The Spirit of Society Journal
International Journal of Society Development and Engagement
LPPM - Universitas Narotama
ISSN : 2594 - 4777 (Online)
2597 - 4742 (Print)
https://jurnal.narotama.ac.id/index.php/scj/index

Digital Reputation as a Protected Economic Interest under Indonesian Criminal Law

Evi Retno Wulan*, Arief Budiman

Faculty of Law, Universitas Narotama

Corresponding author: evi.retno@narotama.ac.id

Abstract: The rapid expansion of Indonesia's digital economy has transformed online reputation into a measurable economic asset for Micro Small and Medium Enterprises, as algorithm-based rating systems directly determine visibility, consumer trust, and revenue sustainability. Despite its growing economic significance, the juridical status of digital reputation within Indonesian criminal law remains underdeveloped. This article examines whether online review extortion may be prosecuted under Law Number 1 Year 2023 concerning the Criminal Code and Law Number 11 Year 2008 concerning Electronic Information and Transactions as amended by Law Number 1 Year 2024. Using a normative juridical method with systematic and teleological interpretation, the study analyses the structural elements of extortion, including unlawful threat, intent, causality, attempt, participation, and corporate liability, in the context of algorithm based reputational manipulation. The analysis demonstrates that Articles 482 and 483 of the Criminal Code, together with Article 27B of the Electronic Information and Transactions Law, provide a normative basis to prosecute digital coercion when reputational harm is conditionally linked to economic demand. However, neither statute explicitly recognizes digital reputation as an independent protected economic interest. This normative silence creates interpretative ambiguity and risks inconsistent enforcement. This article contributes to criminal law doctrine by conceptualizing digital reputation as a legally relevant economic interest within the framework of economic autonomy protection. Strengthening doctrinal clarity is therefore essential to ensure legal certainty, enhance deterrence, and reinforce the integrity of Indonesia's digital economic governance.

Keywords: digital reputation, online review extortion, economic coercion, Indonesian Criminal Code 2023, Electronic Information and Transactions Law

INTRODUCTION

The development of the digital economy in Indonesia has significantly transformed the structure of commercial interaction. Micro Small and Medium Enterprises, as a central pillar of the national economy, increasingly rely on digital platforms to access markets, expand consumer networks, and maintain competitiveness. Within this digital ecosystem, rating systems and consumer reviews function as indicators of credibility and quality. Digital reputation therefore no longer represents merely social perception but constitutes a measurable economic asset that directly affects transaction volume and business sustainability.

The dependence on digital reputation mechanisms creates new legal consequences. A growing phenomenon known as online review extortion has emerged, whereby individuals intentionally publish or threaten to publish negative reviews on digital platforms with the purpose of obtaining economic benefit. Such conduct exploits algorithmic systems and public perception to pressure business actors into transferring money or other advantages. Unlike conventional defamation, which primarily protects personal honour and dignity, this practice targets economic autonomy by manipulating digital visibility.

This phenomenon raises fundamental questions within the Indonesian criminal law framework. Law Number 1 Year 2023 concerning the Criminal Code regulates extortion and unlawful threats as crimes against property and individual freedom. Meanwhile, Law Number 11 Year 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 Year 2016, regulates the dissemination of false electronic information and electronic defamation. However, neither statute explicitly recognizes digital reputation as an economic interest that receives specific criminal law protection.

The absence of explicit recognition generates interpretative challenges. Can a threat to damage digital reputation be classified as an element of unlawful coercion under extortion provisions? Does the publication of negative reviews containing economic pressure fall within the scope of electronic information offenses? How should intent and causality be constructed in cases involving algorithm based reputational harm? These questions demonstrate potential normative ambiguity in addressing misconduct within the digital economy.

Based on this background, this research aims to analyse criminal law protection of digital reputation as an economic asset of Micro Small and Medium Enterprises under Law Number 1 Year 2023 and Law Number 11 Year 2008 as amended. The study focuses on the doctrinal interpretation of extortion elements, the relationship with electronic information offenses, and the implications for legal certainty within Indonesia digital economic governance. Through systematic and teleological interpretation, this research seeks to clarify the position of digital reputation within Indonesian criminal law and to contribute to the development of coherent legal protection in the digital era.

RESEARCH METHOD

This research employs a normative juridical method, which focuses on the analysis of legal norms as formulated in statutory regulations and doctrinal legal principles. The study does not rely on empirical field data but examines the coherence, adequacy, and interpretative scope of positive law in addressing online review extortion within the Indonesian legal system.

The primary approach used in this research is the statutory approach. This approach examines relevant provisions contained in Law Number 1 Year 2023 concerning the Criminal Code, particularly those regulating extortion, unlawful threats, attempt, participation, and corporate criminal liability. In addition, the study analyses Law Number 11 Year 2008 concerning Electronic Information and Transactions as amended by Law Number 19 Year 2016, focusing on provisions concerning dissemination of false electronic information and electronic defamation. The objective of this approach is to identify whether existing statutory elements are normatively capable of accommodating coercive manipulation of digital reputation.

This research also applies a conceptual approach. Through this approach, digital reputation is analysed as an intangible economic asset within criminal law doctrine. The study examines whether digital reputation can be categorized as a legally protected interest comparable to property or economic rights. Conceptual clarification is necessary to determine whether reputational harm in digital platforms satisfies the protected object requirement in extortion offenses.

Furthermore, the research utilizes systematic and teleological interpretation. Systematic interpretation is employed to assess the position of extortion provisions within the broader structure of the Criminal Code 2023. Teleological interpretation is applied to evaluate the legislative purpose underlying criminalization of coercive conduct, particularly the protection of economic autonomy and property interests. By integrating these interpretative methods, the study aims to reconstruct the doctrinal application of existing provisions to contemporary digital phenomena.

Legal materials in this research consist of primary legal sources, including the Criminal Code 2023 and the Electronic Information and Transactions Law as amended, as well as secondary legal materials such as scholarly journal articles, legal commentaries, and contemporary academic discussions published after 2020. These secondary sources are used to support doctrinal reasoning and to ensure the analysis reflects current developments in digital governance and criminal law discourse.

The analysis is conducted qualitatively through normative reasoning. Each statutory element is examined article by article, followed by doctrinal evaluation of its applicability to online review extortion. The research ultimately seeks to determine whether interpretative expansion is sufficient or whether legislative clarification is required to ensure legal certainty within Indonesia digital economy.

RESULTS AND DISCUSSION

Conceptualization of Digital Reputation as a Protected Legal Interest

Digital reputation in platform-based markets operates as a structured trust mechanism embedded within algorithmic systems. In contemporary digital environments, review systems function not merely as informal expressions of opinion but as institutionalized indicators of reliability and quality. Empirical studies consistently demonstrate that online reviews significantly influence purchasing behaviour, revenue performance, and price sensitivity (Wu et al., 2020; Munzel, 2021; Borchers, 2023). Rating scores operate as reputational capital that determines search ranking, platform visibility, and competitive positioning within digital ecosystems.

Post 2020 scholarship confirms that manipulation of review ecosystems generates measurable economic distortion. Mayzlin et al. (2021) demonstrate that deceptive and promotional reviews alter consumer perception and distort market competition. Lim (2025) identifies the emergence of structured review manipulation networks that strategically influence digital reputation for financial advantage. For Micro Small and Medium Enterprises, whose financial resilience is often limited, even minor fluctuations in digital ratings may result in immediate decline in transaction volume, liquidity constraints, and long term sustainability risks.

Within Indonesian criminal law, the concept of a protected legal interest traditionally encompasses property, personal freedom, honour, and public order. However, doctrinal development recognizes that criminal law may protect intangible interests when they possess economic value and social relevance. The Criminal Code 2023 reflects a modernized and adaptive approach, as indicated in its general objectives and systematic consolidation of contemporary forms of harm. Notably, extortion under Article 482 paragraph (1) protects against coercive surrender of property or economic advantage, while Article 483 paragraph (1) protects against coercion through threats of defamation or disclosure of secrets for economic gain. These provisions demonstrate that the protected legal interest extends beyond tangible property to encompass economic autonomy.

The principle of legality under Article 1 paragraph (1) of the Criminal Code 2023 requires that criminal liability be grounded in statutory provisions. However, legality does not preclude systematic interpretation of the protected interest when statutory elements are fulfilled. What becomes decisive is not the material form of the object but the presence of legally relevant economic value and the potential for harm.

Digital reputation satisfies at least three juridically significant criteria. First, it produces quantifiable economic effects, as evidenced by measurable changes in revenue following rating fluctuations (Wu et al., 2020; Chen et al., 2021). Second, it influences transactional decision making by reducing information asymmetry and shaping consumer trust (Borchers, 2023). Third, its manipulation may cause identifiable financial loss, particularly when negative reviews are strategically deployed to influence market perception.

Furthermore, digital governance literature emphasizes that trust infrastructures within online platforms are central to economic stability (OECD, 2023). When reputational systems are distorted, harm extends beyond individual enterprises and undermines systemic market confidence. This broader economic dimension reinforces the argument that digital reputation constitutes a legally relevant economic interest within the framework of crimes against property and economic autonomy.

Accordingly, although digital reputation is not expressly enumerated in statutory language, it may be doctrinally analysed as falling within the protective scope of extortion and coercion provisions under Articles 482 and 483 of the Criminal Code 2023, as well as electronic extortion provisions under Article 27B of the Electronic Information and Transactions Law as amended by Law Number 1 Year 2024. Recognizing its juridical relevance enables Indonesian criminal law to respond coherently to contemporary forms of digital economic harm without departing from existing statutory foundations.

Structural Interpretation of Extortion under Law Number 1 Year 2023

Law Number 1 Year 2023 concerning the Criminal Code regulates extortion as unlawful coercion aimed at obtaining economic benefit. The core provision is contained in Article 482 paragraph (1), which criminalizes compelling another person, with intent to unlawfully benefit oneself or another, through violence or threat of violence to surrender property, incur debt, acknowledge debt, or extinguish receivables.

In addition, Article 483 paragraph (1) criminalizes coercion carried out through threats of defamation, written defamation, or threats to disclose secrets for the purpose of obtaining economic benefit. These two provisions together establish the normative structure of extortion and coercive economic pressure.

Doctrinally, extortion consists of three essential elements:

1. The existence of unlawful threat or coercion.
2. The intent to obtain unlawful economic benefit.
3. The surrender of economic value as a consequence of the threat.

The statutory construction does not confine coercion to physical violence. Although Article 482 refers to violence or threat of violence, Article 483 explicitly recognizes non physical coercion through threats of defamation or disclosure of secrets. This indicates that the protected legal interest is not bodily integrity alone, but economic autonomy, namely freedom from forced transfer of property under unlawful pressure.

From a teleological perspective, extortion provisions aim to prevent economic decision making under fear. The fundamental rationale of criminalization is to protect individuals from being compelled to surrender economic value due to coercive pressure. Modern criminal law scholarship recognizes that coercion may arise not only from physical force but also from economic or psychological pressure when such pressure significantly restricts freedom of decision making (Furnell & Karweni, 2020).

In digital environments, reputational harm may generate substantial financial consequences, particularly in platform-based markets where visibility and consumer trust are algorithmically structured. Empirical research demonstrates that rating manipulation and exposure to negative reviews significantly influence purchasing behaviour and firm revenue (Wu et al., 2020; Chen et al., 2021). For Micro Small and Medium Enterprises, reputational degradation may result in immediate decline in sales and competitive disadvantage. Consequently, threats to damage digital reputation carry foreseeable economic consequences.

The central interpretative question is therefore whether algorithm based reputational manipulation may satisfy the element of unlawful threat under Articles 482 and 483. When reputational destruction is intentionally deployed as leverage to extract payment, its functional character mirrors traditional

economic coercion. The fear induced is not physical injury but financial loss. From a systematic and purposive interpretation, this form of pressure falls within the protective rationale of extortion doctrine because the law safeguards economic autonomy rather than merely protection from bodily harm.

Accordingly, a structural interpretation of Articles 482 and 483 supports the view that algorithm based reputational manipulation may, under certain conditions, fulfil the elements of extortion as regulated in Law Number 1 Year 2023.

Unlawful Threat in the Context of Algorithmic Reputational Harm

The concept of unlawful threat in extortion under Law Number 1 Year 2023 must be interpreted systematically rather than restrictively. Article 482 paragraph (1) of the Criminal Code 2023 criminalizes compelling another person, with intent to unlawfully benefit oneself or another, through violence or threat of violence to surrender property or assume economic obligation. Meanwhile, Article 483 paragraph (1) extends criminalization to coercion carried out through threats of defamation, written defamation, or threats to disclose secrets for the purpose of obtaining economic benefit.

The statutory formulation does not confine the concept of threat to bodily harm or physical violence. In criminal law doctrine, a threat exists when conduct generates fear sufficient to restrict the victim's freedom of economic decision making. The contemplated harm need not be physical. Economic harm may equally constitute coercive pressure when it significantly affects the victim's business interests.

In online review extortion, perpetrators typically communicate conditional statements indicating that payment will result in removal or mitigation of negative reviews, whereas non-payment will result in continued or intensified reputational damage. The conditional structure reveals its coercive nature. The reputational act is positioned as leverage, and economic compliance is presented as the only means of preventing foreseeable harm.

Empirical research confirms that rating manipulation significantly alters consumer behaviour and firm performance. Wu et al. (2020) demonstrate that fake or strategically manipulated reviews influence purchasing decisions and sales outcomes. Munzel (2021) explains that consumers often cannot distinguish between authentic and deceptive reviews, amplifying economic distortion. Borchers (2023) emphasizes that trust in digital platforms depends heavily on the perceived credibility of review systems. Consequently, threats to manipulate digital reputation carry measurable and foreseeable economic consequences, particularly for Micro Small and Medium Enterprises operating with limited financial resilience.

From a teleological perspective, extortion provisions aim to protect economic autonomy and prevent coercive transfer of property. The protected legal interest extends beyond tangible assets to freedom of economic decision making. When reputational destruction is intentionally used as leverage to extract payment, its functional effect mirrors traditional economic coercion, even though the medium is algorithmic rather than physical.

In addition to the general extortion doctrine under the Criminal Code 2023, the Electronic Information and Transactions Law as amended by Law Number 1 Year 2024 provides a more specific basis. Article 27B paragraph (2) criminalizes intentional and unlawful distribution of electronic information with the intent to obtain unlawful benefit by threatening defamation or disclosure of secrets in order to compel another person to surrender goods or incur debt. This provision directly accommodates review-based coercion where reputational harm is deployed as digital leverage.

Accordingly, review extortion may simultaneously fall under:

- Articles 482 and 483 of the Criminal Code 2023
- Article 27B paragraph (2) of Law Number 1 Year 2024 amending the Electronic Information and Transactions Law

To satisfy the unlawful threat element in digital contexts, three cumulative criteria may be articulated. First, the perpetrator intentionally employs reputational harm as leverage. Second, reputational harm is capable of generating measurable economic loss, as supported by empirical findings (Wu et al., 2020; Chen et al., 2021). Third, the threat is explicitly or implicitly conditional upon economic demand. Absent conditional demand, the conduct would remain within the realm of expression rather than coercion.

When these elements are fulfilled, algorithm based reputational manipulation may reasonably be subsumed within unlawful coercion. Such interpretation remains consistent with the protective purpose of the Criminal Code 2023 and the Electronic Information and Transactions Law, ensuring that economic autonomy is safeguarded against contemporary forms of digital pressure within Indonesia's evolving digital economy.

Mens Rea, Causality, and Conditional Economic Extraction

The subjective element of extortion requires the presence of intent to obtain unlawful economic benefit. Under Article 482 paragraph (1) of the Criminal Code 2023, extortion occurs when a person, with intent to unlawfully benefit themselves or another, compels another through violence or threat of violence to surrender property or assume economic obligation. Similarly, Article 483 paragraph (1) criminalizes coercion through threats of defamation or disclosure of secrets for economic gain.

The element of intent, or mens rea, functions as the decisive distinction between criminal coercion and lawful conduct. In the context of online review extortion, intentional economic extraction separates unlawful behaviour from ordinary consumer dissatisfaction. Legitimate negative feedback constitutes expressive conduct aimed at conveying dissatisfaction. By contrast, extortion scenarios are characterized by explicit or implicit conditional economic demands, such as offers to remove, modify, or cease reputational harm in exchange for payment. The reputational act becomes instrumental rather than expressive.

Recent empirical research demonstrates that fake review networks frequently operate in strategic and organized manners, reflecting deliberate planning rather than spontaneous consumer expression (Mayzlin et al., 2021; Lim, 2025). Posting schedules, rating patterns, and communication strategies are often coordinated to maximize economic leverage. In extortion contexts, negative reviews serve as calculated instruments of pressure designed to trigger fear of financial loss. Such structured conduct reinforces the inference of intentional economic extraction.

Causality further requires that economic surrender occur because of the unlawful threat. The victim's compliance must be attributable to reputational pressure rather than voluntary negotiation. In digital cases, causation may be established through objective indicators, including:

- Temporal proximity between the threat and economic transfer
- Explicit linkage between payment and review removal or modification
- Recorded digital negotiations and electronic correspondence
- Platform logs and payment documentation

Electronic communications such as chat logs, emails, digital payment instructions, and platform messages constitute admissible evidence under the Electronic Information and Transactions Law, which recognizes electronic documents and electronic information as valid legal proof. Documented negotiations linking reputational harm to monetary demand provide a strong evidentiary basis for establishing both intent and causality.

Even where payment has not yet occurred, criminal liability may arise under the general provisions on attempt contained in Book One of the Criminal Code 2023. Once execution of the offense has commenced, liability attaches even if completion is prevented by circumstances beyond the

perpetrator's control. Posting negative reviews combined with an explicit economic demand may constitute commencement of execution because the coercive mechanism has already been activated. The reputational pressure and the financial request form a unified coercive strategy.

Empirical literature confirms that reputational manipulation significantly affects business performance and revenue outcomes (Wu et al., 2020; Chen et al., 2021). Therefore, when a perpetrator threatens to intensify reputational harm unless payment is made, economic extraction becomes both foreseeable and intentional.

This interpretation remains consistent with the principle of legality under Article 1 paragraph (1) of the Criminal Code 2023, which requires that criminal liability be grounded in existing statutory provisions. The qualification of online review extortion as completed or attempted extortion does not rely on analogy but remains within the textual framework of Articles 482 and 483.

Recognizing mens rea, causality, and attempt at an early stage aligns with the preventive objectives of criminal law, particularly in digital environments where economic harm may escalate rapidly. Accordingly, Indonesian criminal law possesses a coherent doctrinal basis to address conditional economic extraction conducted through digital reputational leverage.

Causality and Attempt in Digital Extortion

Causality constitutes a central element in establishing extortion under the Criminal Code 2023. Pursuant to Article 482 paragraph (1), extortion requires that a person, with intent to unlawfully benefit themselves or another, compels another through violence or threat of violence to surrender property, incur debt, acknowledge debt, or extinguish receivables. Similarly, Article 483 paragraph (1) criminalizes coercion through threats of defamation or disclosure of secrets for economic gain.

In both provisions, the surrender of economic value must occur as a consequence of the unlawful threat. Thus, causality requires that the victim's economic compliance be attributable to coercive pressure rather than voluntary commercial negotiation.

In the context of online review extortion, economic compliance may take various forms, including monetary transfer, provision of goods, service discounts, promotional benefits, or other economic concessions. The decisive issue is whether the victim acted because of reputational pressure generated through digital platforms.

In digital environments, causality must be established through objective indicators. These may include:

- Temporal proximity between the threat and the economic transfer
- Explicit linkage between payment and removal or modification of negative reviews
- Recorded electronic communications demonstrating conditional demands
- Platform activity logs and payment records

Electronic correspondence, transaction documentation, and review modification history may collectively demonstrate that the economic surrender resulted directly from reputational coercion.

Empirical research confirms that online review manipulation produces measurable economic effects on firm performance (Wu et al., 2020; Chen et al., 2021). When perpetrators threaten to maintain or intensify reputational harm unless payment is made, the foreseeable financial loss becomes the motivating factor behind compliance. In such circumstances, the causal relationship between threat and economic surrender satisfies the doctrinal requirement of extortion.

Importantly, criminal liability is not limited to completed payment. Under the general provisions on attempt contained in Book One of the Criminal Code 2023, liability arises when the execution of a

criminal act has commenced but is not completed due to circumstances beyond the perpetrator's control. Once the coercive mechanism has been activated, the offense may be considered in progress.

In digital extortion, posting negative reviews combined with an explicit economic demand may constitute commencement of execution. The act of deploying reputational harm as conditional leverage already reflects the operationalization of coercion. Even if payment has not yet occurred, attempt liability may arise because the elements of coercive intent and execution have been initiated.

This interpretation remains consistent with the principle of legality under Article 1 paragraph (1) of the Criminal Code 2023, which requires that criminal liability be grounded in existing statutory provisions. The qualification of digital reputational coercion as either completed extortion or attempted extortion does not rely on analogy but remains within the textual scope of Articles 482 and 483.

Recognizing attempt liability at an early stage also aligns with the preventive function of criminal law. Digital coercion can generate rapid economic harm within networked environments, often before payment is finalized. As noted in contemporary cybercrime scholarship, early intervention is essential in digital offenses where reputational damage can escalate quickly (Furnell & Karweni, 2020).

Accordingly, a purposive and systematic interpretation of causality and attempt provisions enables Indonesian criminal law to respond effectively to online review extortion while remaining fully grounded in the existing statutory framework of the Criminal Code 2023.

Complementary Application of Electronic Information and Transactions Law

Law Number 11 Year 2008 concerning Electronic Information and Transactions as amended by Law Number 19 Year 2016 and most recently by Law Number 1 Year 2024 provides several provisions that are directly relevant to online review extortion.

First, Article 28 paragraph (1) criminalizes the dissemination of false and misleading electronic information that causes material loss to consumers. This provision becomes applicable when negative online reviews contain objectively fabricated factual claims, such as false allegations regarding product defects, regulatory violations, fraud, or unsafe business practices. Where falsity can be demonstrated and material loss is established, liability may arise under this article.

However, contemporary research demonstrates that deceptive online reviews rarely rely on clearly falsifiable statements. Instead, they frequently employ ambiguous, subjective, or emotionally charged language that is strategically designed to evade strict evidentiary standards (Munzel, 2021; Wu et al., 2020). Reviews may express dissatisfaction in vague terms or rely on insinuation rather than verifiable falsehood. Because Article 28 paragraph (1) requires proof of falsity and material loss, this ambiguity often complicates prosecution. As a result, reliance solely on false information provisions may be insufficient in cases of review-based coercion.

Second, Article 29 criminalizes sending electronic information containing threats of violence or intimidation directly to a specific person. This provision is particularly relevant where perpetrators communicate private messages to business owners stating that negative reviews will remain published or be escalated unless payment is made. In such circumstances, the electronic threat itself may independently constitute an offense under Article 29.

Third, the amended framework also introduces Article 27B, which explicitly addresses electronic extortion and coercion. This provision strengthens the legal basis for prosecuting digital economic pressure conducted through electronic systems, especially where reputational harm is used as leverage to obtain unlawful financial benefit.

Despite these specific provisions, it is important to recognize their respective normative focus. Article 28 paragraph (1) addresses false electronic content. Article 29 addresses direct electronic intimidation. Article 27B addresses electronic extortion. None of these provisions alone fully captures

the structural economic dimension of review-based coercion when reputational harm functions as instrumental leverage for economic extraction.

In contrast, Articles 482 and 483 of the Criminal Code 2023 regulate extortion and coercive threats in a broader doctrinal framework, focusing on unlawful economic compulsion. Article 482 criminalizes coercion through violence or threat of violence to obtain property or economic advantage, while Article 483 criminalizes coercion through threats of defamation or disclosure of secrets for economic gain. These provisions are particularly relevant where reputational damage is used as a conditional bargaining instrument.

Accordingly, effective legal protection against online review extortion requires an integrated interpretation between the Electronic Information and Transactions Law and the Criminal Code 2023. The Electronic Information and Transactions Law addresses unlawful electronic content, direct electronic threats, and digital extortion mechanisms. The Criminal Code 2023 provides the general doctrine of economic coercion and protection of economic autonomy. Harmonized application ensures that digital reputational manipulation is assessed not only from the perspective of informational falsity but also from the standpoint of unlawful economic pressure and coercive extraction of benefit.

Such integrated enforcement strengthens legal certainty and enhances the integrity of Indonesia's digital economic governance framework.

Participation and Organized Digital Coercion

The Criminal Code 2023 regulates extortion under Article 482 paragraph (1), which criminalizes compelling another person, with intent to unlawfully benefit oneself or another, through violence or threat of violence to surrender property, incur debt, acknowledge debt, or extinguish receivables.

In addition, Article 483 paragraph (1) criminalizes coercion carried out through threats of defamation, written defamation, or threats to disclose secrets in order to compel the surrender of property or acknowledgment of debt. This provision is highly relevant in the context of online review extortion, where reputational harm is strategically deployed as leverage to obtain economic benefit.

Beyond the substantive offense, KUHP 2023 recognizes the doctrine of participation within its General Provisions in Book One. Criminal responsibility therefore extends not only to principal perpetrators but also to accomplices and instigators who intentionally contribute to the commission of the offense. This doctrinal structure is essential in cases where the criminal act is not carried out by a single individual but through coordinated action among multiple actors.

Online review extortion frequently reflects organized digital coercion rather than isolated misconduct. Different individuals may perform differentiated roles, such as creating or controlling accounts, posting negative reviews, communicating threats to business owners, negotiating payments, or receiving financial transfers. Recent research shows that review manipulation services increasingly operate as organized digital enterprises providing systematic reputational distortion for economic gain (Lim, 2025). In such arrangements, the individual who publishes the review may not be the same person who demands payment. Nevertheless, where there is shared intent and coordinated contribution, participation doctrine allows liability to extend to each contributor.

Furthermore, KUHP 2023 recognizes corporate criminal liability within its general framework of criminal responsibility. Where reputational manipulation operates as a structured business model supported by internal organization, financial benefit, and coordinated strategy, responsibility may attach not only to individual actors but also to the corporate entity itself. This is particularly important when digital coercion becomes commercialized practice embedded within organized service providers.

Through the combined application of Articles 482 and 483 KUHP 2023, together with the doctrines of participation and corporate liability contained in Book One, Indonesian criminal law provides a

normative basis capable of addressing organized digital coercion as a collective and economically motivated criminal practice within the digital economy.

Normative Ambiguity and Legal Certainty

The principle of legality requires clarity, precision, and foreseeability of criminal norms. In criminal law, the maxim nullum crimen sine lege ensures that no conduct may be punished unless it is clearly defined by statute prior to its commission. This principle embodies three fundamental dimensions: lex scripta, which requires that criminal norms be written in legislation; lex certa, which requires that the elements of an offense be clearly formulated; and lex stricta, which prohibits analogical expansion of criminal provisions. Legal certainty is therefore inseparable from legality, as the protected legal interest and the scope of prohibited conduct must be sufficiently defined to enable uniform and predictable application.

The principle of legality is expressly affirmed in Article 1 paragraph 1 of Law Number 1 Year 2023 concerning the Criminal Code, which provides that no act may be punished except on the basis of criminal provisions in legislation that existed prior to the commission of the act. This statutory affirmation reinforces the constitutional requirement that criminal liability must remain anchored in existing legislative text.

Although the extortion provisions under Law Number 1 Year 2023 may, through systematic and teleological interpretation, encompass digital reputational coercion, the absence of explicit statutory reference to digital reputation as a protected economic interest initially appears to create normative ambiguity. Courts may therefore be required to interpret whether algorithm based reputational manipulation satisfies the unlawful threat element of extortion.

Such interpretation must remain within the limits of lex stricta. Criminal liability cannot be constructed through analogy. However, qualification of review-based extortion does not depend on analogical reasoning. Article 27B of the Electronic Information and Transactions Law explicitly criminalizes electronic extortion involving threats of defamation or disclosure aimed at compelling surrender of economic value. When reputational harm is intentionally deployed as leverage for financial extraction, the conduct falls within the textual boundaries of both the Criminal Code 2023 and Article 27B of the Electronic Information and Transactions Law.

Thus, prosecution of online review extortion does not violate nullum crimen sine lege, because the conduct is subsumed under existing statutory provisions rather than created through judicial expansion. At the same time, doctrinal clarity remains essential to satisfy lex certa. If the boundaries of unlawful threat in relation to algorithm based reputational harm are inconsistently articulated, judicial interpretation may vary across cases. Variability undermines predictability and weakens uniform enforcement.

Digital governance scholarship indicates that regulatory ambiguity diminishes institutional trust and limits deterrence effectiveness (OECD, 2023). Empirical studies on review manipulation further demonstrate that uncertainty regarding legal consequences contributes to inconsistent reporting and uneven enforcement (Wu et al., 2020; Munzel, 2021). For Micro Small and Medium Enterprises, ambiguity in legal qualification may discourage formal reporting and encourage informal settlement, thereby weakening the rule of law in digital markets.

From the perspective of legality, criminal norms must balance adaptability with certainty. The Criminal Code 2023 provides interpretative flexibility to address contemporary economic harm, while Article 27B of the Electronic Information and Transactions Law offers explicit textual grounding for electronic extortion. Strengthening doctrinal articulation that algorithm based reputational coercion constitutes unlawful threat reinforces foreseeability, complies with lex scripta, satisfies lex certa, and respects lex stricta.

Clarifying the application of existing provisions therefore strengthens rather than weakens the principle of legality. By ensuring that both perpetrators and victims understand the legal consequences of digital reputational coercion, criminal law enhances predictability, uniformity, and trust within Indonesia's digital economic governance framework.

Economic Governance Implications

Digital reputation constitutes a foundational component of platform based economic governance. In digital marketplaces, review systems function as trust infrastructure that reduces information asymmetry between sellers and consumers. Empirical research demonstrates that online reviews significantly influence consumer trust formation, purchasing behaviour, and revenue performance (Wu et al., 2020; Borchers, 2023). Reputation mechanisms therefore sustain transactional efficiency by enabling market participants to make informed decisions in the absence of direct interpersonal interaction.

The integrity of this reputational infrastructure is essential for maintaining stable digital markets. When online review extortion is inadequately addressed, the resulting distortion affects not only individual enterprises but also the governance structure of platform-based commerce. Manipulation of review systems undermines consumer confidence and disrupts efficient market allocation (Munzel, 2021; Mayzlin et al., 2021). If rating systems are perceived as vulnerable to coercion or strategic abuse, trust in the broader platform ecosystem deteriorates.

At least three systemic consequences may arise when enforcement remains weak or normatively ambiguous.

First, increased reliance on informal settlement outside judicial oversight may occur. Business actors facing reputational threats may choose immediate compliance rather than pursue formal legal remedies in order to prevent prolonged algorithmic damage. Such informal resolution mechanisms weaken deterrence and allow coercive practices to persist without institutional accountability.

Second, private protection costs may increase. Micro Small and Medium Enterprises may be compelled to invest in reputation monitoring services, digital defence strategies, legal consultations, or paid promotional mechanisms to offset reputational harm. These additional expenditures reduce operational efficiency and disproportionately burden smaller enterprises with limited financial resilience.

Third, weak or inconsistent enforcement may reduce confidence in digital market regulation. Predictable legal protection is a core element of economic governance. When criminal law fails to provide clear protection against coercive manipulation of trust systems, regulatory credibility may erode (OECD, 2023). Market actors require assurance that reputational mechanisms are safeguarded against exploitation.

In the Indonesian regulatory framework, Article 40 and Article 40A of Law Number 1 Year 2024 emphasize the government's responsibility to create a fair, accountable, safe, and innovative digital ecosystem. Effective enforcement of extortion provisions under the Criminal Code 2023 and the Electronic Information and Transactions Law directly supports this regulatory objective. Protecting digital reputation from coercive manipulation is therefore not merely a criminal justice issue but a structural requirement of digital economic governance.

Economic governance depends on consistent and predictable enforcement of rules that protect trust mechanisms within digital ecosystems. Criminal law clarity serves not only punitive functions but also stabilizing functions by reinforcing market integrity. Clear recognition that coercive manipulation of digital reputation constitutes unlawful conduct strengthens deterrence, supports fair competition, and enhances confidence in Indonesia's digital economic framework.

Doctrinal Reconstruction within Indonesian Legal Framework

Doctrinal reconstruction is necessary to ensure that existing criminal law provisions effectively respond to online review extortion within Indonesia's evolving digital economy. Rather than introducing entirely new legal categories, reconstruction can proceed through systematic and purposive interpretation of existing statutory norms. Such an approach is consistent with the adaptive character of criminal law in addressing new forms of economic harm emerging from digital environments (Furnell & Karweni, 2020).

First, digital reputation must be recognized as an economically valuable legal interest within the framework of crimes against property and economic autonomy. Empirical studies confirm that online reviews significantly influence consumer trust, purchasing behaviour, and revenue performance (Wu et al., 2020; Borchers, 2023). For Micro Small and Medium Enterprises, reputational degradation may immediately result in measurable financial loss. When an intangible interest produces concrete and foreseeable economic consequences, it may doctrinally be treated as part of property related interests protected by criminal law. Recognizing digital reputation within this structure strengthens the normative foundation for qualifying its coercive manipulation as an offense against economic autonomy.

Second, the concept of unlawful threat under extortion provisions should be interpreted functionally rather than restrictively. The Criminal Code does not confine threat to physical violence. Contemporary digital practices demonstrate that economic pressure may arise through algorithm based reputational mechanisms embedded in platform governance structures (Munzel, 2021; Mayzlin et al., 2021). When a perpetrator intentionally deploys algorithm based reputational destruction to compel payment or economic concession, the conduct constitutes economic coercion in substance. Therefore, reputational manipulation that is conditional upon monetary demand may reasonably satisfy the element of unlawful threat within extortion doctrine.

Third, harmonization between KUHP 2023 and the Electronic Information and Transactions Law is essential to ensure coherent enforcement strategy. The Criminal Code addresses coercion and unlawful economic extraction, while the Electronic Information and Transactions Law regulates false electronic information, electronic threats, and digital communication. Coordinated interpretation prevents normative fragmentation, avoids overlapping or inconsistent application, and supports an integrated enforcement model within Indonesia's digital governance framework (OECD, 2023).

This doctrinal reconstruction remains fully grounded in Indonesian statutory law. It strengthens legal certainty, protects economic autonomy of Micro Small and Medium Enterprises, and enhances stability within the national digital economy. Importantly, it does so without reliance on comparative legal borrowing, relying instead on purposive and systematic interpretation of existing legislative instruments.

CONCLUSIONS

The rapid development of Indonesia's digital economy has transformed digital reputation from a mere symbolic construct into a measurable and strategically decisive economic asset for Micro Small and Medium Enterprises. Within platform-based markets, rating systems and consumer reviews function as algorithmic gatekeepers of visibility, trust, and revenue sustainability. Digital reputation therefore constitutes reputational capital with direct and quantifiable economic consequences.

This study demonstrates that online review extortion is not a regulatory anomaly nor a legal grey area. It constitutes a prosecutable form of economic coercion under the existing Indonesian legal framework. When reputational harm is intentionally deployed as conditional leverage for financial extraction, the conduct satisfies the structural elements of extortion under Articles 482 and 483 of Law Number 1 Year 2023 concerning the Criminal Code. Simultaneously, such conduct may fall within Article 27B of the Electronic Information and Transactions Law as amended by Law Number 1 Year

2024, which explicitly criminalizes electronic extortion involving threats of defamation or disclosure aimed at compelling economic surrender.

Electronic evidence is admissible pursuant to Article 5 of the Electronic Information and Transactions Law. Where fabricated factual allegations are disseminated and cause material loss, Article 28 paragraph 1 becomes applicable. Direct electronic intimidation may independently fall under Article 29. Participation and corporate liability doctrines under the Criminal Code 2023 further ensure that accountability extends to organized digital coercion networks and commercialized manipulation services, rather than being confined to individual actors.

Accordingly, Indonesian criminal law already possesses a coherent doctrinal architecture capable of addressing algorithm based reputational coercion. Qualification of review-based extortion does not require analogical expansion and does not violate the principle of legality under Article 1 paragraph 1 of the Criminal Code 2023. The conduct falls squarely within existing legislative text.

Nevertheless, the absence of explicit statutory recognition of digital reputation as a protected economic interest creates avoidable interpretative hesitation. Legislative clarification would enhance legal certainty, reduce enforcement disparity, and strengthen deterrence. Such clarification would not expand criminalization, but rather articulate more clearly the protected object already embedded within extortion doctrine: economic autonomy.

Protecting digital reputation is therefore not merely about safeguarding business image. It is about preserving economic freedom, maintaining trust infrastructure within digital markets, and ensuring that Indonesia's digital transformation operates within a predictable and enforceable rule of law framework. Online review extortion should be understood and enforced as what it truly is: a contemporary manifestation of unlawful economic coercion, fully prosecutable under Indonesian criminal law.

REFERENCES

Borchers, N. S. (2023). Why do we trust online reviews? Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 17(2). https://doi.org/10.5817/CP2023-2-7

Chen, Y., Wang, Q., & Xie, J. (2021). Online review manipulation and its economic consequences. Electronic Commerce Research and Applications, 46, 101039. https://doi.org/10.1016/j.elerap.2021.101039

Filieri, R., & McLeay, F. (2021). E WOM and accommodation: The role of digital reputation in consumer trust. International Journal of Hospitality Management, 92, 102715. https://doi.org/10.1016/j.ijhm.2020.102715

Furnell, S., & Karweni, T. (2020). Cybercrime and digital manipulation: Emerging threats in online ecosystems. Computer Law & Security Review, 36, 105393. https://doi.org/10.1016/j.clsr.2020.105393

Kim, J., & Kim, M. (2022). Trust formation in digital review systems. Journal of Business Research, 139, 1521–1530. https://doi.org/10.1016/j.jbusres.2021.10.034

Lim, W. M. (2025). The rise of fake reviews in digital markets. Journal of Marketing Analytics. https://doi.org/10.1057/s41270-024-00210-3

Mayzlin, D., Dover, Y., & Chevalier, J. (2021). Promotional reviews and economic distortion in online markets. American Economic Review: Insights, 3(4), 461–476. https://doi.org/10.1257/aeri.20200489

Munzel, A. (2021). Detecting fake reviews in digital commerce: The role of consumer skepticism. Journal of Retailing and Consumer Services, 60, 102462. https://doi.org/10.1016/j.jretconser.2021.102462

Ransbotham, S., & Mitra, S. (2022). Reputation systems and economic impact in online marketplaces. MIS Quarterly Executive, 21(3), 205–219.

Rogers, M., & Seigfried-Spellar, K. (2020). Cybercrime investigation and digital evidence in the modern era. Journal of Digital Forensics, Security and Law, 15(2), 1–15.

Saidon, R., & Hashim, H. (2021). Legal challenges in regulating fake online reviews. International Journal of Law and Information Technology, 29(4), 289–305. https://doi.org/10.1093/ijlit/eaab021

Tadelis, S. (2021). Reputation and platform governance. Annual Review of Economics, 13, 147–170. https://doi.org/10.1146/annurev-economics-082120-051450

Wu, Y., Ngai, E., Wu, P., & Wu, C. (2020). Fake online reviews: Literature review and future research directions. Decision Support Systems, 132, 113280. https://doi.org/10.1016/j.dss.2020.113280

Xu, Q., Chen, J., & Santhanam, R. (2021). The economic value of online reviews. Information Systems Research, 32(4), 1235–1252. https://doi.org/10.1287/isre.2021.1017

Yoo, B., & Gretzel, U. (2020). Influence of online reputation systems on consumer decision making. Journal of Travel Research, 59(7), 1234–1249. https://doi.org/10.1177/0047287519895031

Zhang, Z., & Gupta, A. (2022). Review manipulation and regulatory challenges in digital marketplaces. Electronic Markets, 32(3), 1523–1538. https://doi.org/10.1007/s12525-021-00485-2

OECD. (2023). Consumer policy and digital platforms: Addressing misleading online reviews. OECD Publishing.

Republic of Indonesia. (2008). Law Number 11 Year 2008 concerning Electronic Information and Transactions.

Republic of Indonesia. (2016). Law Number 19 Year 2016 concerning Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions.

Republic of Indonesia. (2023). Law Number 1 Year 2023 concerning the Criminal Code.

Republic of Indonesia. (2024). Law Number 1 Year 2024 concerning Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions.