation. Law and World, 11(36), 137–150. https://doi.org/10.36475/11.4.7

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

Chazawi, A. (2010). Stelsel pidana, tindak pidana, teori-teori pemidanaan dan batas berlakunya hukum pidana (Cetakan V). Raja Grafindo Persada.

Couldry, N. (2012). Media, society, world: Social theory and digital media practice. Polity Press.

Dhamayanti, E. A., Sari, P., & Rahmawati. (2024). Eksplorasi interaksi simbolik pengemis online pada ekosistem TikTok: Motif, relasi emosional, dan pola ketergantungan donasi digital. Jurnal Ilmu Komunikasi, 6(1), 1–15.

Duff, R. A. (2018). The realm of criminal law. Oxford University Press.

Falade, D. A. (2018). Cyber begging and online survival strategies in the digital age. International Journal of Cyber Society and Education, 11(2), 45–60.

Fukuyama, F. (1995). Trust: The social virtues and the creation of prosperity. Free Press.

Idy. (2022). Implementasi kebijakan hukum pidana dalam penanggulangan kejahatan di bidang komputer. PLENO JURE, 11(2), 142–158.

Instagram. (2025, Maret). Pedoman komunitas. https://help.instagram.com/477434105621119

International Journal of Cyber Criminology. (2019). Digital sympathy exploitation: Online begging and fraudulent appeals, 13(4).

Jordan Ministry of Social Development. (2019). Decision on the control of unlicensed online donations and electronic begging.

Kristanto, K., & Rakhmat, B. (2025). Tindak pidana siber di Indonesia: Regulasi, tantangan, dan penegakan hukum. PT Media Penerbit Indonesia.

Lamintang, P. A. F. (2014). Dasar-dasar hukum pidana Indonesia. Sinar Baru.

Lestari, R. (2020). Perlindungan hukum terhadap anak dalam kejahatan dunia maya: Studi kasus cyber begging. Jurnal Hukum dan HAM, 12(2).

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. Communications, 39(3), 283–303.

Meta. (2024). Community standards. Meta Platforms Inc.

Moeljatno. (2008). Asas-asas hukum pidana. Rineka Cipta.

Muhaimin. (2020). Metode penelitian hukum. Mataram University Press.

Nuraeny, H. (2011). Tindak pidana perdagangan orang (kebijakan hukum pidana dan pencegahannya). Sinar Grafika.

Nurullah, A. R., et al. (2024). Sociological and social policy review of the cyberspace begging phenomenon. Interdisciplinary Explorations in Research Journal, 2(2), 621–630.

Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak pidana cyber crime dan penegakan hukumnya. Binamulia Hukum, 12(2).

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Peraturan Pemerintah Republik Indonesia Nomor 31 Tahun 1980 tentang Penanggulangan Gelandangan dan Pengemis.

Radbruch, G. (2006). Legal philosophy. Oxford University Press.

Rahardjo, S. (2012). Ilmu hukum. Citra Aditya Bakti.

Saudi Arabia. (2021). Anti-Begging Law, Royal Decree No. M/20 (September 16, 2021).

Soeroso. (2011). Pengantar ilmu hukum. PT. Sinar Grafika.

Sudarto. (1981). Hukum dan hukum pidana. Alumni. Bandung.

Sudarto. (2018). Hukum pidana I. Yayasan Sudarto.

Surat Edaran Menteri Sosial Republik Indonesia Nomor 2 Tahun 2023 tentang Larangan dan Penertiban Praktik Mengemis di Ruang Publik dan Dunia Maya.

TikTok. (2024). Community guidelines. TikTok Pte. Ltd.

TikTok. (2025, Maret). Pedoman komunitas TikTok. https://www.tiktok.com/community-guidelines

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak.

United Arab Emirates. (2021). Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes.

United Nations. (1989). Convention on the rights of the child. United Nations.

United Nations. (2006). Convention on the rights of persons with disabilities. United Nations.

Wacquant, L. (2009). Punishing the poor: The neoliberal government of social insecurity. Duke University Press.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

YouTube. (2024). YouTube community guidelines and partner program policies. Google LLC.